# *Contents*

10. ***China, Hong Kong, Macau (Traditional Chinese language)***

11. ***China, Hong Kong, Macau (Simplified Chinese language)***

12. ***Czech Republic (English language)***

13. ***Czech Republic (Czech language)***

14. ***French (French language)***

15. ***Hungary***

16. ***Middle East***

17. ***New Zealand***

18. ***Singapore***

19. ***Slovakia (English language)***

20 ***Slovakia (Slovak language)***

21. ***Sweden (in Swedish)***

22. ***Switzerland***

23. ***South Africa***

24. ***United Kingdom***

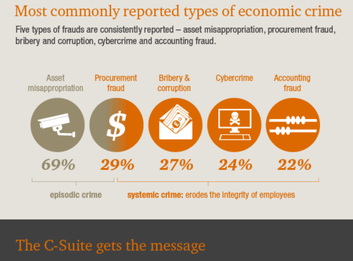
25. ***US Chartpack***

26. ***US Supplement***

# *Economic crime*
# What you need to know

Economic crime continues to be a major concern for organisations of all sizes, across all regions and in virtually every sector. One in three organisations reports being hit by economic crime.

**37%**




## Most commonly reported types of economic crime

Five types of frauds are consistently reported – asset misappropriation, procurement fraud, bribery and corruption, cybercrime and accounting fraud.


## The C-Suite gets the message

**53%** are concerned about the effect of bribery and corruption on their business

*Q* How concerned are you about the following potential business threats to your organisation? ***Bribery & corruption***

*Q* How concerned are you about the following potential business threats to your organisation? ***Cyber threats including lack of data security***

**49%** of global CEOs are concerned about cyber threats to their organisation

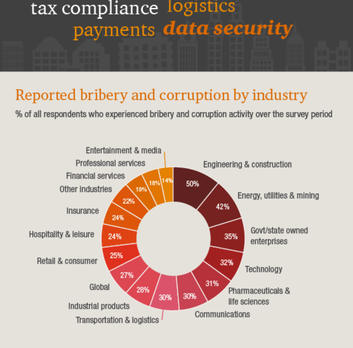
**43%** are concerned about inability to protect intellectual property

*Q* How concerned are you about the following potential business threats to your organisation? ***Inability to protect intellectual property***

Data from PwC's 17th Annual Global CEO Survey

## Where does economic crime occur?

Economic crime is a pervasive global threat. The highest levels of economic crime are consistently reported by respondents in Africa (50%) and North America (41%).




## Which industries are at risk?

By industry, economic crime is most commonly reported in the financial services, retail and consumer, and communications sectors. Nearly 50% of respondents in each said they had been crime victims.


## Processes under threat

Economic crimes threaten the basic processes common to all businesses – paying and collecting, buying and selling, growing and expanding, sourcing and supply chain.

***procurement***
distribution supply chain
marketing ***recruitment***
***onboarding*** ***sales*** international expansion
intellectual property ***vendor selection***
tax compliance logistics
payments ***data security***

## Reported bribery and corruption by industry

% of all respondents who experienced bribery and corruption activity over the survey period




## What's the impact on your business?

Businesses face threats from both internal and external sources and multiple angles. The internal threat has the greatest impact when senior managers are involved.



**Profile of a typical internal fraudster**

| | |
|---|---|
| Gender | male |
| Age | 31-40 years |
| Length of service | 6 or more years |
| Education level | 1st degree, graduate |

**Economic crime erodes employee integrity, your reputation and the bottom line**

pwc

# *Economic crime: A threat to business globally*

**37%**
More than one in three organisations report being victimized by economic crime.

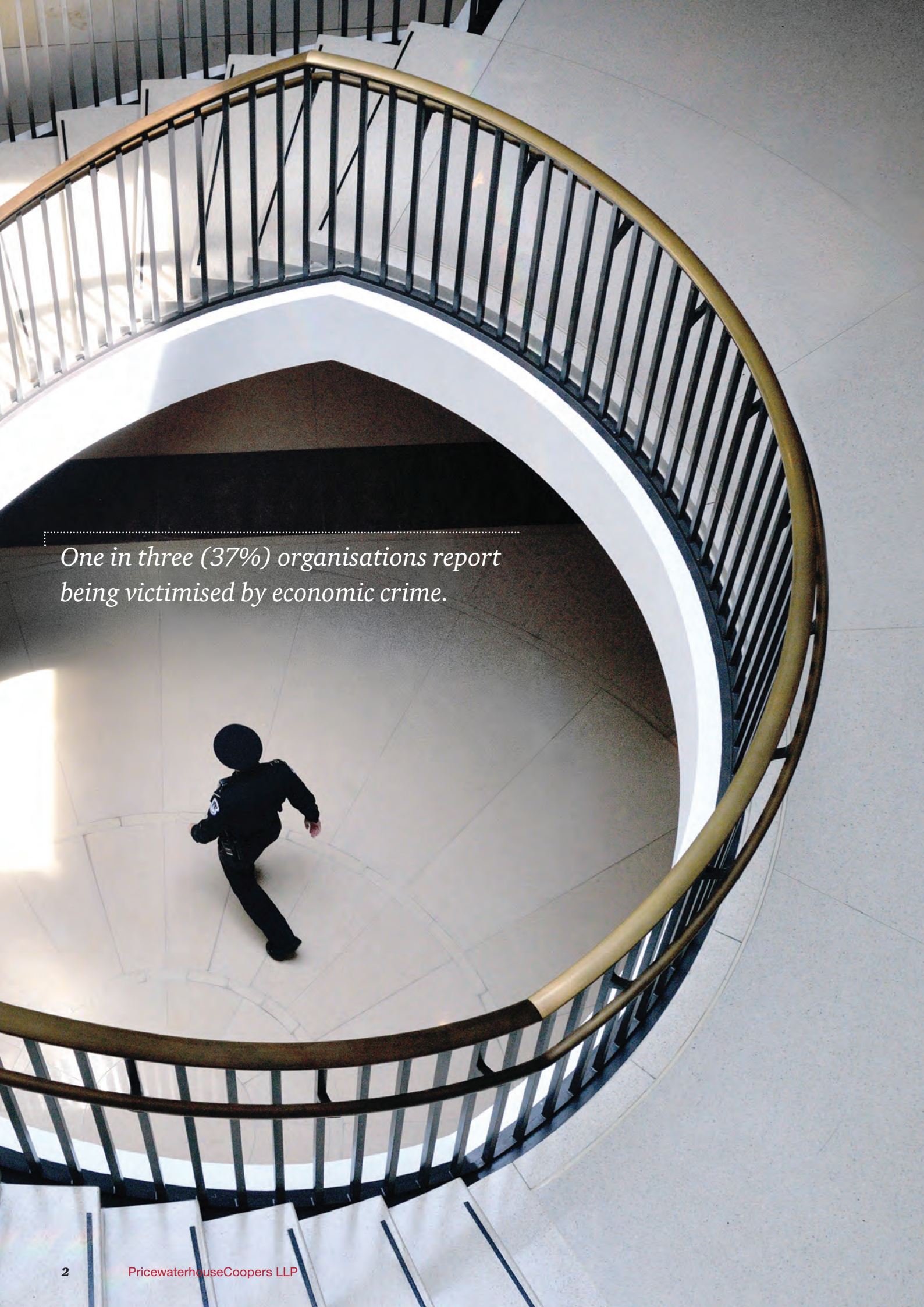
**53%**
More than half of CEOs surveyed reported being concerned about bribery and corruption.

**48%**
Nearly half of our respondents reported the risk of cybercrime had increased, a 23% increase from 2011.

pwc

*Economic crime continues to be a major concern for organisations of all sizes, across all regions and in virtually every sector.*

# Contents



*One in three (37%) organisations report being victimised by economic crime.*

# *Foreword*

It will surprise few to learn that economic crime—such as fraud, IP infringement, corruption, cybercrime, or accounting fraud—continues to be a major concern for organisations of all sizes, across all regions and in virtually every sector.

That's one headline from our *2014 Global Economic Crime Survey,* one of the broadest and most comprehensive economic crime surveys we have ever conducted, with over 5,000 respondents contributing from every corner of the world.

But the real story is not so much that economic crime stubbornly persists. *The real story is that economic crime is threatening your business processes, eroding the integrity of your employees, and tarnishing your reputation.* Which is why this year's report is focused on how and where it may be affecting you—so you can address the issue from both a preventive and a strategic perspective.

The threats from economic crime continue to evolve. Like a virus, economic crime adapts to the trends that affect all organisations. Especially impactful megatrends include the increasing reliance on technology and technology-enabled processes in all aspects of business, and the growing movement of economic energy toward emerging markets.

With organisations increasingly depending on technology, it's perhaps not surprising to find that cybercrime continues to increase in volume, frequency and sophistication. One quarter of all respondents report having been victimised by electronic fraud. Meanwhile, sometimes-overlooked categories of economic crime—such as procurement fraud, money laundering and human resource fraud—are moving up the list of threats, alongside the historically common threats of asset misappropriation, bribery and corruption, and accounting fraud.

Economic crimes fundamentally threaten the basic processes common to all business—buying and selling, paying and collecting, importing and exporting, growing and expanding. All organisations in the course of daily business face exposure to various types of economic crime from multiple angles that threaten these activities as they interact with third parties to create or exchange value.

Small wonder, then, that economic crime is very much on CEOs' minds. More than half of global chief executives, polled in our just-released *2014 Global CEO Survey,* told us they are concerned or extremely concerned about bribery and corruption.

Our hope is that this report will serve *all* your stakeholders, from the board down, as both a useful reference point in an unending campaign—and a useful tool in your business arsenal in the months to come.

—Steven L. Skalak

# Highlights

- Economic crime is a persistent threat to business and business processes—37% of respondents reported economic crime.
- The schemes used may vary, but the global threat remains—Respondents from 79 territories reported experiencing economic crime.
- Economic crimes of a "systemic" nature, such as bribery and corruption, money laundering, and anticompetitive practices, are more regularly examined by regulators and represent a greater risk than "episodic" frauds.
- The most damaging forms of economic crime exploit the tension between two equally fundamental business goals—profit and compliance. Organisations with operations in high risk markets were twice as likely to report being asked to pay a bribe.

*Economic crime threatens a wide variety of business processes, including:*

**Figure 1: Business processes threatened by economic crime**

| | |
|---|---|
| • Sales (or selling) | • Customer "on-boarding" |
| • Marketing | • International expansion |
| • Bidding | • Tax compliance |
| • Procurement | • Facilities construction, leasing and operations |
| • Payments | • Hiring and recruiting |
| • Vendor selection | • Suspicious transaction reporting |
| • Distribution | • IP development and deployment |
| • Logistics | • Data security and privacy |
| • Access to commodities and resources | • IT network operations |
| • Supply chain operations | • Employee expense reimbursement |

- Cybercrime reports continue to rise. It is the fourth-most reported type of crime in this year's survey. However, cybercrime is not just a technology problem. It is a business strategy problem.
- Over the 14 years we have been conducting our Global Economic Crime Survey, the effectiveness of internal controls in detecting economic crime has improved. Respondents to this year's survey report 55% of instances were uncovered by internal controls, be they preventative or detective—up from 50% in 2011.
- Economic crime follows megatrends—such as the movement of wealth from the West to the South and East and the increasing use of technology platforms for all types of business processes.
- There was a relative increase of 13% in reported incidences of bribery and corruption since our last survey; the 17th Annual CEO survey reveals that more than half of CEOs are concerned about bribery and corruption.

*Thirty-seven percent of our respondents reported that their organisation had experienced economic crime during the survey period, an increase of 3 percentage points from our 2011 survey.*

# *Economic crime in 2014*
## The big picture

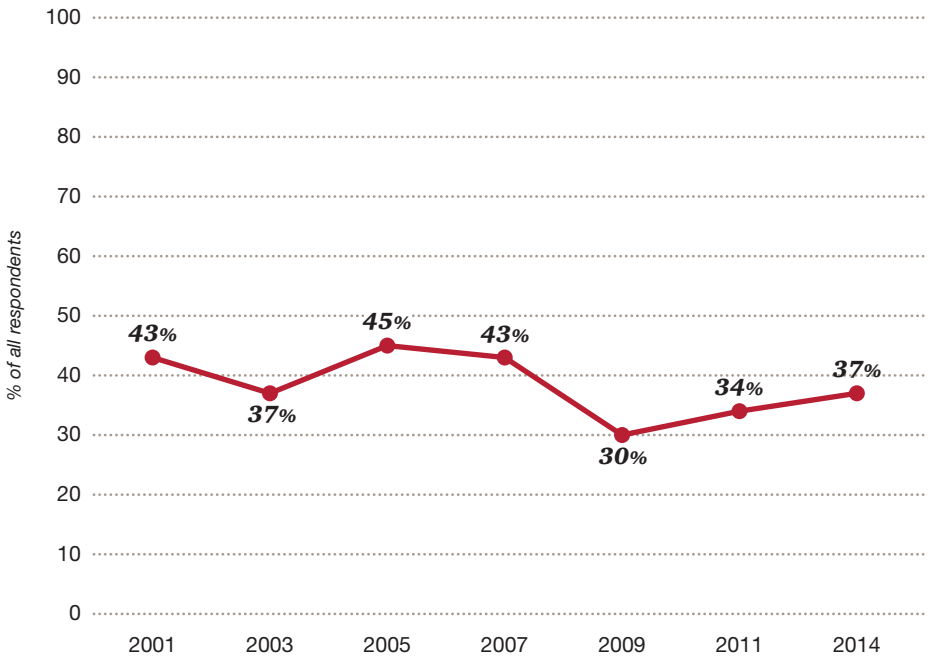
Our 2014 survey respondents included 5,128 representatives from over 95 countries around the world. More than half (54%) of our respondents were employed by organisations with more than 1,000 employees, and over one third (35%) of the survey population represented publicly traded companies.

This year's survey confirms that economic crime remains a fundamental fact of life for every segment of the global business community. Thirty-seven percent of our respondents reported that their organisation had experienced economic crime during the survey period, an increase of 3 percentage points from our 2011 survey.

Economic crime comes in many varieties, each with its own characteristics, threats and strategic consequences. In this report, we address the major crimes in more detail. We analyse today's numbers and our respondents' predictions of tomorrow's, discuss the business processes these economic crimes attack, and offer some additional real-world examples and insights.

While it may ebb and flow in virulence and variety, our 14 years of survey data shows that at any given time period, nearly one in three of those surveyed report suffering a significant economic crime event.

**Figure 2: Evolution of reported rate of economic crime (GECS)**



## Types of fraud

Since our first economic crime survey in 2001, three types of frauds have consistently been highlighted by our respondents—asset misappropriation (usually by a wide margin), bribery and corruption, and accounting fraud. We added cybercrime as a distinct classification in 2011.

This year, we added another new category, procurement fraud. We believe this category is primarily driven by two trends—more-competitive public tender processes from governments and state-owned businesses, and the increasing integration of supply chain into core business activities. Procurement fraud received a significant response (29%), making it the second most frequently reported type of fraud experienced. Thus, from a longstanding identification of three most-prevalent crimes (i.e., those reported by at least one in five respondents), we now have five.

In addition to procurement fraud, we added two other classifications in 2014—human resources fraud and mortgage fraud. Respondents also included a wide range of crimes in the "Other" category, including insurance fraud, loan fraud and credit card fraud.

Figure 3 breaks down the types of economic crime reported by our respondents.

**Figure 3: Types of economic crime reported**


*% of all respondents who experienced economic crime over the survey period*

## The regional story

At the regional level, African respondents continue to report the highest percentage of economic crime, though the gap has narrowed significantly since 2011.

North America consistently reports a high percentage of economic crime, reflecting the global reach of respondents and the sophisticated levels of detection processes. The strong increase seen in Western Europe may be attributable to the recent heightened focus of regulators, including the EU, particularly around banking and financial services frauds, as discussed later in the report.

The Middle East presents a unique situation: while the overall levels of economic crime reported there were the lowest of all, those respondents who did report fraud indicated a high number of types and instances of fraud.

**Figure 4: Economic crime reported by region**

| Territory | Reported Fraud 2014 | Reported Fraud 2011 |
|---|---|---|
| Africa | 50% | 59% |
| North America | 41% | 42% |
| Eastern Europe | 39% | 30% |
| Latin America | 35% | 37% |
| Western Europe | 35% | 30% |
| Asia Pacific | 32% | 31% |
| Middle East | 21% | 28% |
| Emerging Eight* | 40% | 35% |
| **Global** | **37%** | **34%** |

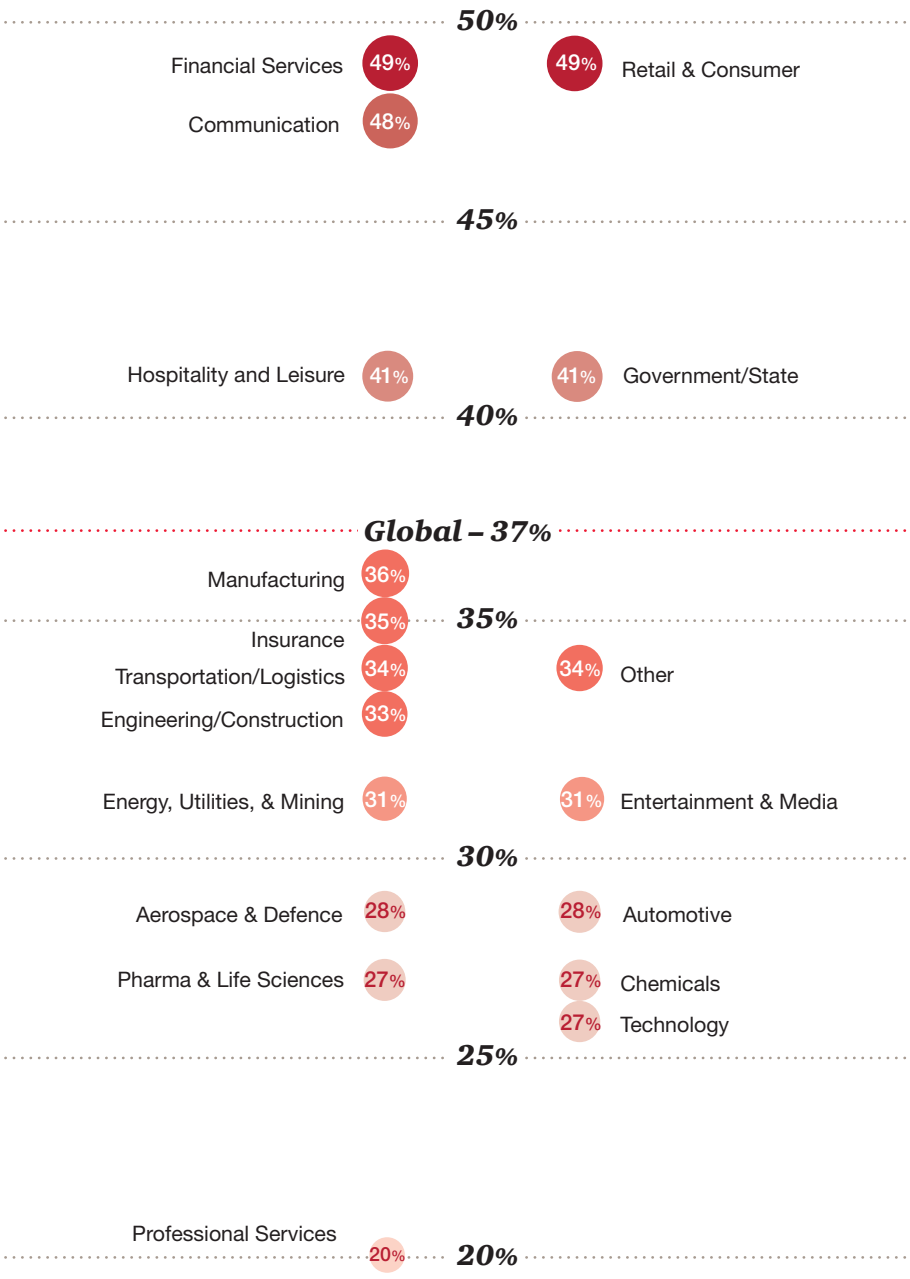
**Emerging Eight include Brazil, China, India, Indonesia, Mexico, Russia, Turkey, and South Africa*

## Economic crime across industries

At the industry level, three sectors stand out for reports of economic crime—financial services, retail and consumer, and communication. Financial services fraud levels appear driven by comparatively high levels of cybercrime and money laundering. The retail and consumer sector, as expected, experienced a comparatively high level of asset misappropriation, as did the communication sector.

There was a large clustering of industries reporting fraud in the 27% to 36% range. While the overall reported percentages are lower than the global mean, many of these industries—in particular the extractive, construction and logistics industries—are relatively more prone to experiencing economic crimes such as bribery and corruption or procurement fraud.

**Figure 5: Economic crime reported by industry**




*% of all respondents who experienced economic crime over the survey period*

*While economic crimes related to a specific episode certainly cause losses, systemic economic crimes have the greater impact.*

# Two kinds of threat

Why is the threat of economic crime so pervasive across a business? As we noted in the introduction, most fundamental business processes—distributing goods, raising financial capital, leveraging intellectual property, selecting business partners, reporting financial results, running a compliant organisation, establishing a brand identity, etc.—rest on the basic process of exchange of cash or other consideration with third parties. These points of contact are generally the vulnerable points where economic crime can threaten.

From an analytical point of view, we can distinguish between two different kinds of threats.

If asset misappropriation, for example, is akin to a pickpocketing or burglary (a *specific* episode of loss due to specific actions), a serious violation of an anti-bribery statute such as the US Foreign Corrupt Practices Act (FCPA) or the UK Bribery Act—or having your organisation compromised by a money laundering scheme—is a more *systemic* assault on your company.

While economic crimes related to a specific episode certainly cause losses, systemic economic crimes have the greater impact. Not only can enforcement of these crimes lead to substantial fines and a black mark on your reputation, they can cause lasting damage. They erode the integrity of employees and exploit weaknesses in internal control structures in a company's sales, marketing, distribution, compliance, supply chain, payments processing, government relationships, and accounting and financial reporting.

## *How corruption and bribery threaten your business processes*

*To highlight the threat that economic crimes of all types pose to numerous basic business processes, consider the following scenario, compiled from our portfolio of real-world experiences.*

A global company seeks growth in a culture where the risk of corruption is high. The company establishes a local sales force that puts in place an aggressive programme to market and sell to a wide spectrum of commercial, academic and government customers.

The sales force promptly engages the market with a series of meetings, events and demonstrations. They hire key staff with relationships with strategic buyers and influencers. They establish a distribution network after consulting with customers about their needs and expectations relative to logistical operations. In short, they enter the market and set about achieving your goals in an organised, insightful, energetic manner.

This straightforward act of business building will nonetheless expose many of your business processes to broad challenges.

The challenges will range from relatively mundane issues in your ***disbursements process*** (Do you have adequate records of who attended meetings, dinners, demonstrations and events? Did government officials participate? Were the value of the meals or any gifts exchanged within the bounds of corporate policy and local law?), to more complex issues concerning the business practices of your newly appointed distributors—and whether or not your ***due diligence process*** was adequate to identify potential issues, including whether or not you are dealing with government officials.

Meanwhile, your ***HR processes*** are challenged by the hiring of local staff with good connections in the marketplace—which may include relatives working as government officials at customer agencies. Your ***customs agent,*** conscious of the expectations that both you and your customers have placed on him for timely clearances, is entertaining local port officials on a regular basis. Your technical team has hired consultants recommended by the government and employed retired agency officials to assist with the approval and ***licensing processes*** for your products—again, challenging your ***due diligence process for vendor selection and your payment controls.***

Your ***sales*** people are actively competing for business and are offering a few extra percentage points of discount to your distributors to win certain orders. Your ***law firm*** has placed a network of local labour attorneys on monthly retainer to deal with ***labour force*** issues. Finally, your tax team is engaged in a series of discussions with local tax authorities over the classification of your imports for ***customs duties,*** as well as your ***transfer pricing*** structure as it affects the profitability of your local subsidiary.

*The reason we identify economic crimes as threatening your business processes is that none of the activities in the example above are per se improper or inappropriate. Still, each has the potential to challenge the integrity of your employees and pressure them as they struggle to manage the tensions of achieving your financial goals while operating in compliance with policy and regulation—in a local political and business culture characterised by a high demand for corrupt payments.*

## The damage

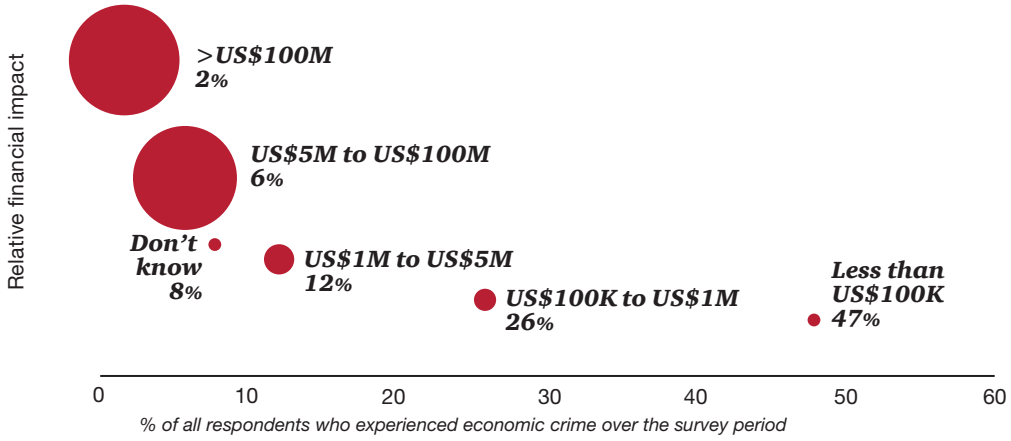
Organisations often don't grasp the true financial impact of an economic crime until after it has happened—sometimes well after. As in previous years, our survey underscores that the cost of fraud—both in financial and non-financial terms—is significant.

### *The financial damage: Rising stakes*

As Figure 6 indicates, nearly one in five (18%) organisations suffering fraud experienced a financial impact of between US$1 million and US$100 million. And the percentage of respondents reporting losses in excess of US$100 million doubled, from one to two per cent.

While the more-than-US$100 million category is comparatively small, representing 30 organisations, the fact that twice as many respondents reported a loss of this size, relative to our last survey, may be a significant marker of the major negative impacts of systemic frauds. These large losses may be connected to the reported increase in incidents of bribery and corruption—frauds which can be especially costly to organisations, with regulatory fines, legal fees and remedial expenses potentially reaching billions of US dollars.

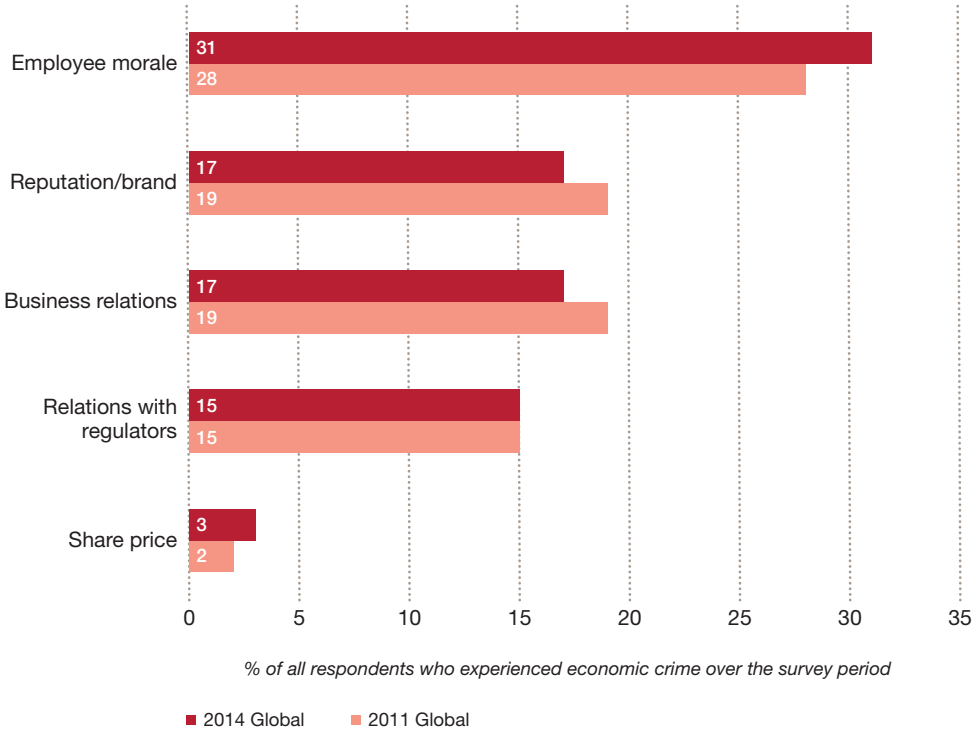
**Figure 6: Relative financial impact of economic crime on organisations**



### *Collateral damage: Hard to quantify, hard to ignore*

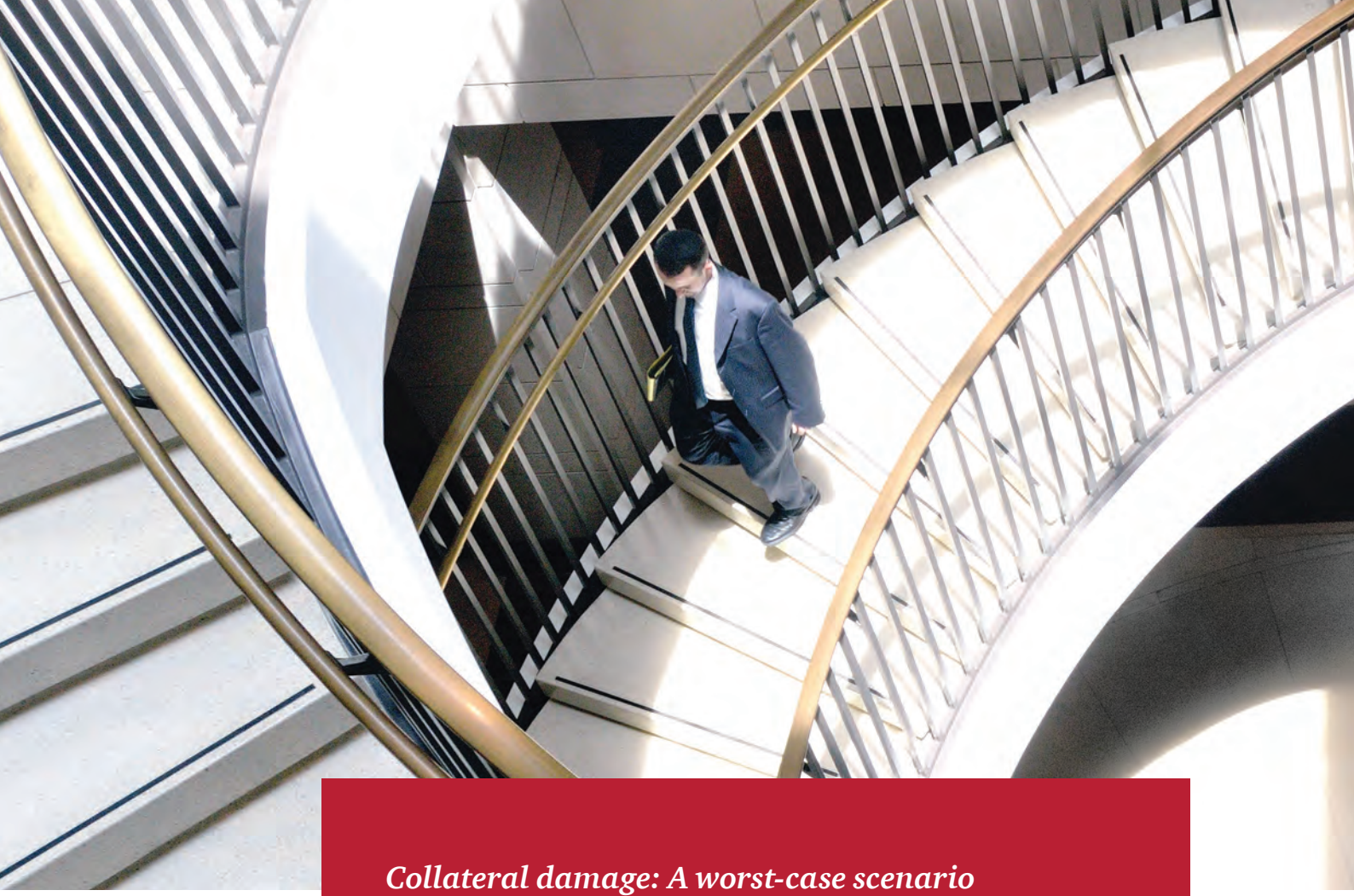
Economic loss is not the only concern that companies face when combating fraud. Our respondents pointed at damage to employee morale, corporate and brand reputation, and business relations as some of the most severe non-financial impacts of economic crime.

**Figure 7: Collateral effects of economic crime**




When taking into account the secondary damage, the true cost of an incidence of economic crime can be long lasting. Consider the long chain of adverse events that can follow a single, high-profile incident of economic crime: lost revenues, as customers look for other business partners; delayed entry to new markets due to regulatory issues; a battered stock price; and declining productivity and morale.

Fortunately, top management appear to understand the importance of collateral impacts: our 2014 Global CEO Survey reports that half of chief executives (a sharp increase from 37% just a year ago) see a "lack of trust in business" as a key marketplace issue, with significant majorities recognising that business has a wider role to play in society than just building shareholder value.



## *Collateral damage: A worst-case scenario*

We have witnessed cases where a single incident led to a situation where an entire business disintegrated.

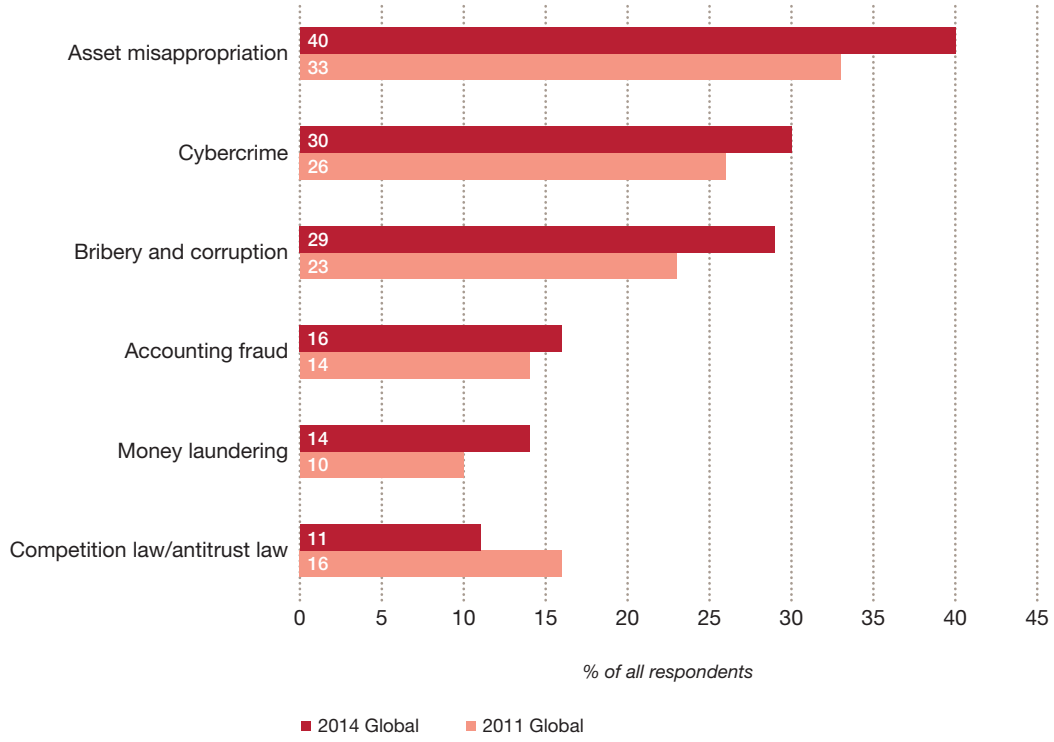
Starting with a report of a single event such as insider trading or financial statement fraud, incidents may appear compartmentalised, involving only one account, division, or customer. Still, in a competitive marketplace, there are often few reasons for customers, counterparties or partners to maintain a relationship with a tainted entity. In addition, potential government enforcement actions give rise to uncertainty concerning the company's future operational condition. Customers, capital, employees, and partners disassociate themselves from the organisation. Caught in a storm of uncertainty about its future, the organisation implodes.

## Looking ahead

In addition to looking at economic crimes suffered in the past, we asked our respondents to look forward and tell us which economic crimes they believe pose the highest risks to their companies in the coming years. In virtually every category, respondents said they expect their organisations will experience more fraud in the coming periods.

Figure 8 shows their predictions for key crimes in 2014, along with comparable responses from 2011.

**Figure 8: Trends in expectations of economic crime**




The results appear to reflect the megatrends of global expansion into less-developed markets, and the expectation of increasing incidents of cybercrime as more technology is deployed in all areas of business.

We do note that expectations of future competition law/antitrust law issues fell approximately 5%. Later in the survey we explore how this crime appears to be receding in the minds of many—except for those in Europe, where an active European Commission and recent press may be driving perceptions.

*Some types of economic crimes attract significantly more attention from government enforcement agencies than others.*

# Under the eye of enforcement

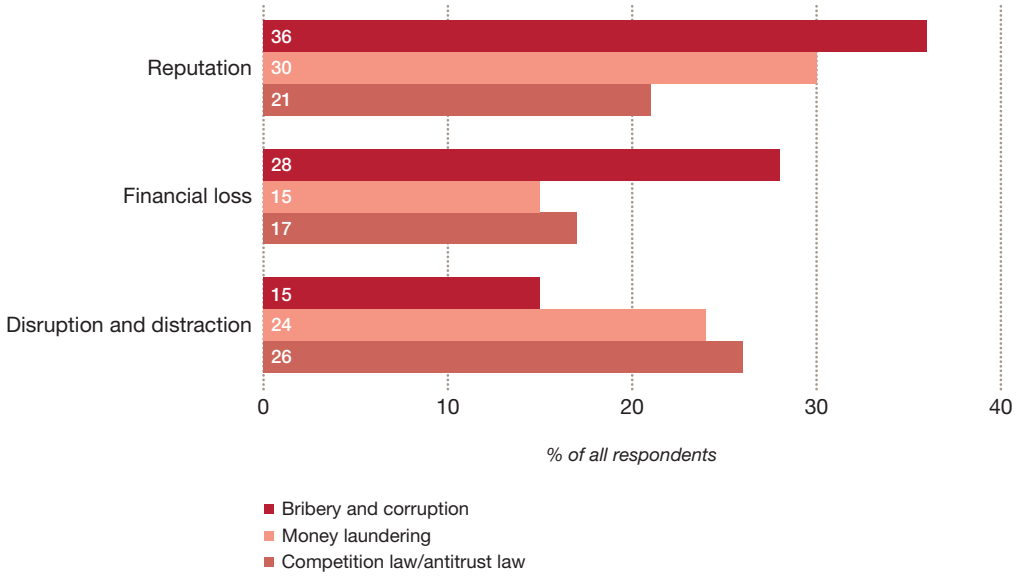
Some types of economic crimes attract significantly more attention from government enforcement agencies than others. For this reason we have decided to dedicate a section of our analysis to an important subset of economic crime—bribery and corruption, money laundering, and anticompetitive behaviour.

All three of these crimes arise from the failure of businesses to adhere to the expected code of business conduct established by countries around the world. And several countries, among them the US and the UK, are committed to enforcement programmes with increasingly stringent standards and stiff penalties.

In an interconnected world, these categories of economic crime pose unique threats to global organisations. In addition to triggering fines and even criminal indictments, such violations can be seen as part of a larger organisational problem (be it a failure of internal controls, processes, or lack of appropriate culture or tone at the top). They can also create a great deal of damaging fallout—from reputational harm (including viral negative attention in social media, unwanted publicity in traditional media, litigation or adverse stock market reaction) to financial losses, costly disruptions to business plans, and loss of critical talent.

Our findings seem to bear this out. Across these three areas of economic crime, which are frequent targets of regulatory scrutiny, respondents cited reputational risk as well as disruption and distraction as having the greatest impact.

**Figure 9: Perceived most severe impact, by highlighted economic crime**

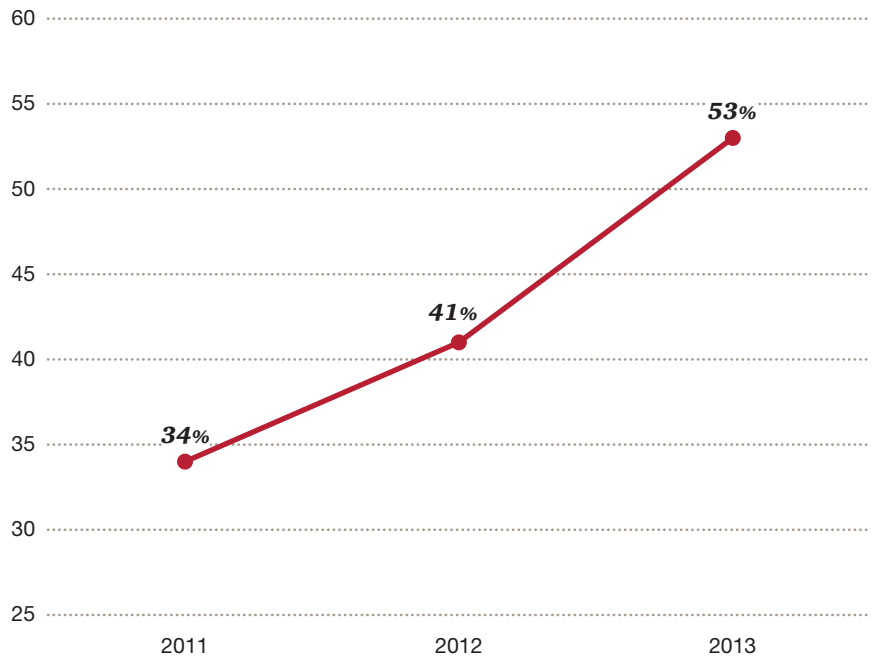


# Bribery and corruption: The C-Suite gets the message

While it is not the most common form of crime reported, of all the types of fraud covered in our survey, bribery and corruption may pose the greatest threat to global businesses because of the number of business processes it threatens. Sales, marketing, distribution, payments, international expansion, expense reimbursement, tax compliance, and facilities operations are all vulnerable processes.

Every region reported a significant number of incidences of bribery and corruption. Twenty-seven per cent of all respondents who reported economic crime experienced corruption during the survey period, making it the third-highest crime specified and a relative increase of 13% from the 24% reported in 2011.

**Figure 10: Rising CEO concern regarding bribery and corruption**




*% of all respondents in PwC's Annual Global CEO Survey*

When an economic crime threatens a company in so many ways, it deserves CEO attention—which could explain the sharp increase in CEO focus on the risks of corruption and bribery in this year's CEO Survey.

**27%**

of all respondents who reported economic crime experienced corruption during the survey period.

## *Sales and marketing under threat*

While the risk of bribery and corruption is a threat to many different types of transactions, it is of particular concern when companies are dealing with government agencies and state-owned businesses—and, consequently, with government officials.

For example: A pharmaceutical organisation would like to sell a recently developed medicine to a country that operates a public healthcare programme. The permission to sell the medicine, the decision to buy it and the price paid will likely be in the hands of government officials.

Or, an equipment company would like to sell their product to a state-owned enterprise whose senior executives are members of the political party currently in office. The specifications in the tender documents, the budget available for the acquisition, the ancillary support services needed for training, spare parts, and maintenance, the evaluation of the bid proposals—all will likely be decided by government officials.

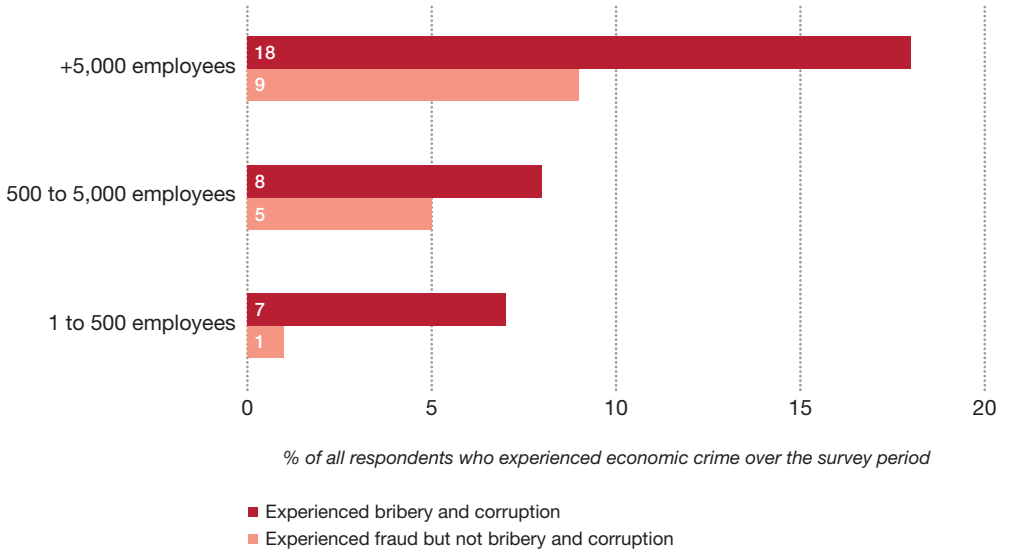
If the territory has a culture that is relatively permissive to bribery and corruption, some of these officials may be predisposed to expect or at least be open to bribes. This exerts pressure on sales and marketing staff, who have been tasked by leadership with bringing a new product to a growing market—pressure which could be felt by individual staff as justifying offering a bribe or kickbacks, or otherwise rigging the sales process to try and secure a better price.

While the profit potential will likely be obvious to the sales and marketing team, the systemic risk of operating in a culture with a "high demand" component of the corruption equation may be less so. As we have often seen, FCPA and other enforcement actions frequently have far-reaching financial and organisational impacts. These can include altering your sales processes, sales incentives, distribution networks, authority levels and approval requirements for marketing activities and other payments, choice of agents and brokers, and in extreme cases, the ability to operate at all in certain countries.

However, while CEOs may be communicating rising concern, the corresponding strengthening of business processes remains a work in progress in many organisations.

The financial costs and collateral damage caused by incidences of bribery and corruption—especially in light of the penalties imposed by governments through increasingly aggressive anticorruption enforcement—can be significant. As Figure 11 illustrates, regardless of their size, companies that experienced incidences of bribery and corruption more frequently reported losses of over US$5 million.

**Figure 11: Losses over US$5M considering bribery and corruption, by company size**




## From the developed to the developing

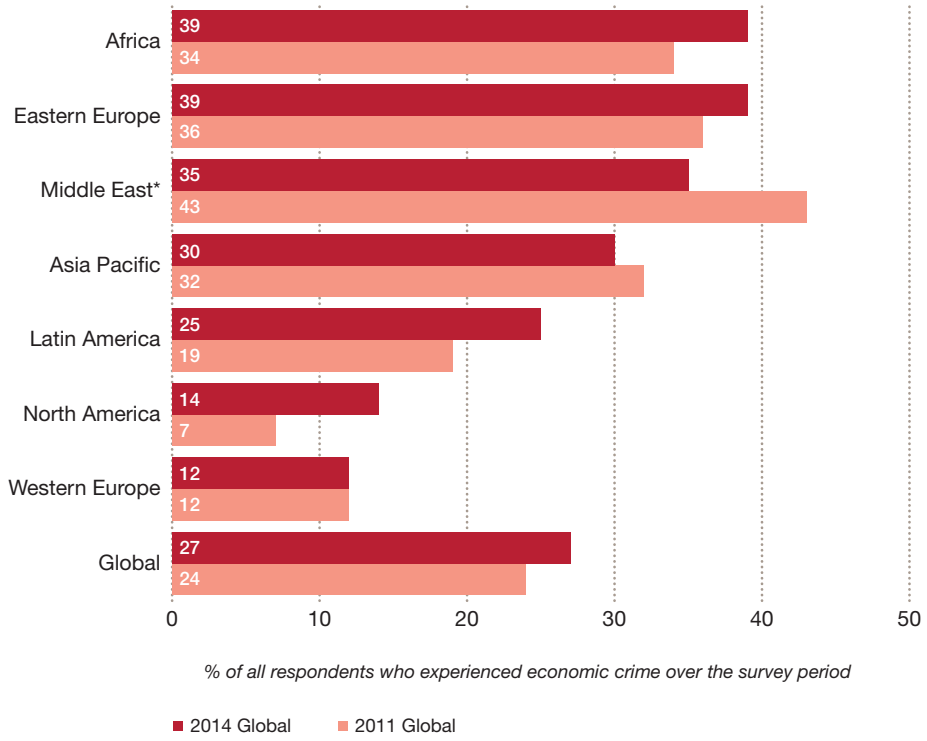
The global economy is generally on the rebound, potentially reinvigorating organisations' appetite for expansion and risk. Our survey results confirm that a large number of organisations operate in territories identified as posing a high corruption risk (50%) and/or plan to pursue opportunities in such areas in the next two years (8%).[1] The data underscores that countries within these regions are experiencing a relatively higher share of incidences of bribery and corruption (36%) vs. the global average (27%).

We believe that one driver of the high reported figures of bribery and corruption may be the megatrend of the shift in wealth from the developed economies of the West to the emerging high-growth economies of the South and East—many of which may have different cultural attitudes toward fraud and corruption, fewer regulations, and less-consistent enforcement of those regulations. These conditions naturally create a higher risk profile for this type of economic crime.

As shown in Figure 12, Africa and Eastern Europe reported the highest overall percentage of bribery and corruption (39%), with the Middle East (35%) also registering above the global average. Notably, the Middle East and Africa have significant resource extraction and infrastructure/construction-based economies, which are traditionally industries with significant fraud and corruption risks.

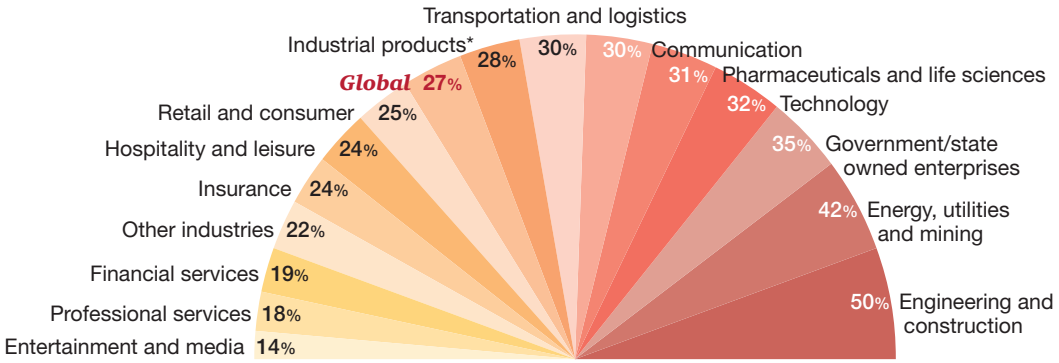
1. Respondents were asked if their organisation had operations or was pursuing operations in high risk areas, with a reference to the 2012 Transparency International Corruption Perception Index ("CPI"). The CPI is compiled annually by Transparency International, a non-profit organisation which tracks a number of corruption indexes.

## Figure 12: Reported bribery and corruption, by region




*Middle East was included in the "Asia Pacific" region in 2011

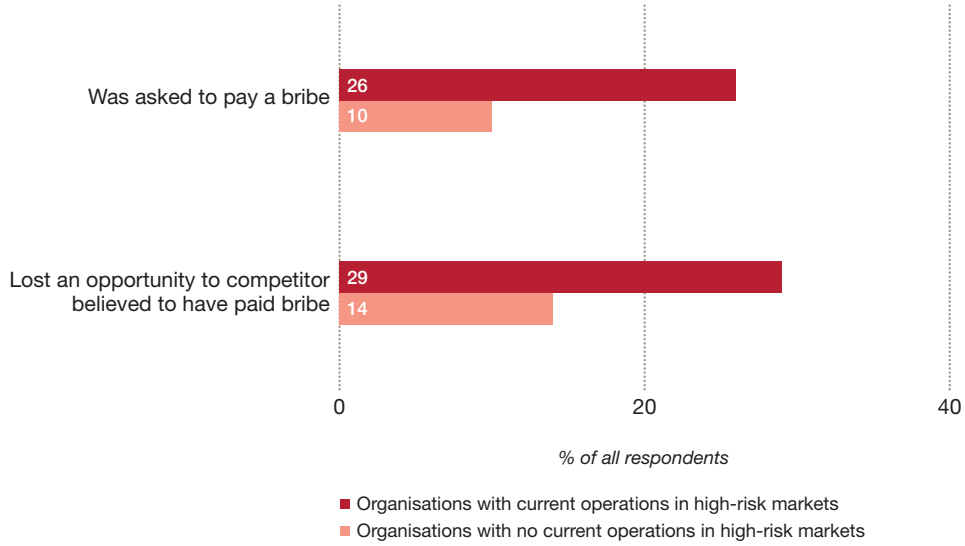
## Figure 13: Reported bribery and corruption, by industry




According to the 2012 Corruption Perception Index ("CPI"), North America is perceived as having less corruption than many other parts of the world. However, this region saw a doubling in percentage of bribery and corruption incidences reported between 2011 and 2014. We believe this reflects more recent expansion into high-risk areas by North American respondents, as 48% stated their organisation pursued an opportunity in a market with a high level of corruption risk during the survey period—second only to respondents in Africa, with 50%.

The results shown below bear this out. There is a notably higher likelihood that an organisation operating in a high-risk market was asked to pay a bribe and/or felt they lost an opportunity to a competitor who did so, compared to those who did not operate in high-risk areas. When the competition is believed to be playing unfairly, the pressure on an organisation to follow suit can intensify.

**Figure 14: Bribery and lost opportunities**




Since bribery and corruption is often prosecuted by regulators across borders, organisations should be mindful of the significant risks involved with operating in these high-growth areas, even if local practices and customs are less rigorous. So while North America and Western Europe are actually low on the scale of regions reporting bribery and corruption (see Figure 12), their government enforcement practices have a deep influence in this area.

## *The endemic challenge*

It is easy for those who have lived in relatively corruption-free societies to underestimate the significance and power of cultural norms related to the "demand side" of corruption. It is likely that when your employees are challenged with sales and other business goals within "high corruption demand" cultures, they may not perceive the risk of participating in a corrupt scheme with the expected, and required, degree of caution.

Accordingly, they are likely to find a wide variety of means and rationalisations for following the local customs, as opposed to abiding by corporate policies.

This continuing contest between corporate expectations and local cultural norms is not as easy to win as many expect. It is this dynamic that threatens your sales and marketing processes by pressuring personnel into improper contracts, adds unnecessary layers in the distribution channel, allows "quid pro quo" transactions like hiring relatives of customer executives, creating marketing or advisory roles for customer employees, or increasing the discount to a distributor or travel agent to create a "slush" fund.

Overcoming the power of local cultural expectations requires a strong and consistent message to all employees to achieve the right balance between your employees' life experience and work experience.

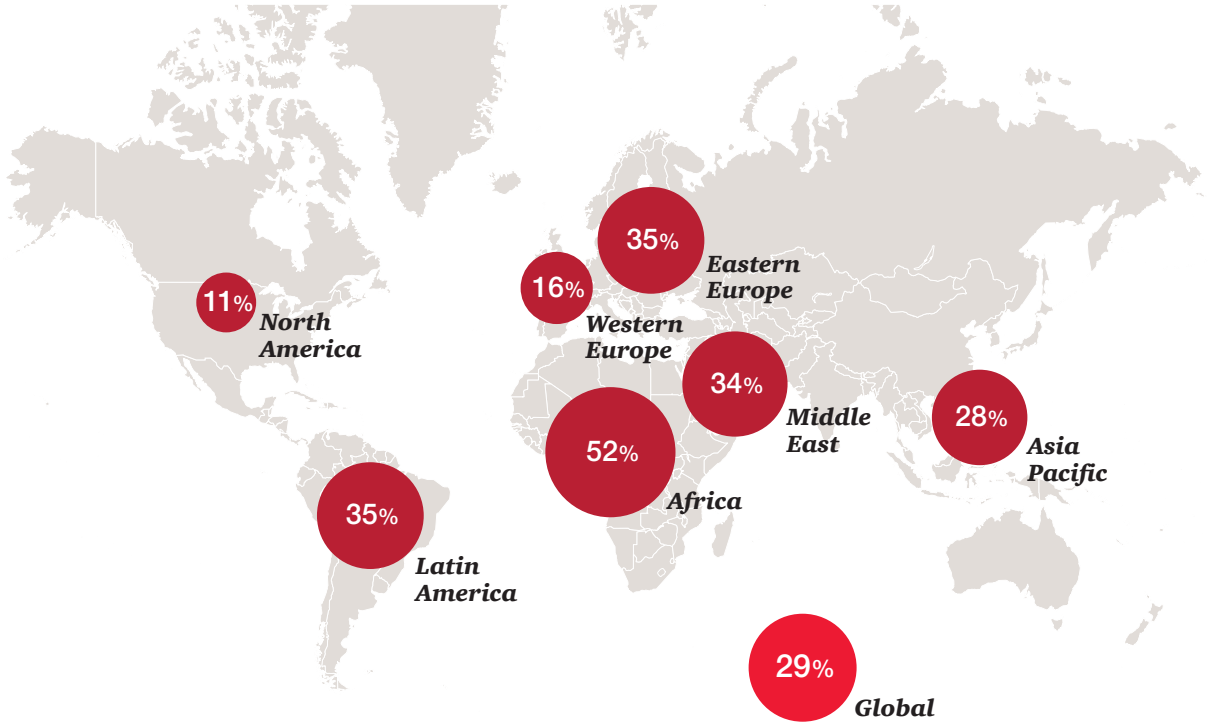
## Today's perceptions, tomorrow's predictions

The threat of bribery and corruption appears to be rising more quickly in the perception of our respondents than most categories of economic crime surveyed. Three in ten viewed their organisations as likely to fall victim to bribery and corruption—a significantly higher number (29% versus 23%) than in 2011, and one essentially equating this category with cybercrime as the second-most likely type of fraud organisations believe they will face.

Not only is the rate of the perceived threat of bribery and corruption accelerating, it is also well distributed across all industrial sectors, with a low of 21% in entertainment and media and a high of 37% in energy, utilities and mining.

At the regional level, our respondents noted diverse expectations, as illustrated by Figure 15. Globally, future expectations generally align with actual experience. However, Africa and Latin America perceived more future risk (52% and 35% respectively) than what respondents reported in the present (39% and 25%).

**Figure 15: Perception of future bribery and corruption, by region**



# Money laundering: A special concern for financial firms

Financial services industry respondents report that their number-one concern about economic crime is entirely different than most other industry sectors: money laundering—defined as actions intended to legitimise the proceeds of crime by disguising their true origin.

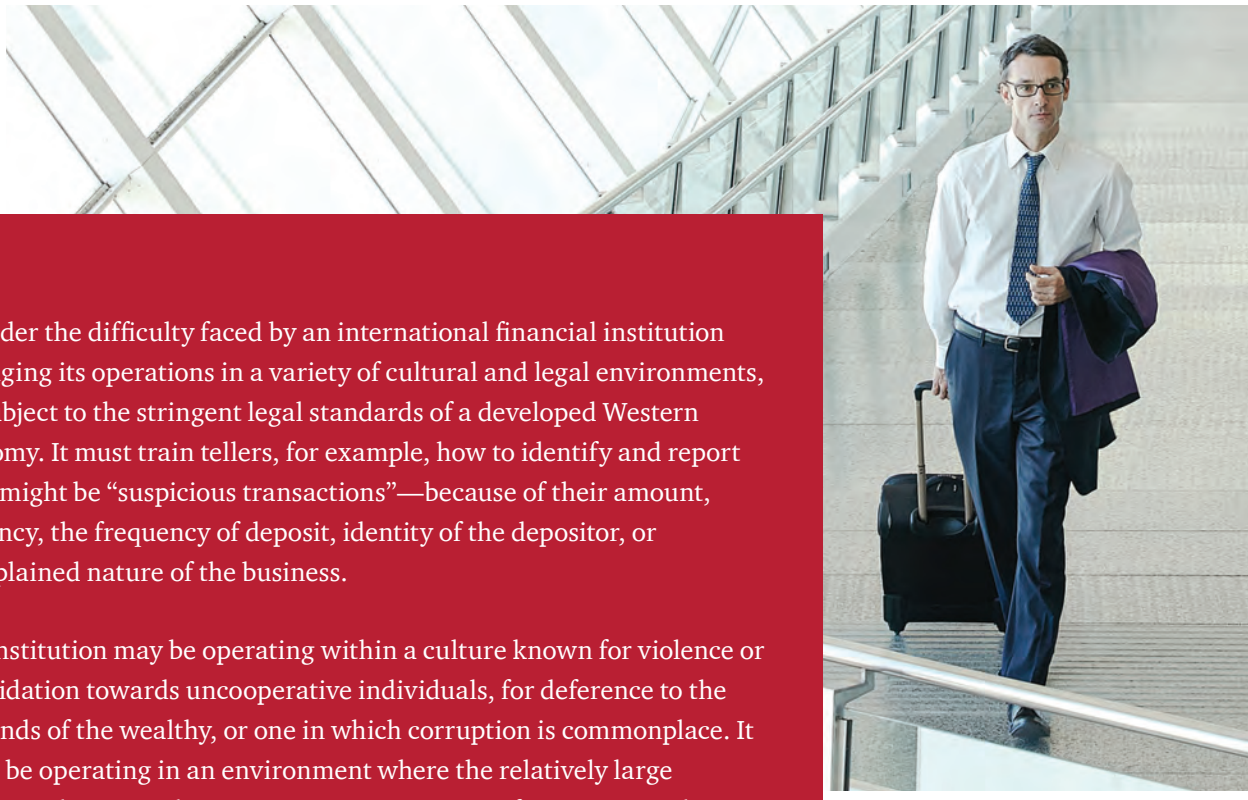
Money laundering represents a risk if a financial institution fails to report it. If the organisation is diligent in its compliance efforts to review customer transactions in accordance with the law, they are not likely to be punished by regulators, even if some incidents do occur.

Over one quarter (27%) of respondents in the financial sector reported experiencing money laundering during the survey period, a response rate more than double that of the next closest industry sector, insurance (11%). In addition, financial services respondents perceive far more risk from money laundering than either corruption and bribery or competition law, with 58% reporting this as their biggest concern among the three.

While money laundering schemes vary in their sophistication and complexity, in every scheme they require access to the facilities and services of a financial institution. In this, the threats they pose share a common, very real aspect: money laundering is facilitated by human weakness—whether benignly by inattention or incompetence, or maliciously by corruption and intent. The challenge of such systemic threats is that they can't be completely avoided—at least not without irrational steps like withdrawing from the market in question—so business processes must operate in the face of such threats.

The crime of money laundering threatens the business processes of financial institutions in several ways:

- ***Know your customer (KYC).*** The process of marketing to potential customers, as well as integrating new customers, is directly affected by the threat of money laundering.
- ***Compliance.*** Equally significant, money laundering threatens the institution's processes for maintaining compliant operations—at the teller's window, in the money transfer room, and in its check processing and settlement process.
- ***Risk management.*** Money laundering also threatens an institution's due diligence, suspicious transaction reporting and risk management—especially when risk is concentrated in a commonly controlled group of accounts or loans used by money launderers, or when systems monitoring capabilities fall behind the service platforms in use.



Consider the difficulty faced by an international financial institution managing its operations in a variety of cultural and legal environments, yet subject to the stringent legal standards of a developed Western economy. It must train tellers, for example, how to identify and report what might be "suspicious transactions"—because of their amount, currency, the frequency of deposit, identity of the depositor, or unexplained nature of the business.

The institution may be operating within a culture known for violence or intimidation towards uncooperative individuals, for deference to the demands of the wealthy, or one in which corruption is commonplace. It could be operating in an environment where the relatively large difference between the economic circumstances of customers, relative to bank employees, allows for gifts or threats to pave the way for inappropriate use of its facilities by those charged with conducting transactions, approving transactions or reporting issues.

Money laundering presents collateral threats as well. In addition to enforcement settlements, this crime can bring reputational damage, negative publicity and adverse relationships with regulators. Additional burdens include the cost of compliance, surveillance, and other business process upgrades.

Recently, a new form of money laundering threat has developed: alternative payment networks using "virtual" currencies. While the transactions on these sites may be "virtual," they are backed by actual deposits in financial institutions around the world. Identifying such tainted funds is yet another challenge to bank compliance and operating systems.

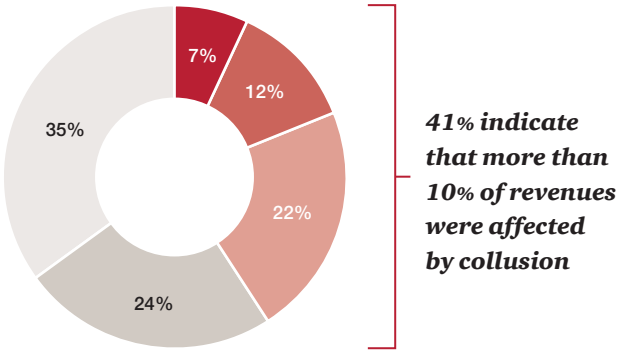
So operating in environments that pose a systemic threat of money laundering to the business processes of financial institutions is a unique challenge. Not only are money laundering schemes numerous and sophisticated, but they create a potentially significant tension between the equally laudable goals of acquiring and serving profitable customers and operating a wholly compliant institution across multiple jurisdictions.

# Competition law/ Antitrust law

In the competition law/antitrust law sector, our survey data reflects a European focus. Of the three economic crimes under the eye of government enforcement mechanisms we have highlighted (bribery and corruption, competition law, and money laundering), competition law was cited as a higher risk by one in four respondents in both Western Europe and Eastern Europe—with Asia Pacific, Africa, and both American continents showing less concern.

It appears that the EU Commission, which has been increasingly aggressive in pursuing high-profile actions against cartel, price-fixing and other forms of market abuse—including in the recent, highly publicised LIBOR affair (see callout on following page)—is having a definitive impact on the concerns and operations of EU-based companies.

**Figure 16: Organisations affected by collusion**




Results of 2013 survey on economic crime conducted by PwC Germany
*Reported % of revenues affected by collusion*

Over 30% 20-29% 10-19% 5-9% Below 5%

We found more evidence of this in PwC Germany's recently launched study on economic crime. Approximately four out of ten (41%) respondents estimated that more than 10% of their revenues were affected by market distortions (defined as the collusion of two or more businesses).[2]

Another takeaway from the German survey is that while seven in ten organisations (71%) overall had not implemented an antitrust compliance programme, those who already had in place an anticorruption programme were more likely to expand their compliance activities to include antitrust measures (47%). Only 9% of organisations without anticorruption programmes had addressed competition law issues.

Unfortunately, the German survey also suggests that the two programmes have similar weaknesses. For example, approximately one quarter of German antitrust compliance programmes did not include employee training. Nearly a third did not include a systematic risk analysis of business partners or markets and industries, which are common to antitrust compliance programmes. There was also room for improvement with internal audits (71%) and whistle-blower systems (67%), two other important elements for the detection of antitrust violations.

2. The PwC Germany survey sampled 603 organisations based in Germany on their experience over the last two years.

*Four out of ten German organisations reported that more than 10% of revenues were impacted by collusion.*

While these results were specific to Germany, we believe they shine a light on conditions within the European continent as a whole. And while this risk resonated primarily with European respondents, the actions of the EU Commission affect entities on a *global* scale.

## *LIBOR scandal*

Competition law violations reached the headlines during our 2014 survey in the form of wide-spread allegations of collusion among banks in reporting LIBOR, the benchmark London Interbank Offered Rate.

European Commission officials became the latest global regulators to take action against multiple global financial institutions after the discovery of widespread rigging of LIBOR—an internationally utilised interest rate benchmark underpinning rates paid for securities, loans and other financial contracts worth hundreds of billions of US dollars.

A 2012 international investigation revealed that employees of multiple banks had participated in a scheme to manipulate LIBOR by submitting false rates in an effort to influence the publicly reported rate. These artificial distortions allowed traders to then generate additional profits based on their positions—and presumably greater bonus packages. In addition, financial institutions may have attempted to manipulate the markets' impression of their safety and soundness by submitting artificially low LIBOR rates.

As of January 2014, regulators in the US, UK and EU had fined a group of banks more than US$8 billion for rate-rigging, and regulators in Switzerland, Canada, and Japan were continuing their investigations. Interestingly, unlike the national regulators, the European Commission's investigation was centred not on fraud but on the antitrust violation of illegal cartels.

What business processes were attacked? At banks—where employees were for many years able to circumvent rules and collude with counterparts who were supposed to be competitors—the events have uncovered significant vulnerabilities in compliance, risk management and internal controls. On a larger scale, the primary treasury and capital function at organisations around the globe were impacted.

Many observers see the LIBOR case as pointing to a more aggressive future stance by European antitrust authorities in investigating alleged anticompetitive behaviours in any industry.

# The eye of enforcement: Future expectations

Finally, we asked our respondents to rank the three systemic economic crimes we have highlighted here—bribery and corruption, money laundering and competition law/antitrust law—in the order of perceived risk, going forward.

More than half of respondents (53%) listed bribery and corruption as the highest risk in doing business worldwide, followed by money laundering (22%) and competition law/antitrust law (21%).

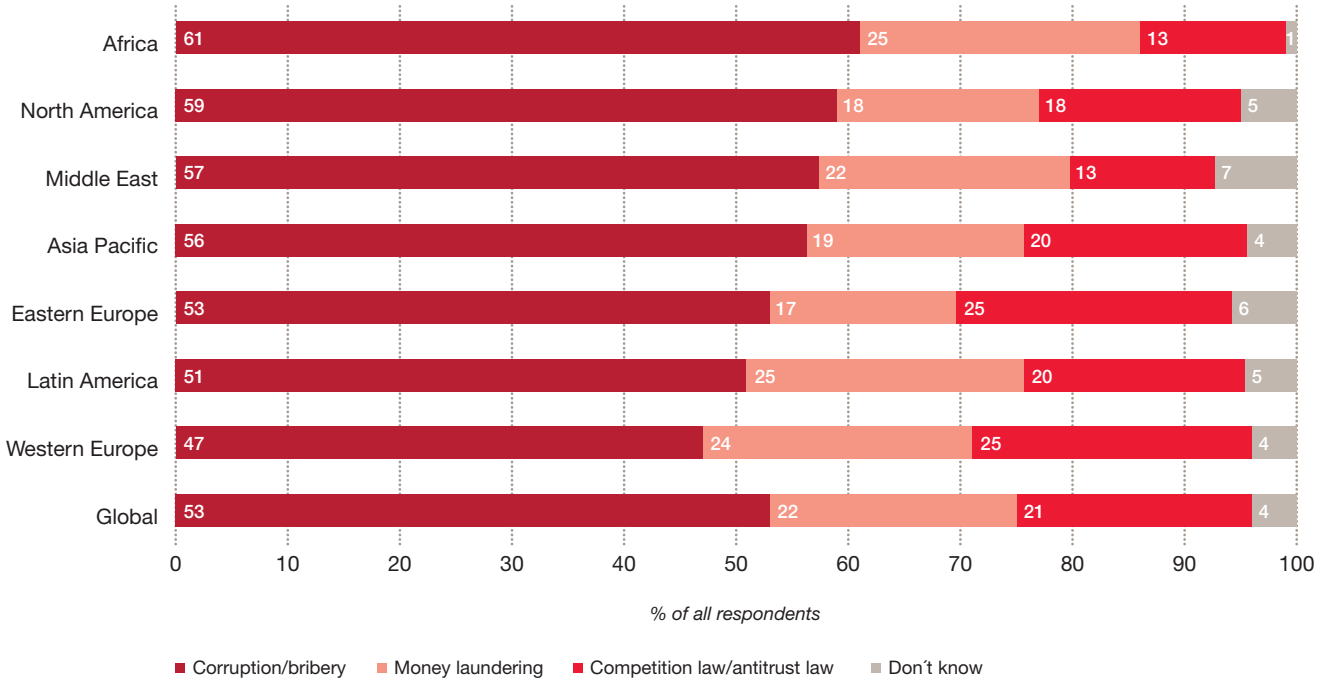
**Figure 17: Perceived greatest relative economic crime risk**


*% of all respondents*

As displayed in Figure 18, every region reported bribery and corruption as posing the greatest relative risk to the organisation across these three categories.

North America's position in second place (59%), between Africa (61%) and the Middle East (57%), likely reflects American respondents' wariness of the high cost of violating the FCPA and other anticorruption statutes.

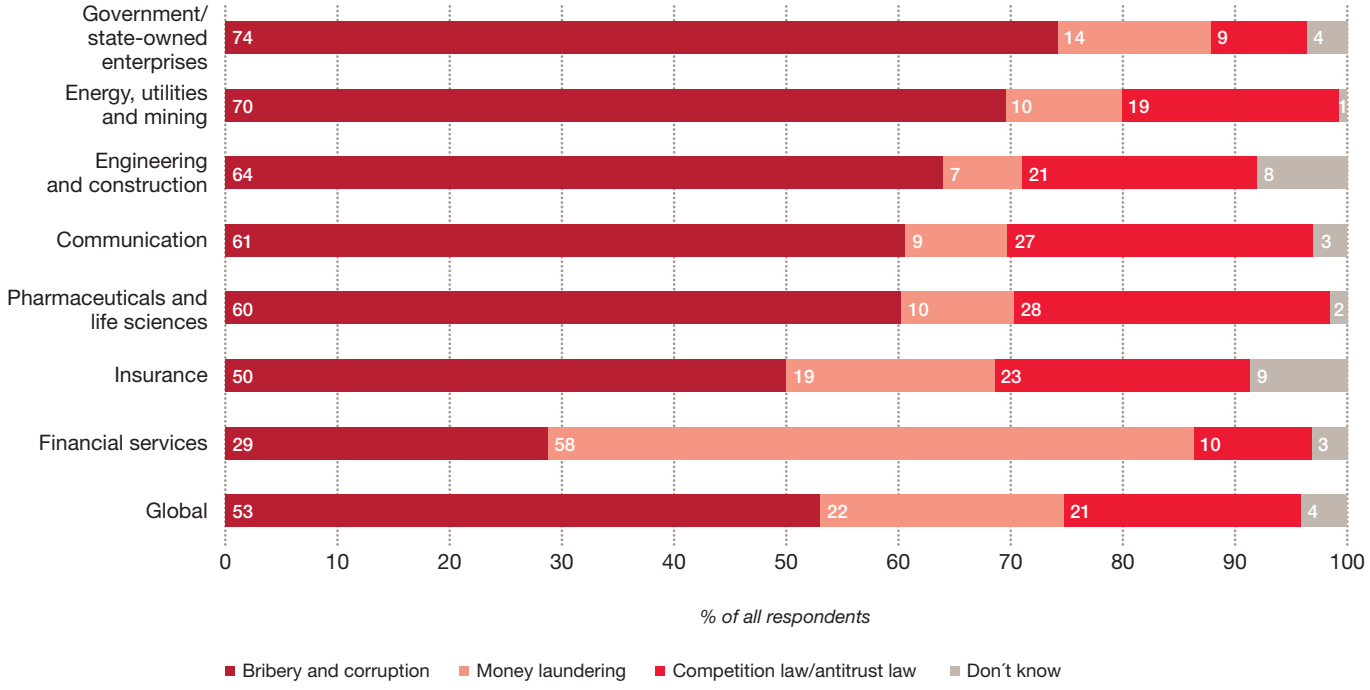
**Figure 18: Perceived greatest relative economic crime risk, by region**



Across all industries, corruption/bribery also ranked as the greatest of these three risks in doing business globally—with the exception of financial services (29%), where, as we have noted, respondents perceive a greater risk from money laundering.

Compared to other industries, government/state-owned enterprises (74%) saw the highest future risk from corruption/bribery, followed by energy, utilities and mining (70%), and engineering and construction (64%). Apart from these heavy industries, the pharmaceuticals and life sciences sector (60%) is also considered high risk, as borne out by recent enforcement actions in Asia.

**Figure 19: Perceived greatest relative economic crime risk, by industry**



*Connectivity and access also have a dark side—one which empowers motivated, sophisticated criminals who are able to operate below the radar.*

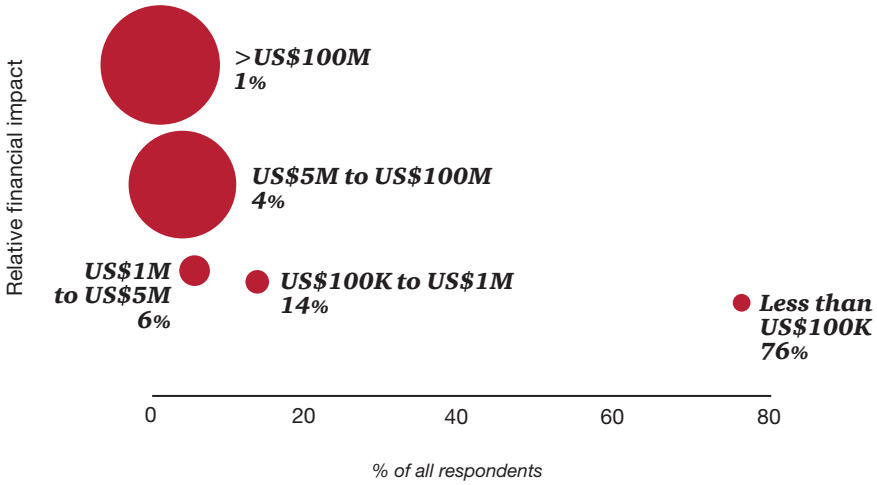
# ***Cybercrime:***
# The risks of a networked world

The advancement of technology in business services, combined with the explosive growth in social media and data connectivity, has permanently altered—and in many ways, brought together—the business and consumer landscapes.

Unfortunately, connectivity and access also have a dark side—one which empowers motivated, sophisticated criminals who are able to operate below the radar. And because cybercrime operates largely unseen, organisations may never even realise they are being targeted until long after the damage is done.

This fact alone makes the many varieties of electronic fraud one of the most threatening types of economic crime.

**Figure 20: Relative financial impact of cybercrime on organisations**

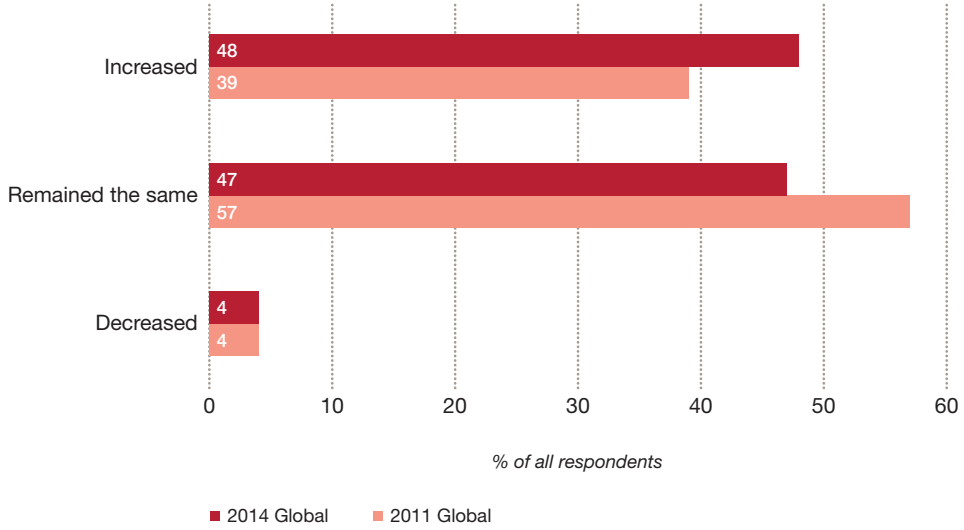


Our 2011 Global Economic Crime Survey was the first in our series to highlight cybercrime as a high-level threat to organisations. This year's survey confirms the significant, continuing impact of this crime on business, with now one in four of respondents reporting they have experienced a cybercrime—and over 11% of these suffering financial losses of more than US$1 million.

In a sign that organisations are taking this threat more seriously, our survey indicates that the perception of the risk of cybercrime is increasing at a faster pace than that of reported actual occurrences. This year, 48% of our respondents said their perception of cybercrime risk at their organisation increased, up from 39% in 2011.

Reinforcing this, an identical percentage (48%) of CEOs in our latest Global CEO Survey said they were concerned about cyber-threats, including lack of data security.

**Figure 21: Perception of the risk of cybercrime**




## Cybercrime: What you don't know can hurt you

While one quarter of respondents reporting they have suffered a cybercrime is concerning enough, we must also consider that a significant percentage of those who did not report cybercrime may also have suffered an event—and not even known about it.

This underscores the challenge of the threat. Many entities do not have clear insight into whether their networks and the data contained therein have been breached, and they don't know what has been lost—or its value.

Further complicating the picture is a third aspect of the lack of transparency into cybercrime events: even when it is detected, cybercrime often goes unreported. Outside of privacy breaches in regulated areas such as identity theft, there are few regulatory conventions requiring disclosure. And often—such as in the case of theft of key intellectual property—there may be compelling competitive reasons for organisations to keep such losses confidential.

For example, if a confidential bid planning document were accessed by cybercriminals and utilised by rivals to gain an advantage, would a company disclose the incident? Are organisations adequately defending against such cybercrime breaches, and if they were discovered, how would they value the loss?

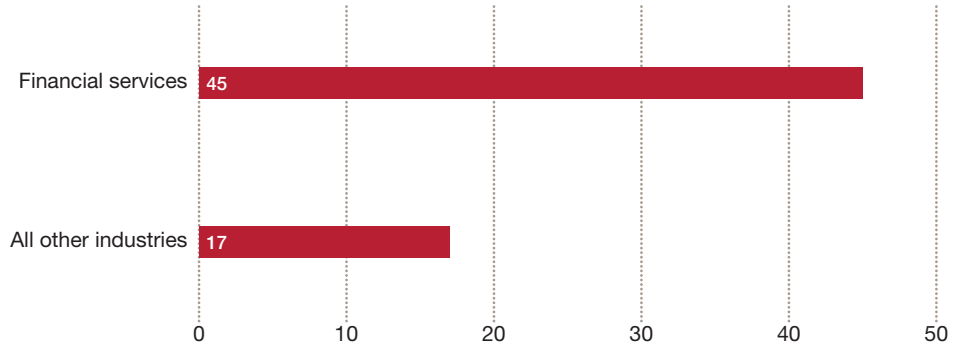
The bottom line is that much of the damage caused by these kinds of attacks is not disclosed, either because it is not known, because it is difficult to quantify, or because it is not shared. Naturally, this poses risks in a global business ecosystem that is increasingly reliant on both technology and intellectual property—and that values transparency.

An environment where it may be easier to steal a vital intangible asset than it is to value, disclose, or even realise its loss is an inherently risky one.

## Focus on financial services

Forty-five per cent of financial services organisations affected by fraud reported being victims of cybercrime—nearly three times the frequency as reported by all other industry sectors.

**Figure 22: Cybercrime and financial services**




*% of all respondents who experienced cybercrime over the survey period*

Why such a large percentage? Large, regulated financial institutions often have more and better system safeguards—which may increase the chance of a breach's being detected. In addition, banks are where the money is!

Finally, financial institutions are an appealing target because they provide large amounts of customer and personal financial information online, which can potentially be accessed—and sold on the black market—as a precursor to organising a theft of funds.

## *Data confidentiality under threat*

The data collection and storage process handles private information, providing cybercriminals with opportunities to steal data which can be used for multiple purposes, including accessing financial accounts and extracting cash.

Well-known hacking groups in Eastern Europe have targeted the systems underlying payment card infrastructure—the systems that facilitate payment card transactions between consumers, merchants and banks. When they gain access to these systems, they can map out business processes and products (such as pre-paid cards), download account and personal identification numbers (PINs), control account information such as withdrawal amounts, and use the stolen account number and PINs to clone onto blank cards and withdraw cash.

*A typical scenario:*
A hacker group targets a company that provides payment card system infrastructure to banks and payment card brands. The hacking group exploits a known vulnerability in a Web-facing corporate system, which gives them a foothold into the company network. Using this foothold, the hackers steal company user credentials, install malicious software (malware), and begin mapping out the network, to identify security systems and links to business processes.

The hackers then put a different group of experts on the case, to explore business processes and product lines—e.g., pre-paid cards, credit cards, and debit cards. They identify a production system that contains the account numbers for a pre-paid card product line with associated fraud controls. They then disable the fraud controls, download the account numbers and associated PINs, and adjust the "purse" settings on the products to allow high withdrawals against the accounts, which are underwritten at several different banks.

Finally, the hackers use easily available equipment to embed the account information onto blank cards with magnetic strips. These cards are then used to conduct thousands of transactions across 1,700 ATMs worldwide in a 36-hour period, resulting in a net cash theft of millions of US dollars. A year later, the same hacker group, using the same technique but with improved ability to coordinate "mules"—the individuals who actually withdraw the cash—withdraw tens of millions in only 12 hours.

## A moving target

In a changing technological landscape, the sophisticated adversary takes advantage by attacking new weaknesses. This is why it is essential for organisations to at least try to keep pace with the criminals who threaten them.

Even when organisations are generally aware of the types of cyber-threats they face, many do not truly understand the capabilities of cybercriminals, what they might target, and what the value of those targets might be. Yet companies continue to make their critical data available to management, employees, vendors, and clients on a multitude of platforms—including high-risk platforms such as mobile devices and the cloud—because the economic and competitive benefits appear so compelling.

While nobody expects the benefits of technology to diminish, or for organisations to shrink their digital footprint, it's clear that—with more data accessible on more platforms—valuable data will remain under attack, and that the cost of security breaches will continue to be steep. In fact, in every region, between a quarter and a third of organisations told us they believe they will likely encounter cybercrime in the near future.

## Cybercrime is a strategic problem

Ultimately, cybercrime is not strictly speaking a technology problem. It is a strategy problem, a human problem and a process problem.

After all, organisations are not being attacked by computers, but by people attempting to exploit human frailty as much as technical vulnerability. As such, this is a problem which requires a response that is grounded in strategy and judgement about business process, access, authority, delegation, supervision and awareness—not merely tools and technologies.

This is illustrated in at least four ways. First, knowing that people are often the weakest link in the security chain, hackers often exploit human naiveté, through attacks such as "spear phishing"—a targeted email supposedly sent from a source that you trust, such as your bank—to take advantage of the inattentive. Alternatively, hackers can try to break data encryption codes through the brute computing power of modern machines, or they can guess at, steal, or bribe their way to possession of an easy password. Encryption power doubles every 18 months, but the human brain's ability to remember a complex password without writing it down has not improved in at least 10,000 years.

Second, hackers innovate non-technologically as well as technologically. The scenario described above of falsified ATM cards, which closely mirrors real-world cases, shows how hacker "productivity" has jumped by an order of magnitude approaching 4 times—not because of new technology, but because of better-organised use of people in the "mule" capacity.

Third, cybersecurity solutions often require non-technical processes and tools—for example, training and awareness, and the involvement of legal and privacy experts for response, media relations, crisis management and remediation solutions in the wake of uncovering a cybercrime.

Finally, good security requires people to remain focused on their most important data. Companies that inventory and prioritise the data on their networks are able to focus on the "crown jewels"—and spend their limited cybersecurity budgets wisely.

Thus, one of the key organising principles of cybersecurity is not a technical question for the IT staff at all. It is a business question for senior managers. Yes, your IT team has to know what the best tools and technologies are for your business, but knowing that will do little good if you are focused on protecting the wrong assets.

## *Cybercrime threatens technology-enabled business processes*

The growing use of technology-enabled business processes makes cybercrime a very real threat to a wide variety of business operations. In our recent experience the systems most threatened are those that contain data directly leading to financial assets that can be stolen, or personal data that can be used to assemble an attack on financial assets. The technology-enabled business processes that are threatened by cybercrime include:

- ***Point of sale purchases*** by debit and credit cards in the everyday retail environment.

- ***ATM transactions*** in the everyday banking environment.

- Preserving or respecting the ***privacy of customers.*** This is especially true in the health care industry, where providers often maintain systems with considerable amounts of sensitive patient information, including identity, financial circumstances, insurance plans, and medical condition.

- ***E-commerce or on-line sales processes.*** Same issues as penetration of point of sales systems in the retail store or banking environment, except that it is in the on-line environment.

- ***Electronic business communications (email).*** External cyber criminals can penetrate corporate communications systems and steal critical commercial information, intellectual property, and sensitive executive communications.

- Taking advantage of ***infrastructure weak points*** to accomplish any of the above—for example, penetrating Wifi access points or intercepting other people's communications through them; attacking business operating systems using a "cloud" architecture by penetrating the server environment maintained by the cloud provider.

- ***Consumer incentives.*** Loyalty and other consumer incentive programmes that retain customer data and spending habits/preferences offer a treasure trove of data that can be used for identity theft and targeting for additional cybercrime.

- ***M&A.*** After the completion of a merger or acquisition, the company will often delay full integration of information security policies, processes and tools. This leaves vulnerabilities in a corporate IT environment which hackers can exploit—for example, by gaining access to databases from legacy enterprises that contain valuable intellectual property or other types of sensitive data.

- ***Supply chain.*** Suppliers, contractors and distributors are part of a company's ecosystem—often with authorised staff-like access to sensitive data and systems. Their risk is your risk, and a breach in the supply chain can have cascading effects on network security or, worse, allow direct access to sensitive data.

- ***Research, development and engineering.*** Proprietary technology, trade secrets, and intellectual property are targeted by nation-states, state-owned enterprises, and unethical corporations. Businesses have lost billions of US dollars in this way through theft by hackers and insiders of intellectual property to the benefit of competing organisations.

- ***Expansion into new markets.*** As a company moves into a new geographical market, it can become the target of the host government or local competitors who want to steal its technology, client lists or marketing plans. As the company is literally on another's "home turf," the insider problem extends beyond employees, to facility providers, talent search firms, janitorial services, even local government agencies.

*Three-fifths of respondents said procurement fraud occurred during vendor selection, and almost half noted that fraud occurred in the invitation to present a quote.*

# ***Other high-impact economic crimes***

## Procurement fraud: A growing opportunity, a growing threat

As discussed previously, this year we added procurement fraud as a new category in our survey, and 29% of respondents reported this type of economic crime.

Generally speaking, when an organisation goes into a commercial or public tender process or seeks to acquire goods and services for its own use—a common business process across all industries—the potential for procurement fraud exists. We anticipated a significant response in this category driven by three factors.

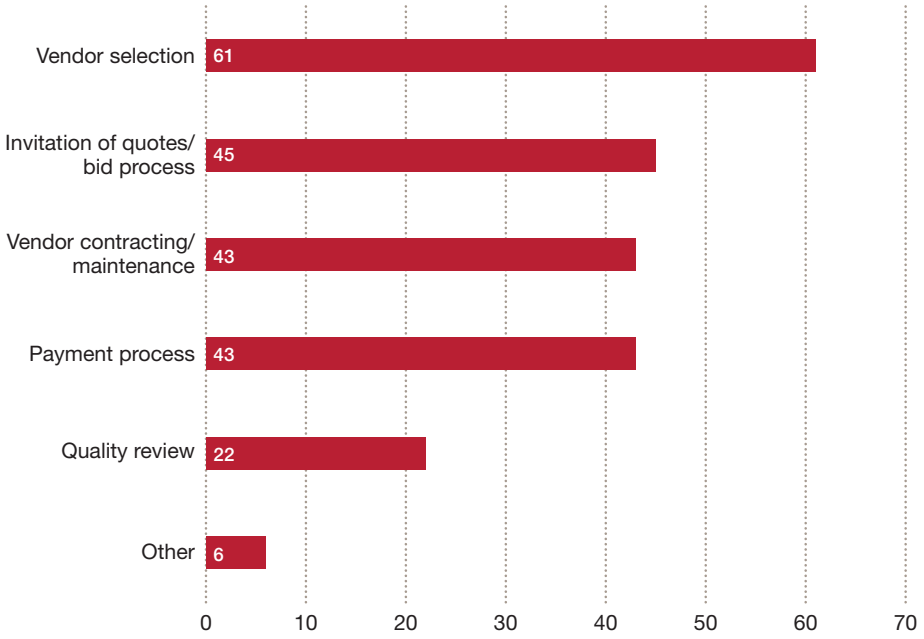
First, there has been an increase in more-competitive public tender processes from governments and state-owned businesses, unleashing the possibility of fraudulent activity on the part of agents and other third parties. No doubt, in past surveys procurement-related kickbacks, bid-rigging, or similar activities were reported as corruption. But with our new inquiry into where in the process procurement fraud primarily occurred, the connection has become clearer (see Figure 23). Three-fifths of respondents said procurement fraud occurred during vendor selection, and almost half noted that fraud occurred in the invitation to present a quote.

Second, as our recently launched 2014 Global CEO Survey highlights, a significant majority of businesses are focusing on making changes to their supply chain in response to global trends. Many are seeking deeper interconnections across their value chain, and using a more global supply model. And as suppliers become more integrated into companies' operations, the threat of significant disruption and monetary loss increases.

Third, as economies have emerged from the recent economic crisis, a shift in employment practices seems to have occurred. Short-term, post-crisis measures such as replacing permanent, in-house positions with more dispensable and scalable outside resources have persisted, with companies more willing to outsource tasks once part of their noncore and core operations.

Based on these responses, we see procurement fraud as a double threat. It victimises businesses in their own acquisition of goods and services. And it prevents companies from competing fairly and successfully for business opportunities subject to a commercial or public tender process.

**Figure 23: Procurement fraud ocurrence by stage**




*% of all respondents who experienced procurement fraud over the survey period*

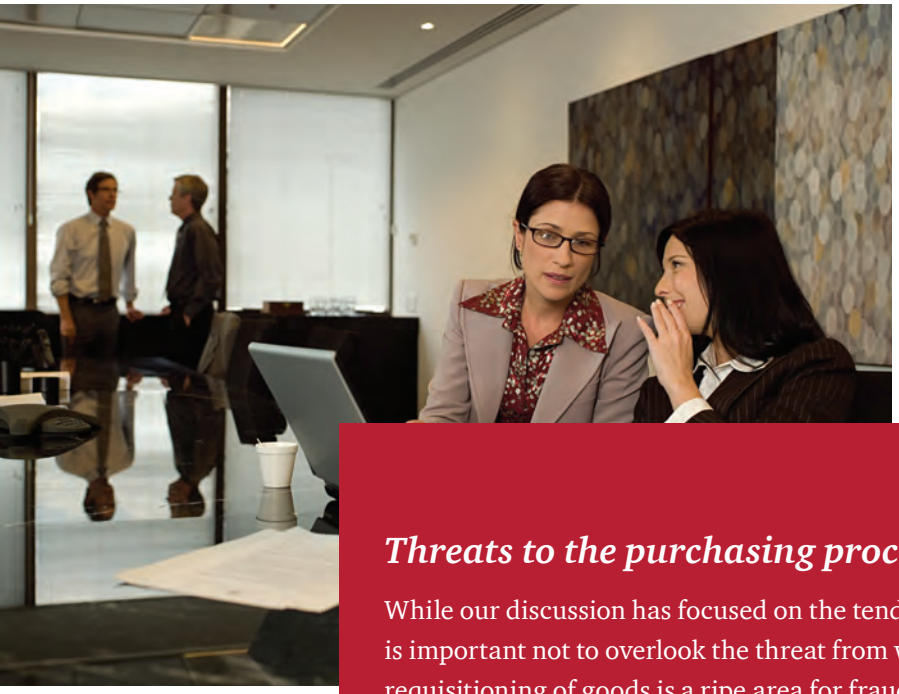
It's worth noting that procurement frauds are not only investigated and enforced at the sovereign level. In recent years, the World Bank has taken a more active stance against fraud in general, with 79 cases opened in 2012. As the institution commonly funds infrastructure projects in developing countries, it applies particular scrutiny to procurement. Running afoul of the World Bank can lead to a host of sanctions, including future contract ineligibility and cross-debarment from other institutions.

## Procurement fraud by industry and region

Not surprisingly, the industries reporting the most procurement fraud included government/ state-owned enterprises (46%), energy, utilities and mining (43%), engineering and construction (42%) and transportation and logistics (39%)—sectors where significant elements of operations depend on close collaboration with governments, government entities and prime contractors likely to use tendering processes.

Like the economic crimes of bribery and corruption and money laundering, procurement fraud erodes the integrity of your employees because it places them at the crossroads of equally laudable goals—profit and compliance.

Regionally, the highest response rates for procurement fraud were found in Africa (43%) and the Middle East (33%)—areas with large government sectors, important energy and mining industries, and growing construction and infrastructure projects. The results underscore the risks organisations in these industries face.



### *Threats to the purchasing process*

While our discussion has focused on the tender process and external parties, it is important not to overlook the threat from within. In our experience, the requisitioning of goods is a ripe area for fraud. The threat is especially great in cultures where loyalty to family, schoolmates, local community, or even national pride are strong influences—stronger perhaps than dry corporate policy statements or legalistic sounding codes of conduct.

An individual within the purchasing and supply department may have a pre-existing relationship with a vendor who wants to win business from the organisation. The insider provides information on the bidding process, such as the bid amounts of competitors, to ensure an advantage for their preferred bidder. Or, the insider could approve a price higher than necessary.

Alternately, your controls may not function as planned. We have observed countless incidences of employees in approval roles acquiescing to pressure from "the boss" to process payments that do not meet all aspects of policy and procedure. This tension between an executive's loyalty to the company versus their connectivity to the local milieu is a real and continuing threat to controls.

# Accounting fraud

Accounting fraud has always been one of the major crimes reported in our survey, and since 2005 it has been cited by over 20% of our respondents that experienced economic crime. This year was no exception, as 22% of respondents reported experiencing accounting fraud.

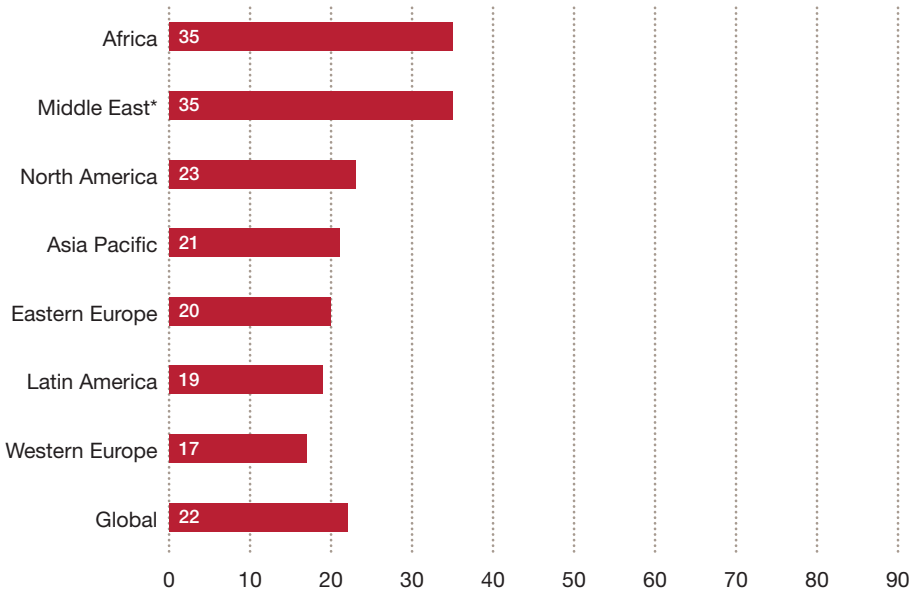
Financial statements are a fundamental barometer of a business—and a traditional starting point for analyses relating to credit decisions, contract awards, and capital raising in public markets. Accounting fraud—which includes misleading or falsely prepared financial statements—can dupe banks, lessors, vendors, and investors into risky or misguided decisions. Due to the ubiquitous use of financial statements and financial data in business operations, this kind of economic crime impacts a variety of business processes.

*Cross border listings*

*Recently, accounting fraud was in the spotlight as a variety of foreign-based businesses were exposed as trading in the US NASDAQ, Hong Kong, and Singapore stock markets on falsely prepared or misleading financial statements. The losses to investors have led to a series of regulatory investigations and a long series of discussions between China and the United States regarding the division of regulatory responsibility for these companies and their auditors.*

The Middle East and Africa report notably more accounting fraud than the global rate of 22%, with a response rate of over one third. Asia Pacific and North American respondents reflect the global average of 22%. We believe this may reflect the megatrend of wealth moving from West to East, as many businesses and private equity funds are investing in emerging-market economies.

**Figure 24: Reported accounting fraud, by region**




*% of all respondents who experienced accounting fraud over the survey period*

*Middle East was included in the "Asia Pacific" region in 2011

From an industry perspective, higher-than-average incidences of accounting fraud were reported in engineering and construction (39%) as well as transportation and logistics (31%).

A possible cause behind these industry results are high incidences of bribery and corruption. As bribes and related payments are not usually recorded accurately in financial statements, a corruption issue can quickly turn into an accounting fraud issue as well. Additionally, construction and engineering projects often use complex accounting estimates to record revenue, leading to potential irregularities.

Accounting fraud (continued)

### *Joint venture*

For investors, the joint venture (JV) form remains a popular market entry approach. Successful governance of joint ventures is highly dependent upon accurate financial information.

Consider, for example, the common circumstance of a Western business forming a JV with an enterprise in an emerging market. Likely, the Western partner is the financial partner and the emerging market's partner is the operating partner, who contributes the personnel and physical facilities being used by the JV. In many such situations the monthly accounting reports are the primary means of informing the overseas venture partner of the progress of the business. If difficulties are encountered, it is a relatively simple matter to delay reporting problems, or hide them entirely by manipulating the financial statements.

This form of accounting fraud is often used to cover over more serious underlying issues, such as establishing competing factories, sometimes with investment funds from the Western JV partner, manipulating cost allocations to the operating partner's other divisions, or otherwise undermining the venture in numerous fraudulent ways.

# Asset misappropriation

Asset misappropriation is by far the most common economic crime experienced by organisations reporting any fraud, with 69% of respondents suffering from it. This amount is more than double the second highest occurring type of economic crime, procurement fraud (29%). While the individual impact of this fraud may be lower than that of cybercrime or government-enforced frauds, the magnitude of the threat requires organisations to be vigilant.

You have likely heard the phrase "falling off the back of the truck." This euphemism for asset misappropriation points to one of the fundamental business processes it attacks—distribution, logistics and warehousing.

Take a global operating retail company with warehouses of inventory. Not only are these products exposed to the organisation's own employees, they also constantly pass through the hands of third parties, leading to several points of vulnerability in the supply chain and distribution process. Schemes can be as simple as employees stealing inventory or more complicated endeavours, such as covering up a theft by marking good inventory as "scrap," removing it from the premises, and then reselling it.

Another function which is commonly threatened by asset misappropriation is the expense reporting process—which further impacts cash disbursements and potentially leads to collateral impacts such as inaccurate books and records.

## Intellectual property theft—The crown jewels at risk?

Intellectual property (IP) infringement and theft is often an especially damaging economic crime—and one that is very much on the mind of global CEOs, 43% of whom reported they are worried about being able to protect it, according to our latest Global CEO Survey.

In our cybercrime section, we noted that organisations should focus their cybersecurity on protecting these crown jewels, rather than on just their network. In certain industries intellectual property is the key asset that allows the company to win in the marketplace.

Eighteen per cent of respondents indicated that they expect to be threatened by this economic crime in the next 24 months, more than double the percentage actually reported in the survey period (8%).

The gap between expectations and experience is a consistent theme in the area, and we believe it demonstrates another concept: successful crimes which target assets often go undetected. Our respondents appear to be aware that their IP is threatened, but their controls may not be detecting the actual attacks.

*While global averages continue their 56% internal/ 40% external split…the financial services sector was unique in reporting almost the inverse…*

# The Fraudster: Know your adversary

We asked respondents whose organisation experienced economic crime to profile the main perpetrator of the most serious fraud faced. The picture which emerged was similar to previous years, with 56% reporting that the main perpetrator was internal, and 40% reporting the main perpetrator was external.

But dig a little into the data, and some sharp contrasts begin to emerge at the sector level.

While global averages continue their 56% internal/40% external split, Figure 25 shows the financial services sector was unique in reporting almost the inverse, citing external perpetrators (59%) as their greatest fraud adversaries—a continuation of a pattern evident in 2011 as well. This is likely due to the disproportionately high rate of cybercrime affecting financial services (45%, compared to all other industries at 17%) and to the fact that cybercrime tends to involve external fraudsters.

*But dig a little into the data, and some sharp contrasts begin to emerge at the sector level.*

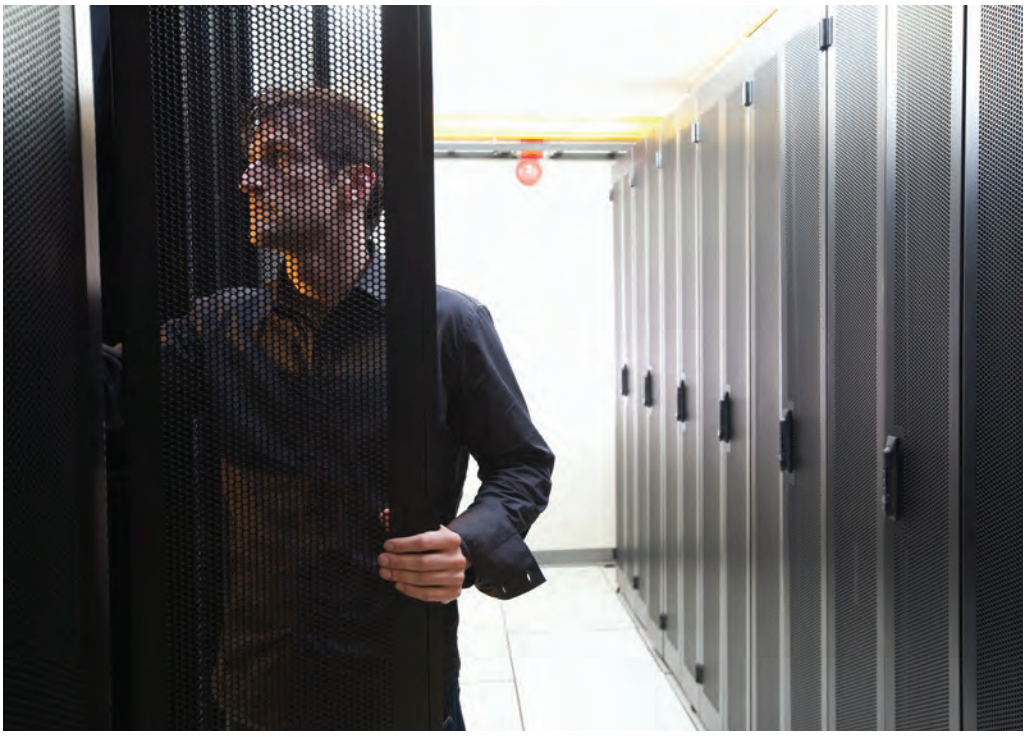
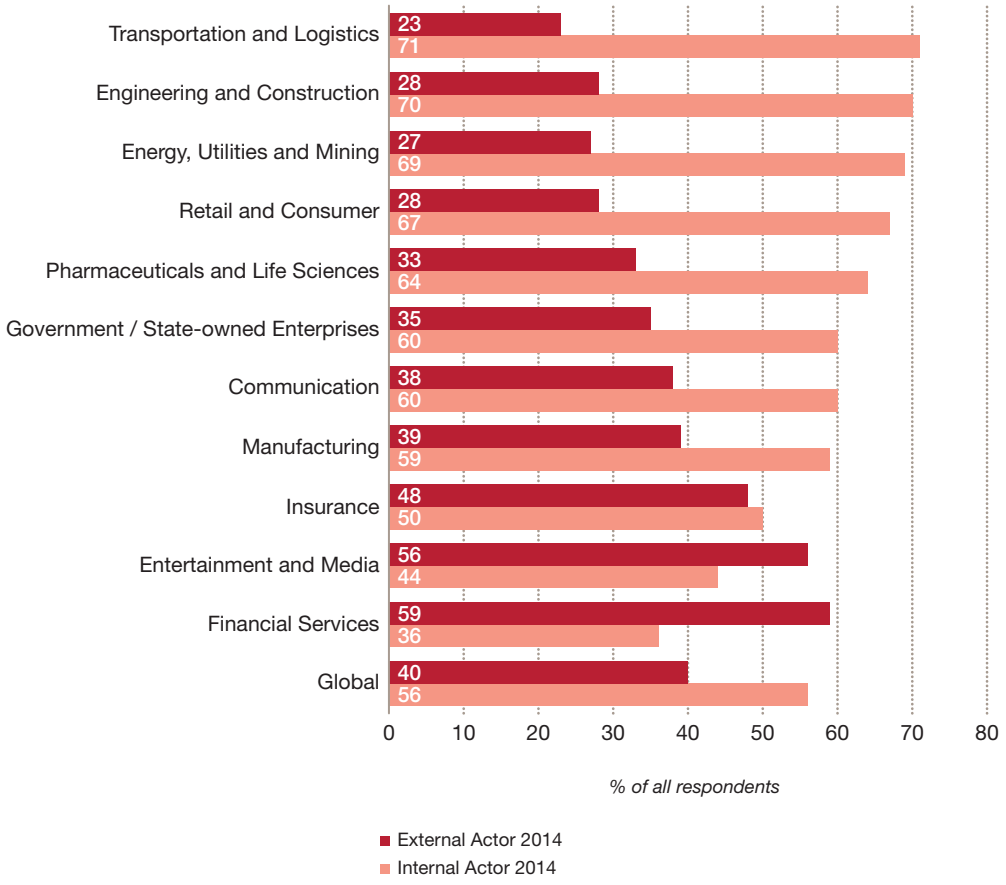


**Figure 25: Internal vs. external perpetrator, selected industries**




On the other hand, certain industries consistently report a preponderance of internal perpetrators—for example, the engineering and construction (70%) and energy, utilities and mining (69%) sectors. We've seen these industries grouped before—in discussions of both bribery and corruption and procurement fraud. These results could be telling us two things: that organisations involved in these heavy industries are especially threatened by these frauds; and, that keeping an eye on internal players is a key to controlling these risks.

Presumably, there is a silver lining to having most of one's fraud losses attributable to internal players—you have a better opportunity to mitigate these risks through improved internal policies, processes and controls when the fraudster is someone employed by the company. Mitigating the actions of external criminals may not be so easy.

# To catch a thief

So how do you stop an economic crime in progress—or better yet, before it happens?

Methods of fraud detection usually fall into one of three categories: corporate controls, corporate culture, or beyond corporate control. The figure below displays how the major fraud at responding organisations was detected. Note that the percentage of fraud detected through transaction monitoring and data analytics increased by over a third, from 18% to 25%.

**Figure 26: Method of detection of most serious economic crime experienced**


*Data Analytics was added as a category in the 2014 survey.

**Figure 27: Economic crime detection methods**

| | 2005 | | 2007 | | 2009 | | 2011 | | 2014 | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Controls** | 36 | 67 | 34 | 77 | 46 | 80 | 50 | 73 | 55 | 78 |
| **Culture** | 31 | | 43 | | 34 | | 23 | | 23 | |
| **Accident** | 33 | | 23 | | 20 | | 28 | | 21 | |

*Historical % reported, how economic crime was detected*

## *Rise of data analytics*

Over the past several years, we have seen a marked rise in the number of major frauds discovered through data analytics and suspicious transaction reporting. What does this process entail?

Data analytics begins with a systematic approach to data gathering, cleansing, and standardisation. Current technology enables analytics to leverage a growing abundance of available and disparate information, allowing for better comprehension of an organisation's data—and therefore a better understanding of potential risks.

A well-designed programme will efficiently risk-rank transactions and entities for investigation, and may use an approach which facilitates the detection of hidden relationships and connections with known high-risk entities. It identifies atypical transactional patterns through statistical, keyword, and exception-based data mining.

Through continuous feedback, anticorruption and antifraud analytics continue to evolve and improve. Companies are implementing frameworks and optimizing findings by leveraging their collective knowledge and experiences from past reviews and investigations.

Moving forward, we expect more organisations to build on this success story, and use these leading data analysis tools to help detect and mitigate fraud.

One other encouraging sign was the drop in the number of respondents who indicated that they "Don't Know" how fraud was detected, which we had flagged in our 2011 report. Greater awareness of how fraud is detected can help organisations tailor their procedures to increase effectiveness.

## Whistle-blowing

Just as the oft-repeated law enforcement mantra—"If you see something, say something"—can help stop or detect a crime by amplifying the potential number of witnesses, one would expect whistle-blowing to be an effective fraud detection tool. Many countries, recognising the important role whistle-blowing plays in combating economic crime, have enacted or are considering enacting laws protecting whistle-blowers from retribution.

Yet our survey uncovered some interesting contrasts. While more than six in ten companies report having a whistle-blower mechanism in place, and half describe their programme as being either effective or very effective, only a fraction (5 per cent) of all companies reported that their whistle-blowing system was the mechanism by which they uncovered fraudulent events.

This suggests several important points. First, while having a sophisticated whistle-blowing mechanism may meet current expectations about quality fraud detection efforts, it is not a stand-alone solution. There is no substitute for a strong culture and strong controls to immunise your organisation against fraud.

Second, the low rate of whistle-blowing reported could in fact reflect the increasing sophistication of internal controls and suspicious transaction reporting, which may detect frauds before employees feel the need to call the fraud hotline. Another possibility is a fear of adverse consequences for reporting an incident.

Also, whistle-blowing practices can vary widely from country to country. For example, in India more than four-fifths of respondents reported their entity had a whistle-blowing mechanism—and a recently opened fraud "hotline" to report government fraud was overwhelmed by thousands of calls.

## The enemy hiding in plain sight

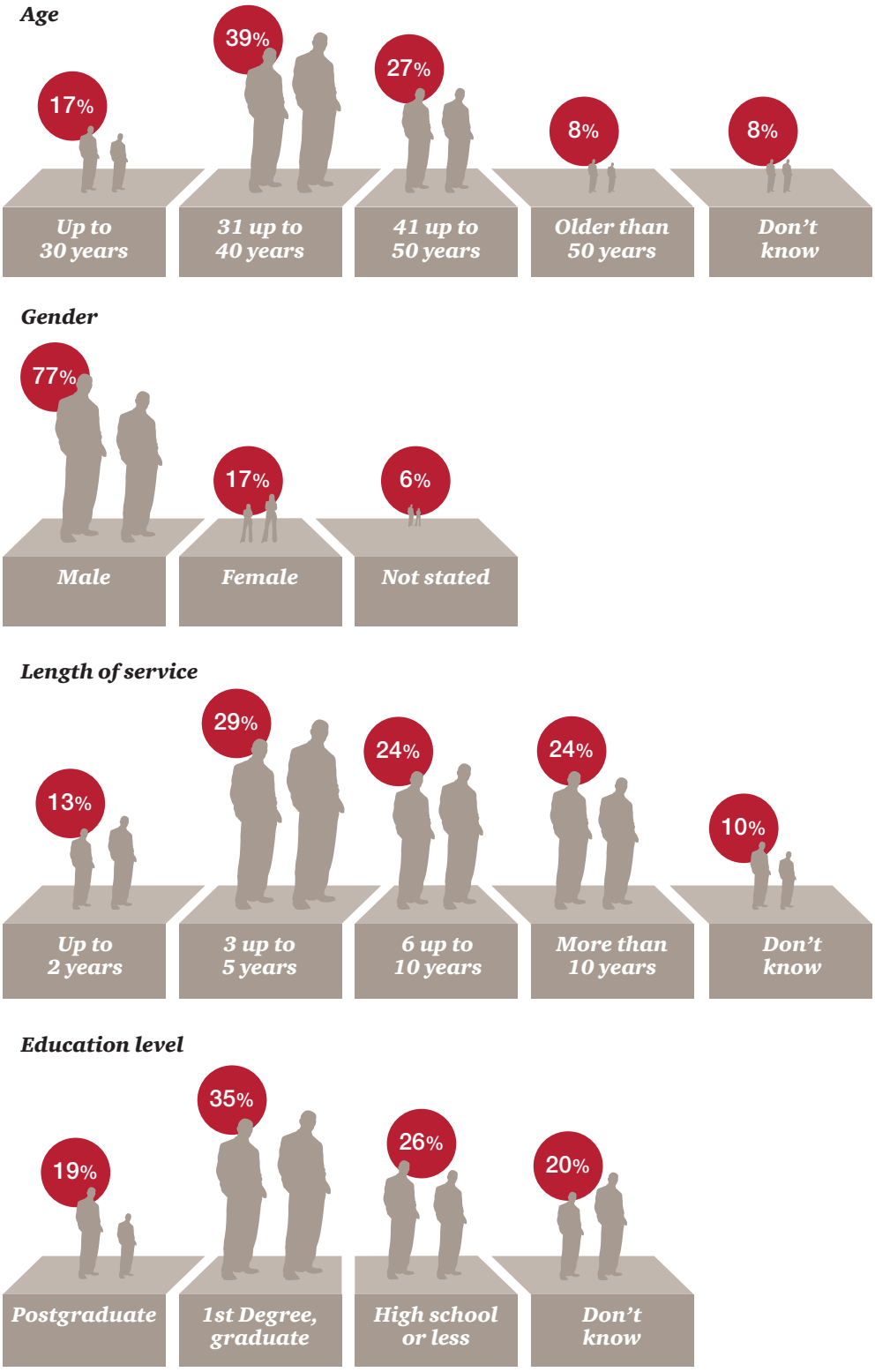
Practitioners commonly refer to a "Fraud Triangle"—the three elements that are often present when a perpetrator commits fraud: pressure, opportunity and rationalisation.

Three quarters (73%) of our respondents indicated that the opportunity or ability to commit the crime was the factor that most contributed to economic crime by an internal fraudster. Of the three factors, opportunity is the one most within an organisation's control. While life's pressures and the ability to rationalise may swirl around employees, if an organisation can limit the opportunity, they may be able to more often stop the fraud before it starts.

So who's committing internal fraud? As Figure 26 shows, our results indicate that the overall profile of the internal fraudster generally remained the same as in 2011—middle-aged males with a college education or higher who have substantial tenure with the organisation. Globally, almost half of all frauds are committed by employees with 6 or more years of experience and almost a third (29%) are committed by employees with 3 to 5 years of experience.

However, individual territories report a wide variety of responses and potential emerging trends. For example, in the UK, more than one quarter of internal fraudsters were female, double the figure reported in our previous survey.

## Figure 28: Age, gender, length of service and education level of internal perpetrator




*% respondents who reported that an internal party was the main perpetrator of economic crime*

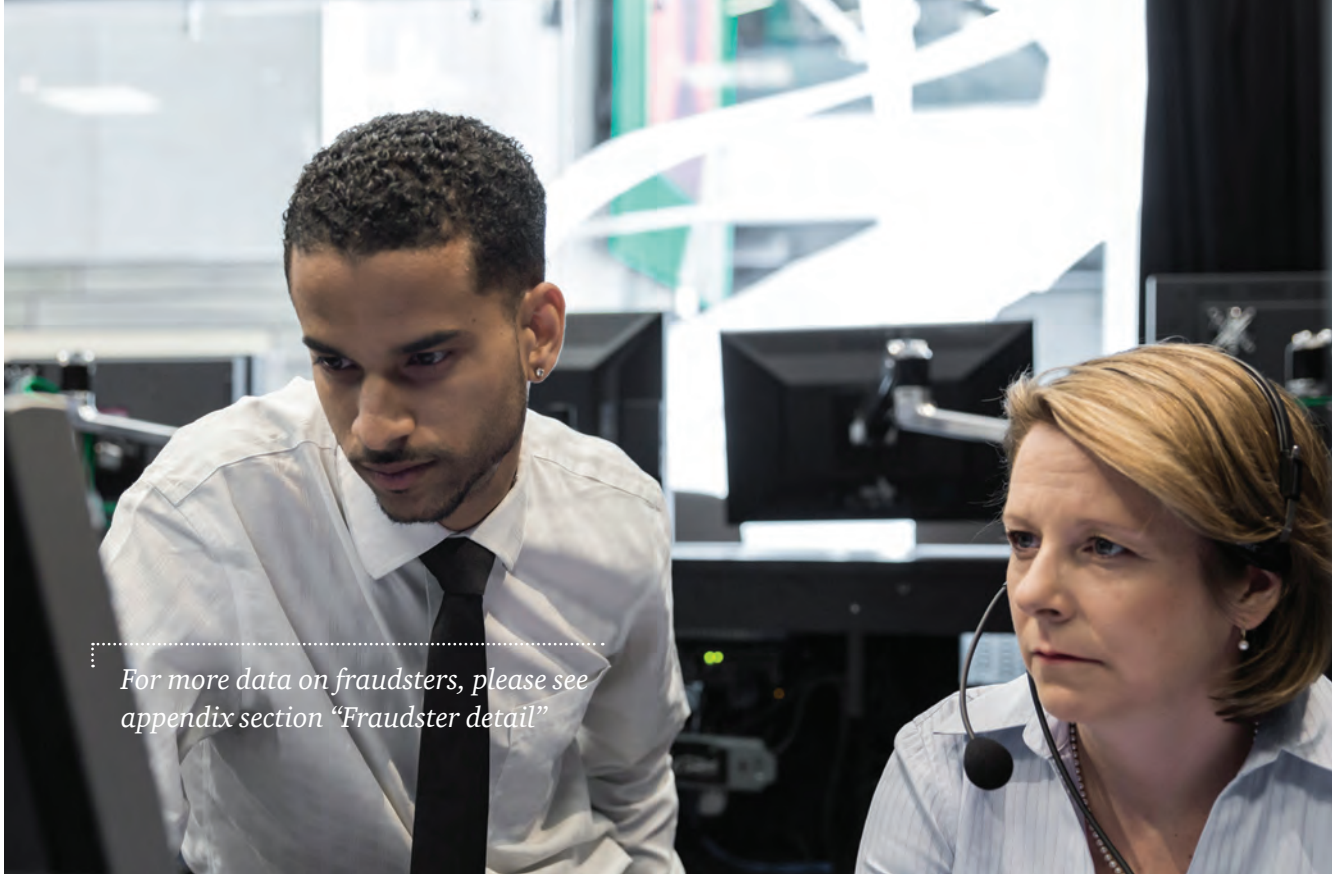
● 2014 Global

## *Senior management and fraud impacts*

In our experience, the age and seniority of the perpetrator of an internal act of fraud have a proportionately large effect on its impact. That's because executives of greater seniority are likely to get a greater degree of deference in navigating exceptions to internal control policies.

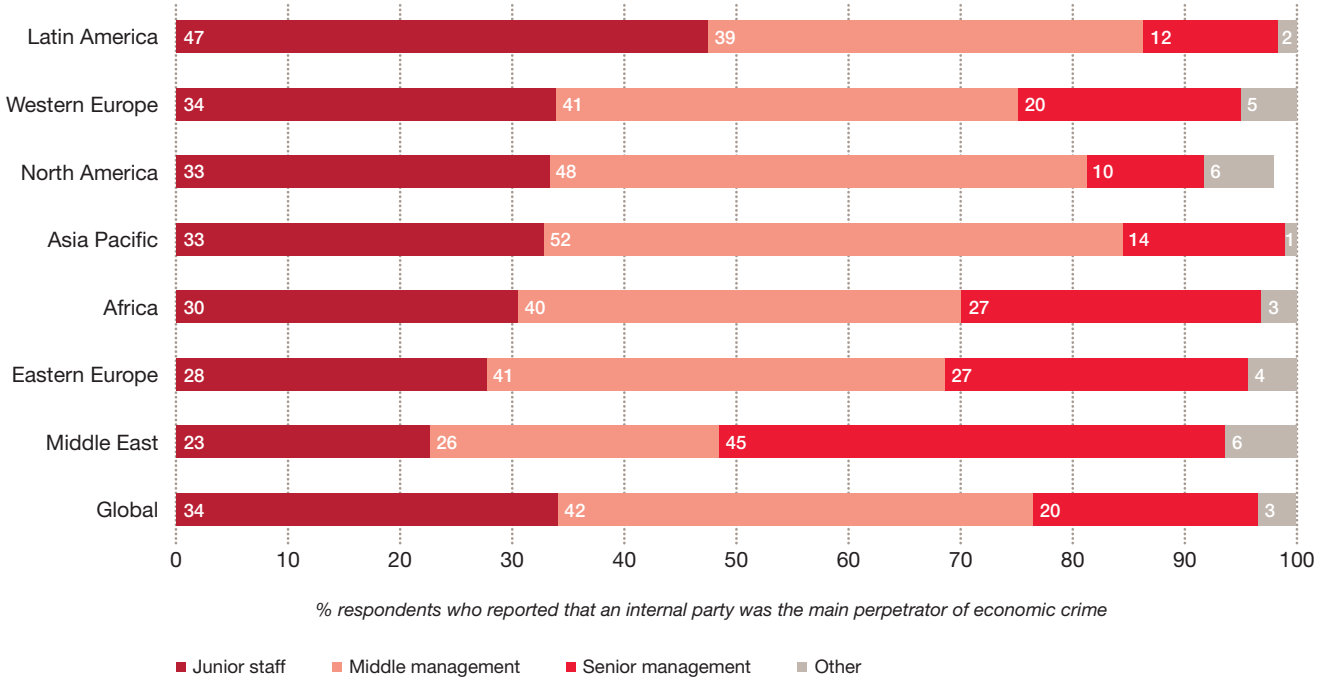
Consider the senior private banker who assures the wire transfer operators that he'll handle the client call-back procedure to confirm instructions for payments. Or the boss who says she'll take care of getting the documentation needed to support the payment. Or even the division manager who budgets for the amount he intends to "withdraw" from the corporate coffers based on bogus invoices for services.

These real-life examples from North America, Asia and Europe illustrate the unique position of senior people. Not only are they authority figures with respect to internal control policies—and thus have access not enjoyed by employees of lesser rank—they are also custodians of the corporate culture. As such, the financial damage of the fraud may be compounded by its corrosive effect on that same culture.



*For more data on fraudsters, please see appendix section "Fraudster detail"*

**Figure 29: Profile of internal perpetrator, by region**



*5,128 respondents from over 95 countries completed the 2014 Global Economic Crime Survey.*

# *Data appendix*
## Detailed regional and industry data

5,128 respondents from over 95 countries completed the *2014 Global Economic Crime Survey*. We asked these respondents to indicate whether they had experienced an economic crime in the survey period. Figure 30 lists the top territories reporting economic crimes.

**Figure 30: Territories with highest percentage of economic crime**

| Territory | Reported Fraud 2014 | Reported Fraud 2011 |
|---|---|---|
| South Africa | 69% | 60% |
| Ukraine | 63% | 36% |
| Russia | 60% | 37% |
| Australia | 57% | 47% |
| Papua New Guinea | 57% | NA |
| France | 55% | 46% |
| Kenya | 52% | 66% |
| Argentina | 51% | 45% |
| Spain | 51% | 47% |
| **Global** | **37%** | **34%** |

As indicated by the table, a number of growing economies have reported higher rates of economic crime. Certain developed countries also registered high figures, potentially reflecting greater detection capabilities.

**Figure 31: Territories with lowest percentage of economic crime**

| Territory | Reported Fraud 2014 | Reported Fraud 2011 |
|---|---|---|
| Malaysia | 24% | 44% |
| Italy | 23% | 17% |
| Turkey | 21% | 20% |
| Peru | 20% | 35% |
| Hong Kong/ Macau* | 16% | n/a |
| Japan | 15% | 5% |
| Portugal | 12% | n/a |
| Denmark | 12% | 29% |
| Saudi Arabia** | 11% | n/a |
| **Global** | **37%** | **34%** |

* Part of greater China in 2011; ** Part of greater Middle East in 2011

Low reports of fraud can reflect a number of things: respondents reluctant to report fraud, low levels of asset misappropriation (the most common fraud), or a lack of controls which can help detect fraud.

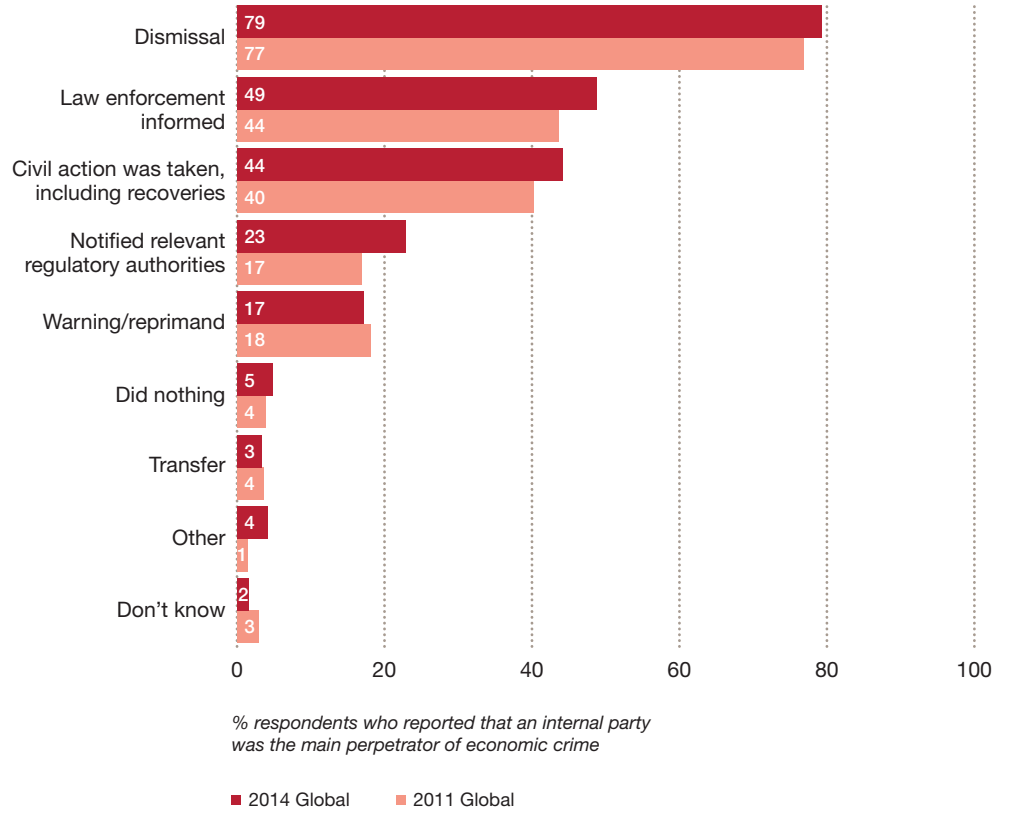
**Figure 32: Emerging 8 percentage of economic crime**

| Territory | Reported Fraud 2014 | Reported Fraud 2011 |
|---|---|---|
| Brazil | 27% | 33% |
| Russia | 60% | 37% |
| India | 34% | 24% |
| China* | 27% | NA |
| South Africa | 69% | 60% |
| Turkey | 21% | 20% |
| Mexico | 36% | 40% |
| Indonesia** | NA | 16% |
| **Global** | **37%** | **34%** |

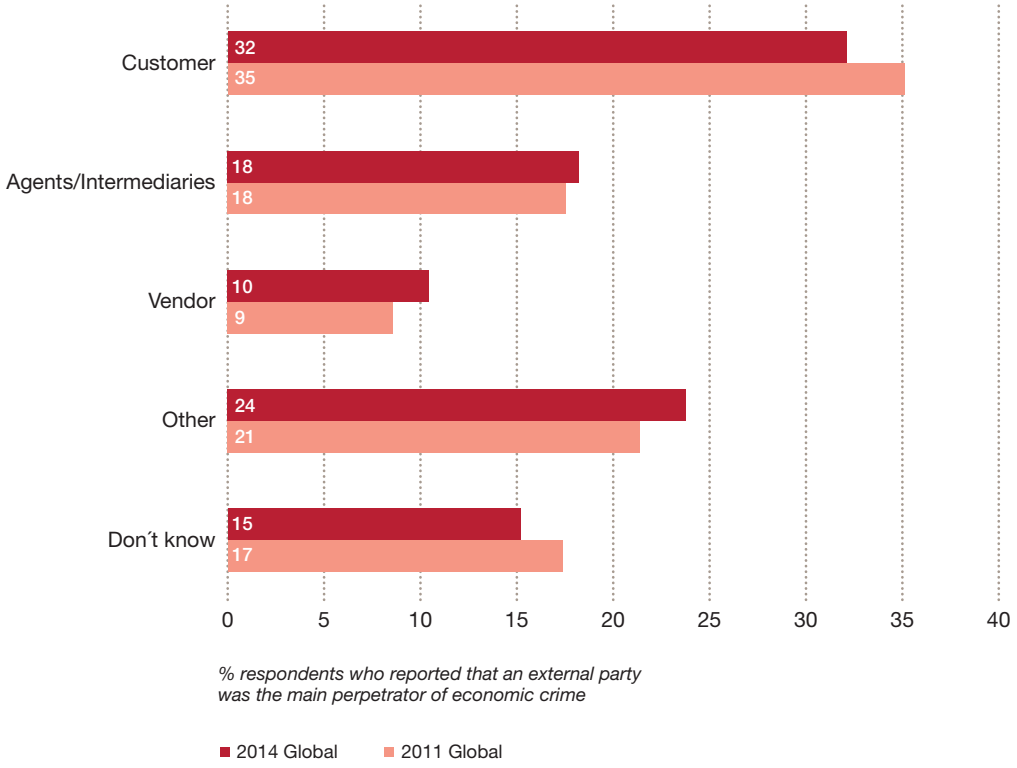
* 2014 statistic for China excluding Hong Kong/Macau—figures unavailable for 2011; ** Figures unavailable for 2014

# Fraudster detail

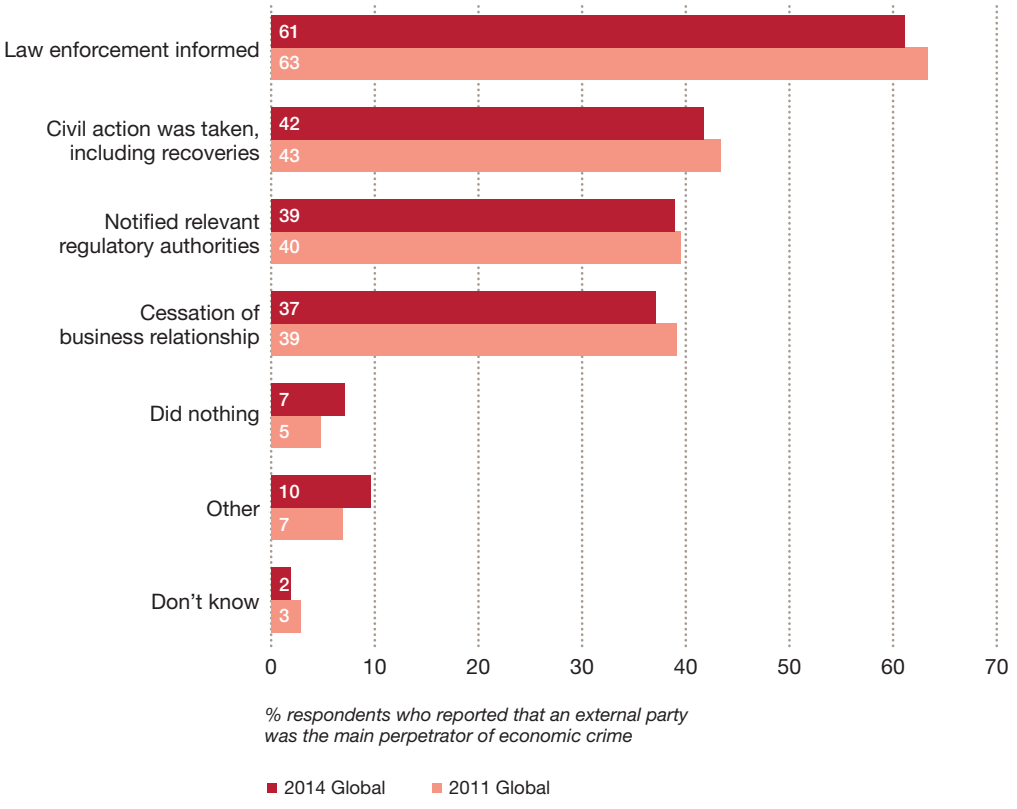
**Figure 33: Actions taken against internal perpetrator**



## Figure 34: Profile of external perpetrator




## Figure 35: Actions taken against external perpetrator



# Methodology and acknowledgments

We carried out our seventh Global Economic Crime Survey between August 2013 and February 2014.

The survey had four sections:

- general profiling questions
- comparative questions looking at what economic crime organisations had experienced
- cybercrime fraud threats
- corruption/bribery, money laundering and competition law/antitrust law

### *About the survey*

The 2014 Global Economic Crime Survey was completed by 5,128 respondents (compared to 3,877 respondents in 2011) from 99 countries (compared to 78 countries in 2011). Of the total number of respondents, 50% were senior executives of their respective organisations, 35% represented listed companies and 54% represented organisations with more than 1,000 employees.

### *We used the following research techniques:*

1. ***Survey of executives in the organisation.*** The findings in this survey come from executives' reports of their experiences of economic crimes in their organisations. We obtained information from them on the different types of economic crime, their impact on the organisation (both the financial loss and any collateral damage), the perpetrator of these crimes, what action the organisation took and how they responded to the crime.

2. ***Questions relating to cybercrime, corruption/bribery, money laundering and competition law/antitrust law.*** This survey takes a detailed look at these threats which are often systemic in nature and thus are more prone to have a long term, damaging impact on the organisation.

3. ***Analysis of trends over time.*** Since we started doing these surveys in 2001, we have asked a number of core questions, and extra ones that are relevant from time to time, dealing with issues likely to have an impact on organisations around the world. With this historical data to hand, we can see current themes, chart developments, and find trends.

### *Other Resources:*

- *PwC—17th Annual CEO Survey* [http://www.pwc.com/gx/en/ceo-survey/]
- *PwC—Building Trust in a Time of Change: Global Annual Review 2013* [http://www.pwc.com/gx/en/annual-review/megatrends/index.jhtml]
- *PwC—German Economic crime survey: Economic crime and corporate culture 2013* (German language only) [http://www.pwc.de/de/risiko-management/wirtschaftskriminalitaet-2013.jhtml#]
- *PwC—Global State of Information Security Survey* [http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml]

## Figure 36: Participating territory counts

| Territory | 2014 | 2011 |
|---|---|---|
| **Asia Pacific** | **906** | **669** |
| Australia | 79 | 79 |
| China including Hong Kong[1] | N/A | 22 |
| Hong Kong / Macau | 116 | N/A |
| China (excluding Hong Kong) | 85 | N/A |
| India | 115 | 106 |
| Indonesia | 4 | 84 |
| Japan | 75 | 73 |
| Malaysia | 110 | 93 |
| New Zealand | 82 | 93 |
| Papua New Guinea | 81 | 1 |
| Singapore | 82 | 18 |
| Taiwan | 0 | 2 |
| Thailand | 76 | 79 |
| Vietnam | 1 | 19 |
| **Africa** | **604** | **259** |
| Algeria | 2 | 0 |
| Angola | 22 | 1 |
| Botswana | 5 | 1 |
| Cameroon | 6 | 0 |
| Democratic Republic of Congo | 1 | 0 |
| Ghana | 3 | 29 |
| Guinea | 2 | 0 |
| Ivory Coast | 3 | 0 |
| Kenya | 124 | 91 |
| Lesotho | 1 | 0 |
| Liberia | 0 | 5 |
| Malawi | 1 | 0 |
| Morocco | 17 | 0 |
| Mozambique | 4 | 0 |
| Namibia | 26 | 2 |
| Nigeria | 82 | 3 |
| Sierra Leone | 1 | 0 |
| South Africa | 134 | 123 |
| Swaziland | 4 | 1 |
| Tanzania | 12 | 0 |
| Tunisia | 17 | 2 |
| Uganda | 12 | 0 |
| Zambia | 83 | 1 |
| Zimbabwe | 42 | 0 |

| Territory | 2014 | 2011 |
|---|---|---|
| **Middle East[2]** | **232** | **128** |
| Unspecified Middle East Countries | N/A | 127 |
| Bahrain | 2 | N/A |
| Egypt | 7 | N/A |
| Jordan | 9 | N/A |
| Lebanon | 8 | N/A |
| Oman | 1 | N/A |
| Qatar | 12 | N/A |
| Saudi Arabia | 74 | N/A |
| Sudan[3] | 1 | 1 |
| Syria | 1 | N/A |
| UAE | 117 | N/A |
| **Western Europe** | **1,555** | **1,317** |
| Andorra | 0 | 1 |
| Austria | 6 | 8 |
| Belgium | 68 | 84 |
| Cyprus | 88 | 5 |
| Denmark | 118 | 116 |
| Finland | 34 | 61 |
| France | 131 | 112 |
| Germany[4] | 10 | 38 |
| Greece | 11 | 92 |
| Ireland | 78 | 80 |
| Israel | 31 | - |
| Italy | 101 | 127 |
| Luxembourg | 12 | 3 |
| Netherlands | 75 | 41 |
| Norway | 92 | 67 |
| Portugal | 75 | 0 |
| Spain | 79 | 85 |
| Sweden | 91 | 79 |
| Switzerland | 83 | 140 |
| UK[5] | 372 | 178 |
| **North America** | **215** | **209** |
| Canada | 100 | 53 |
| USA | 115 | 156 |

*1) China and Hong Kong/Macau were combined from 2005-2011. They were separated in the 2014 survey.*

*2) Middle East was previously part of Asia Pacific region totals.*

*3) Sudan was previously part of Africa region totals.*

*4) PwC Germany conducted a separate survey which captured 603 respondents from Germany in 2013.*

*5) UK includes instances when the survey responder indicated Guernsey as territory.*

## Figure 36: Participating territory counts (continued)

| Territory | 2014 | 2011 |
|---|---|---|
| **Central & Eastern Europe** | **877** | **804** |
| Bulgaria | 79 | 58 |
| Croatia | 0 | 1 |
| Czech Republic | 94 | 84 |
| Estonia | 0 | 1 |
| Hungary | 91 | 85 |
| Kazakhstan | 1 | 0 |
| Lithuania | 1 | 7 |
| Moldavia | 0 | 1 |
| Montenegro | 0 | 1 |
| Poland | 94 | 79 |
| Romania | 77 | 76 |
| Russia | 111 | 126 |
| Serbia | 52 | 14 |
| Slovakia | 76 | 84 |
| Slovenia | 33 | 48 |
| Turkey | 78 | 55 |
| Ukraine | 90 | 84 |

| Territory | 2014 | 2011 |
|---|---|---|
| **Latin America** | **711** | **483** |
| Argentina | 82 | 77 |
| Bahamas | 2 | 0 |
| Barbados | 1 | 0 |
| Bolivia | 0 | 3 |
| Brazil | 132 | 115 |
| Chile | 75 | 1 |
| Colombia | 1 | 1 |
| Cuba | 2 | 0 |
| Dominican Republic | 1 | 0 |
| Ecuador | 22 | 11 |
| Mexico | 211 | 174 |
| Peru | 82 | 17 |
| Venezuela | 100 | 84 |
| **No primary country specified** | **28** | **8** |
| **Total** | **5,128** | **3,877** |

## Figure 37: Participating industry groups

*% respondents*

| Industry | 2014 | 2011 |
|---|---|---|
| Aerospace and defence | 1% | 1% |
| Automotive | 4% | 4% |
| Chemicals | 2% | 2% |
| Communication | 3% | 3% |
| Energy, utilities and mining | 7% | 7% |
| Engineering and construction | 6% | 5% |
| Entertainment and media | 2% | 3% |
| Financial services | 19% | 18% |
| Government/state-owned enterprises | 5% | 5% |
| Hospitality and leisure | 2% | 2% |
| Insurance | 7% | 5% |
| Manufacturing | 9% | 12% |
| Pharmaceuticals and life sciences | 5% | 5% |
| Professional services | 6% | 6% |
| Retail and consumer | 7% | 8% |
| Technology | 5% | 5% |
| Transportation and logistics | 5% | 4% |

## Figure 38: Principal function of participants

*% respondents*

| Industry | 2014 | 2011 |
|---|---|---|
| Audit | 14% | 16% |
| Advisory/Consultancy | 4% | 3% |
| Compliance | 6% | 5% |
| Customer service | 1% | 1% |
| Executive management | 18% | 17% |
| Finance | 28% | 29% |
| Human resources | 1% | 1% |
| Information technology | 2% | 4% |
| Legal | 4% | 4% |
| Marketing and sales | 3% | 2% |
| Operations and production | 2% | 3% |
| Procurement | 1% | 0% |
| Research and development | 1% | 1% |
| Risk management | 6% | 6% |
| Security | 3% | 4% |
| Tax | 1% | 1% |
| Other (please specify) | 6% | 2% |

## Figure 39: Job title of participants

| | % respondents | |
|---|---|---|
| | 2014 | 2011 |
| **Senior Executives** | **50%** | **53%** |
| Board Member | 4% | 4% |
| Chief Executive Officer/President/ Managing Director | 12% | 10% |
| Chief Operating Officer | 2% | 2% |
| Chief Financial Officer/Treasurer/ Comptroller | 23% | 23% |
| Chief Information Officer/ Technology Director | 1% | 3% |
| Chief Security Officer* | 2% | |
| Other C-level Executive (please specify) | 6% | 10% |
| **Non-Senior Executives** | **49%** | **47%** |
| Senior Vice President/Vice President/ Director | 7% | 8% |
| Head of Business Unit | 4% | 7% |
| Head of Department | 15% | 15% |
| Head of Human Resources* | 1% | |
| Manager | 22% | 17% |
| Others (please specify) | 2% | 0% |

**Option added in the 2014 survey*

## Figure 40: Organisation types participating

| | % respondents | |
|---|---|---|
| | 2014 | 2011 |
| Listed on a stock exchange | 35% | 36% |
| Private | 50% | 51% |
| Government/state-owned enterprises | 9% | 10% |
| Other (please specify) | 6% | 3% |

## Figure 41: Size of participating organisations

| | % respondents | |
|---|---|---|
| | 2014 | 2011 |
| Up to 1,000 employees | 44% | 43% |
| 1,001–5,000 employees | 20% | 20% |
| More than 5,000 | 34% | 34% |

# Terminology

## Accounting fraud

Financial statements and/or other documents are altered or presented in such a way that they do not reflect the true value or financial activities of the organisation. This can involve accounting manipulations, fraudulent borrowings/raising of finance, fraudulent application for credit and unauthorised transactions/rogue trading.

## Asset misappropriation, including embezzlement/ deception by employees

The theft of assets (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit.

## Bribery and corruption

The unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail. It can also refer to the acceptance of such inducements. Specific examples include kickbacks, extortion, gifts (with strings attached), facilitation payments, etc.

## Competition law/Antitrust law

Law that promotes or maintains market competition by regulating anticompetitive and unfair business practices conduct by organisations. Examples may include price fixing, excessive, predatory or discriminatory pricing, unfair trading terms, and tying (i.e., stipulating that a buyer wishing to purchase one product must also purchase all or some of his requirements for a second product).

## Cybercrime

Also known as computer crime; an economic offence committed using the computer and internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a by-product in order to create the fraud and only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one.

## Economic crime

The intentional use of deceit to deprive another of money, property or a legal right.

## Espionage

Espionage is the act or practice of spying or of using spies to obtain secret information.

## Financial loss/Financial terms

When estimating financial losses due to fraud, the participants should include both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to "loss of business opportunity".

## Fraud risk assessment

Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to specifically consider:

i. The fraud risks to which operations are exposed;

ii. An assessment of the most threatening risks (i.e., Evaluate risks for significance and likelihood of occurrence);

iii. Identification and evaluation of the controls (if any) that are in place to mitigate the key risks;

iv. Assessment of the general antifraud programmes and controls in an organisation; and

v. Actions to remedy any gaps in the controls.

## Human Resources fraud (recruitment and/or payroll fraud)

Fraud committed by members of the Human Resources department, including payroll fraud, ghost employees, pay-to-work, recruitment (i.e., hiring friends and/or relatives, hiring unqualified individuals, falsification of documents, etc.).

## Terminology (continued)

### Incentive/Pressure to perform

The individual has some financial problem that he/she is unable to solve through legitimate means so he/she begins to consider committing an illegal act as a way to solve the problem. The financial problem can be professional (e.g., job is in jeopardy) or personal (e.g., personal debt).

### Insider trading

Insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. Insider trading violations may also include 'tipping' such information, securities trading by the person 'tipped', and securities trading by those who misappropriate such information.

### IP infringement (including trademarks, patents, counterfeit products and services)

This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing them off as genuine.

### Markets with a high level of corruption risk

While corruption risk levels can be subjective, for the purposes of this survey we suggest a territory with a 2012 Transparency International Corruption Perception Index ("CPI") score of 50 or less be considered a market with a high level of corruption risk.

### Money laundering

Actions intended to legitimise the proceeds of crime by disguising their true origin.

### Mortgage fraud

Mortgage fraud schemes employ some type of material misstatement, misrepresentation, or omission relating to a real estate transaction which is relied on by one or more parties to the transaction.

### Opportunity or ability

The individual finds some way that he/she can use (abuse) his/her position of trust to solve the financial problem with a low perceived risk of getting caught.

### Procurement fraud

Illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to his organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation.

### Rationalisation

The individual finds a way to justify the crime to himself/herself in a way that makes it an acceptable or justifiable act.

### Tax fraud

An illegal practice where an organisation or corporation intentionally avoids paying its true tax liability.

**Forensic Services**
The PwC forensic services network is comprised of forensic accountants, economists, statisticians, former regulators and law enforcement, fraud examiners, and forensic technologists. We help organisations tackle the major financial and reputational risks associated with economic crime. We identify financial irregularities, analyse complex business issues, and mitigate the future risk of fraud.

# Contacts and contributors

## Survey Leadership and Editorial Board


**Steven Skalak**
Partner, United States
+1 (646) 471 5950
steven.skalak@us.pwc.com

**Darshan Patel**
Partner, India
+ 91 22 6689 1670
darshan.patel@in.pwc.com

**Alex Tan**
Executive Director, Malaysia
+60 (3) 2173 1338
alex.tan@my.pwc.com

**Claudia Nestler**
Partner, Germany
+49 (69) 9585 5552
claudia.nestler@de.pwc.com

**Ian Elliott**
Partner, United Kingdom
+44 (0)20 7213 1640
ian.elliott@uk.pwc.com

**Muniu Thoithi**
Director, Kenya
+254 (20) 285 5000
muniu.thoithi@ke.pwc.com

**Brian McGinley**
Partner, China
86 (10) 6533 2171
brian.mcginley@cn.pwc.com

**David Harley**
Principal, Australia
+61 (3) 8603 0166
david.j.harley@au.pwc.com

**Didier Lavion**
Principal, United States
+1 (646) 471 8440
didier.lavion@us.pwc.com


## Survey Management Team


**Matthew Curry**
Manager, United States
+1 (646) 415 2994
matthew.j.curry@us.pwc.com

**Kristof Wabl**
Manager, Austria
+43 (1) 501 88 2019
kristof.wabl@at.pwc.com


## Forensic Services Leaders


**Chris Barbee**
Partner, USA, Global Leader
+1 (267) 330 3020
chris.barbee@us.pwc.com

**John Donker**
Partner, Hong Kong, East Cluster Leader
+852 2289 2411
john.donker@hk.pwc.com

**Andrew Palmer**
Partner, United Kingdom, Central Cluster Leader
+44 (0) 20 7212 8656
andrew.palmer@uk.pwc.com

**Erik Skramstad**
Partner, USA, West Cluster Leader
+1 (617) 530 6156
erik.skramstad@us.pwc.com


## Survey Marketing Team


**Anjali Fehon**
Marketing Director, United States
+1 (973) 236 4310
anjali.t.fehon@us.pwc.com

**Shannon Schreibman**
Global Marketing Senior Manager, United States
+1 (845) 489 8473
shannon.schreibman@us.pwc.com

*www.pwc.com/crimesurvey*

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

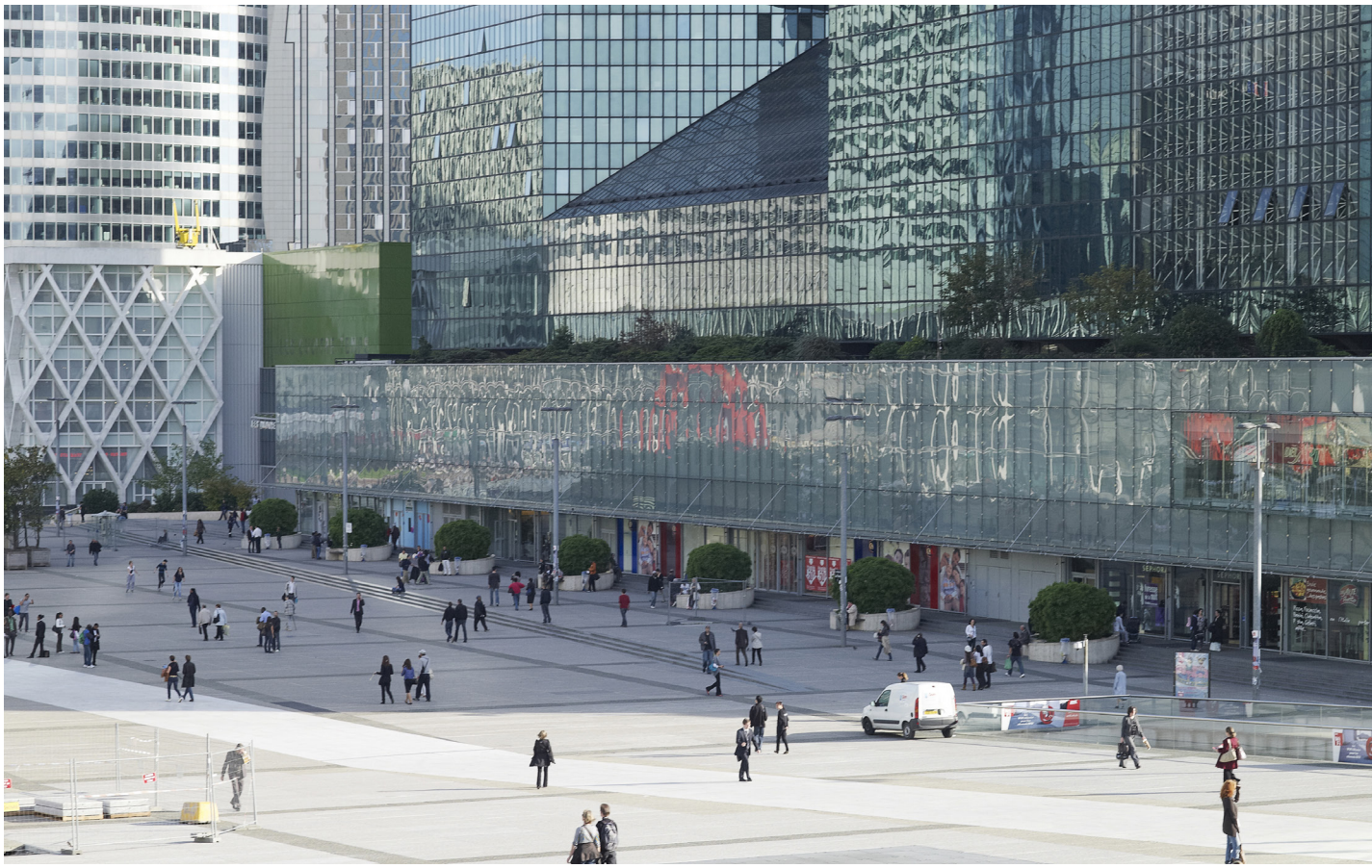
This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2014 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.

Designed by US Studio CMD NY-14-0348

*Financial Services sector analysis of PwC's 2014 Global Economic Crime Survey*

# *Threats to the Financial Services sector*



pwc

*www.pwc.com/crimesurvey*

# Contents

# *Key highlights*
## FS sector survey responses

**An attractive target…** 45% have suffered economic crime during the survey period compared to only 34% across all other industries.

**More than one way to lose…** The sector remains a key target for criminals and asset misappropriation is still the primary type of reported economic crime. Cybercrime, bribery and corruption appear to be increasingly common in the sector.

**Tone from the top…** 1 in 5 internally-perpetrated frauds still involve senior management, though the majority of such fraud tends to be committed by junior staff or middle management.

**Delusions of security…** Cybercrime risk appears to be increasing – however, risk awareness can differ greatly depending on an individual's role and function.

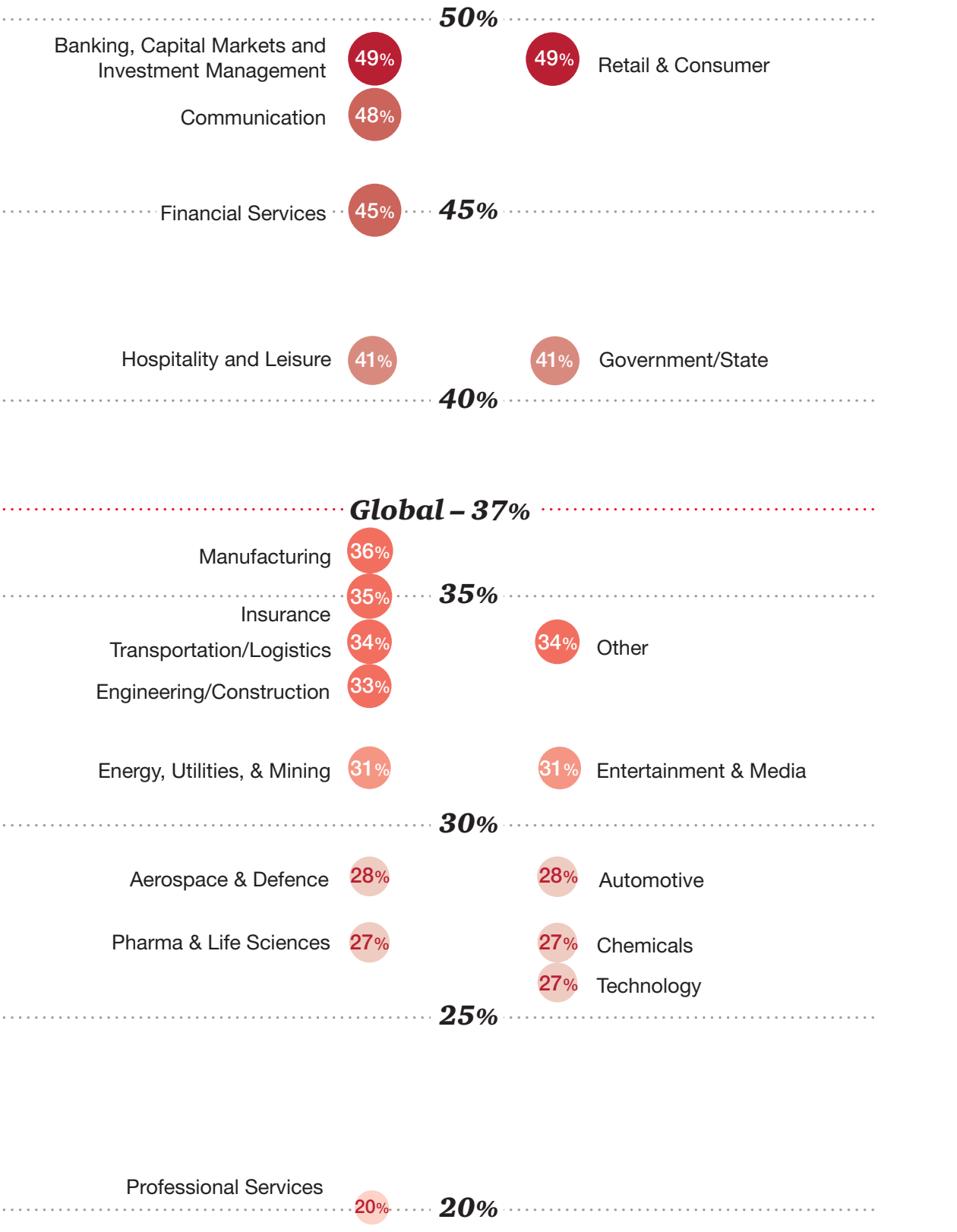
**Where the money's at…** Money laundering remains a hot topic in the FS sector, where it is almost five times more likely to occur than in other industries.

**Named and shamed…** FS organisations fear the fallout of being caught up in money laundering – almost 30% believed that the most severe impact is reputational.

**Telling…** Whistleblowing mechanisms appear to be more prevalent than before, however doubts remain over their effectiveness.

**Underestimating the risk…** 1 in 4 FS respondents failed to conduct annual fraud risk assessments. Over half of those who have not conducted any at all during the survey period are unaware of what these assessments involve or fail to see value in them.

**Fig 1 Economic crime percentage reported by industry**




*% of all respondents who experienced economic crime over the survey period*

The rate of economic crime reported by FS respondents is exceeded only by that in the Retail & Consumer and Communications sectors. Note that the proportion of Insurance-specific respondents who reported economic crime in our survey is lower than that of other Financial Services respondents – this is not unexpected given that other FS organisations such as banks are perceived to be where the money is and therefore more attractive for fraudsters.

# *Introduction*

***45% of Financial Services organisations have suffered economic crime during the survey period, compared to only 34% across all other industries.***

The Financial Services ("FS")[1] sector results from PwC's seventh Global Economic Crime Survey are the most comprehensive and intriguing to date.

There were 1,330 responses from the FS sector alone – 26% of the 5,128 responses received from all sectors.[2] FS respondents hailed from 79 different countries – making this FS sector report truly global[3] and representative of views on economic crime in its many guises, from fraud and cybercrime to money laundering and bribery and corruption.

Our survey questions were designed to assess corporate attitudes to economic crime in the current economic environment, the types of fraud encountered during the survey period, whether cybercrime is becoming more prevalent, and the extent of bribery andcorruption, money laundering and anti-competition experienced.

The FS sector results are intriguing because they often depart from the trends observed in other industries' results. In some areas they also continue to defy what might be expected of a sector that is heavily scrutinised and regulated globally. In this report, we shine the spotlight on the correlation between economic crime, corporate culture and individual behaviour in the FS sector and explain how the FS sector results demonstrate that many FS organisations need to improve their understanding of integrity and conduct risk threats.

The key message from our survey results is this: whilst the FS sector may be ahead of many industries in terms of prevention and detection of economic crime, more can and should be done by FS organisations. Of particular concern are the clear weaknesses in some organisations' fraud risk assessments, whistleblowing (or equivalent 'Speak up/Speak out') mechanisms and awareness of the pervasive and sustained threat of cybercrime.

Our survey findings are accompanied by action points for FS organisations if they wish to achieve or sustain 'best in class' practice.

1 Financial Services: Including retail and investment banking, insurance, investment management, stockbroking and private equity. The survey allowed respondents to identify as being from the "Insurance" sector separately from the "Financial Services" sector (as seen in Fig. 1). For this report, 'Financial Services' or FS shall refer to the combination of these respondents.

2 This compares to 3,877 responses in the 2011 survey – of which 878 (23%) were from the FS sector.

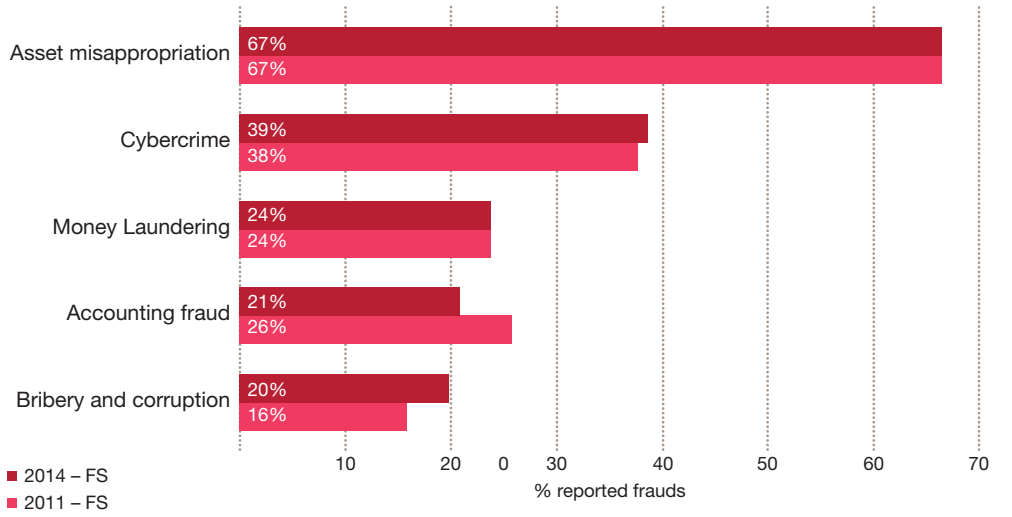
3 There were 79 countries represented in the FS sector responses – a significant (nearly 41%) increase from 56 countries in the 2011 survey.

# *Section 1 – FS economic crime today*
## Occurrences and value

Around half of the FS respondents who have experienced economic crime during the survey period report an increase in the number of occurrences and the financial value of economic crime during the period (more so than other industries' respondents). There are regional variations – in Asia Pacific at least half of FS respondents reported an increase; in contrast, nearly 40% of FS respondents from South & Central America reported a decrease.

### *The key threats*

**Fig 2: Top 5 types of economic crime experienced by the FS sector during the survey period**




Asset misappropriation remains the primary type of economic crime reported by FS organisations (67%) – not unexpected for a sector which processes money, and given the low cost of conversion for fraudsters. This is followed by cybercrime which is becoming more common, as is bribery and corruption. Only 1 in 5 experienced accounting fraud (compared to 1 in 4 previously) – we believe this is explained by improvements in corporate controls.[4]

Definitions of fraud vary, but mostly relate to obtaining financial or personal gain through wrongful deception. The key threats to the FS sector within the broad spectrum of economic crime range from more 'conventional' fraud (e.g. asset misappropriation) to money laundering by third parties.

4 Corporate controls: the suite of activities such as internal audit, fraud risk management, rotation of personnel and physical and IT security procedures undertaken in an organisation to monitor and address risks

## *Internal vs External*

External fraudsters are still the main perpetrators of economic crime for the majority of FS organisations (57% in 2014 and 60% in 2011).

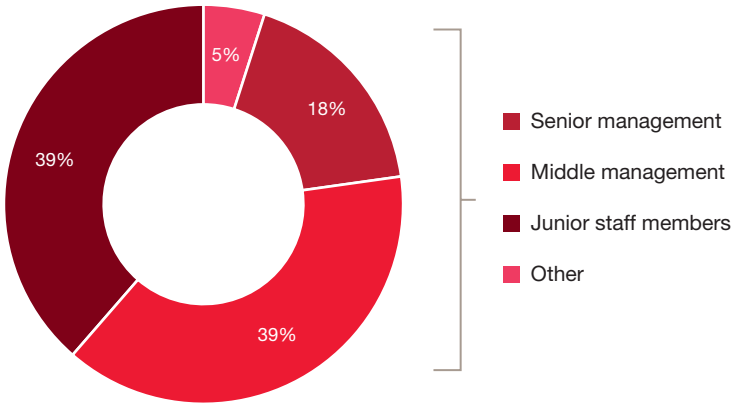
FS organisations are prime targets for external fraud given the amount of money fraudsters could potentially obtain and also the importance and sensitivity of data held by organisations (e.g. credit card and personal identity details). We note – and our FS respondents expect – that cybercrime is most often externally perpetrated and not just for monetary gain but also for valuable information about individuals. For instance, insurers may hold sensitive information and high-profile individuals' security details.

The FS sector also tends to be more strictly regulated and as a result many business processes and functions have corporate controls in place. This makes it more difficult for frauds to be internally perpetrated without discovery. To illustrate this – of the FS respondents who knew how the economic crime in their organisation had been detected, 61% attributed the detection to corporate controls in place compared to 56% in other industries.

## *Rank and profile*

After the economic downturn began in 2008, we saw in previous survey results that the involvement of senior management (whose primary motivation when committing fraud may be to alter performance and stock prices for their own bonus and other benefits) in FS economic crime increased by 50% from 12% in 2009 to 18% in 2011. The involvement of senior management remained at the same levels in 2014 (18%), suggesting that the response by regulators and governments to the financial crisis of imposing more rules and regulations has not sufficiently managed integrity or conduct risk i.e. the risk that people are not doing the right thing when no one is looking.

**Fig 3: Seniority of internal fraudsters in FS**




That said, most FS internal frauds are still committed by junior staff and middle management. In other industries, 64% of internal frauds are committed by middle or senior management, compared to 57% in the FS sector. Internal fraudsters in FS are also more likely to hold at least a university degree qualification than in other sectors, a reflection of the entry requirements of recruitment in the sector.

Our survey results suggest that the average FS internal fraudster is able to carry out fraud from quite a junior level in the organisation. This may be due to the fact that FS products are on the whole more complex by design and function, and consequently more difficult to 'police' (despite the corporate controls and monitoring in place).

Rather than accept these finding as 'status quo', FS organisations should explore what it means for their approach to fighting fraud:

- Is there sufficient emphasis on personal integrity and ethical behaviour?
- Are employees routinely encouraged to advance corporate and personal gain without regard to the impact of their behaviour on others?
- Is there evidence of how policies and procedures are actually deployed in day-to-day operations?
- Are ethical behaviours celebrated and poor behaviours penalised in a consistent, open and transparent way?
- Are employees encouraged to question the behaviour of others or ask questions in an open forum?

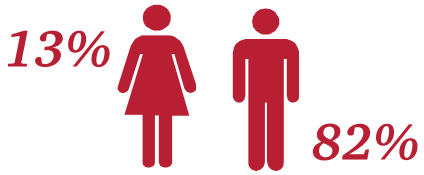
The sector is known for emphasising processes, rules and compliance – yet all too often, conformity can lead to wrongdoing if employees lack the training, incentives and support to question it.

## *Workforce diversity*

**FS respondents reported that the typical internal fraudster is likely to bebetween 31-50 years old.**

When asked about the most significant internal fraud experienced during the survey period, FS respondents reported that 82% were perpetrated by male fraudsters (an increase from 75% in 2011). The proportion perpetrated by female internal fraudsters has dropped (from 20% to 13%) in contrast to other industries which reported no material change in the proportion of internal frauds perpetrated by females. The remaining 5% of FS respondents did not confirm the gender of the fraudster.

Some studies on female representation suggest that the number of women in FS is in decline. The FS sector is less diverse than some other industries in terms of gender representation, and we see that reflected to some extent in the profile of the average internal fraudster.



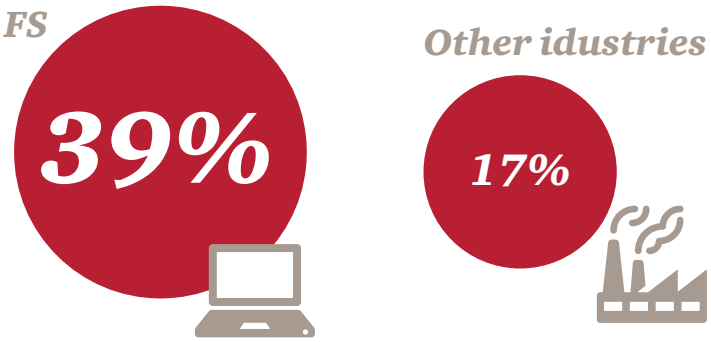

## *What can you do?*

- Define the organisation's strategic aspiration for ethical business conduct – ensure that a clear vision is set and that it is effectively communicated to all in the organisation.
- Assess the organisation's current integrity risk exposure (e.g. by conducting a gap analysis for misalignment between intended, expressed and actual behaviour) and define the risk tolerance level.
- Identify and address the drivers of undesirable behaviours within the organisation. For instance, review the organisation's recruitment policy and 'ethos', communication round risk and reward and other behavioural triggers.

# *Section 2 – Cybercrime*
## Not just an IT risk

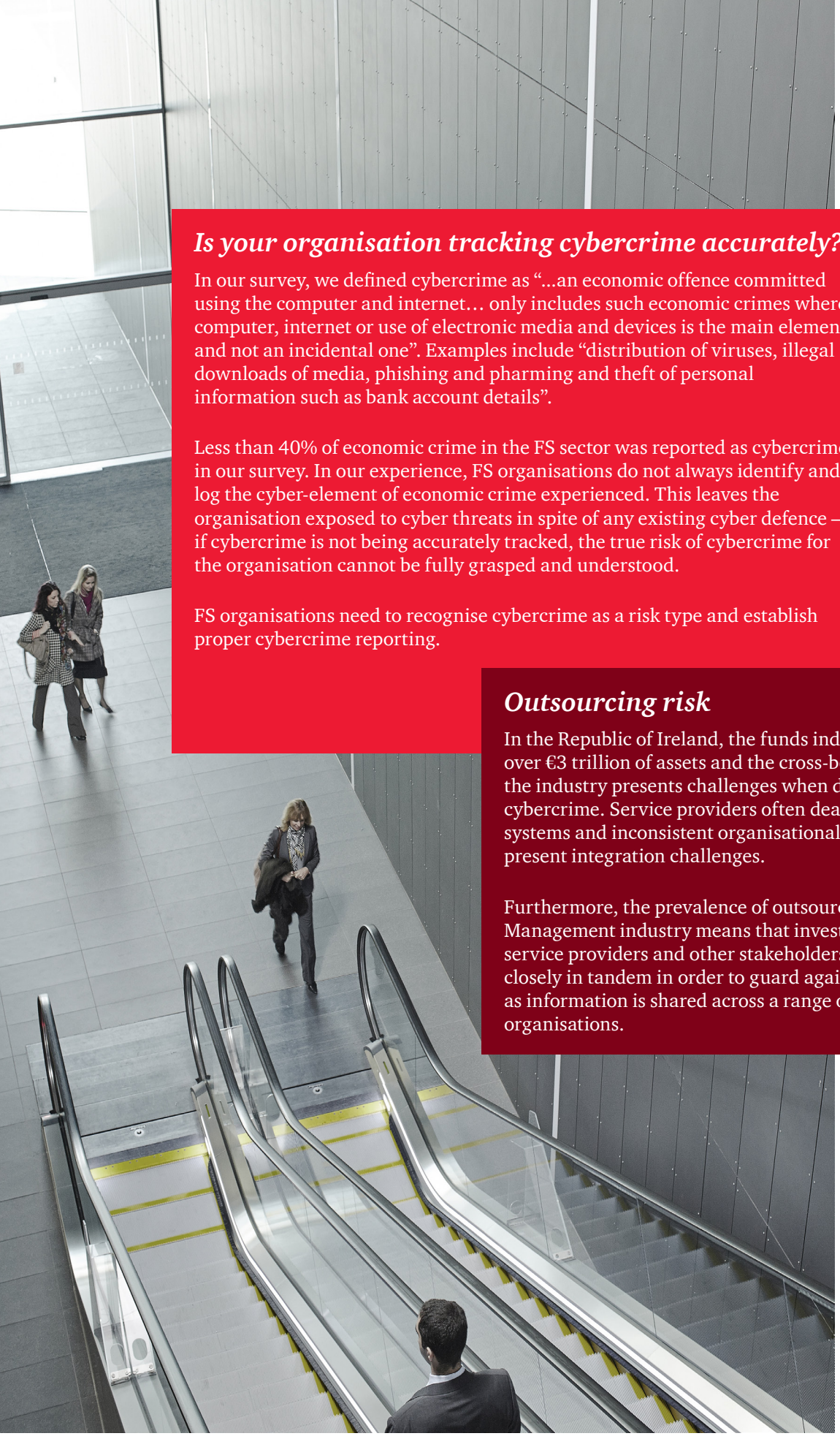
The FS sector was one of the first to be targeted by cybercrime – little wonder, as there have always been significant potential financial gains to be had from subverting computerised processes and corporate controls in banks.

Our survey shows that cybercrime is still the second most common type of economic crime reported by FS respondents (after asset misappropriation) – 38% in 2011 vs 39% in 2014 (this compares to only 16% in 2011 vs 17% in 2014 in other industries). However, we view this percentage of respondents as alarmingly low – our experience has shown that a clear majority of FS organisations (especially retail banks) suffered cybercrime during the survey period.




Similarly, only 41% of FS respondents believe it is likely that they will experience cybercrime in the next 24 months (including some 45% in Africa and36 % in Asia Pacific). This compares to 26% in other industries. A further 19% of FS respondents are unsure whether they are likely or unlikely to experience cybercrime.

FS respondents perceive a greater increase in the risk of cybercrime compared to counterparts in other industries (57% in FS vs 45% in other industries). In 2011, only half of FS respondents felt that the risk was increasing. Clearly, FS organisations believe that cybercrime is becoming a greater threat than ever before, and yet many do not believe that it will actually happen to them.



## *Is your organisation tracking cybercrime accurately?*

In our survey, we defined cybercrime as "...an economic offence committed using the computer and internet… only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one". Examples include "distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details".

Less than 40% of economic crime in the FS sector was reported as cybercrime in our survey. In our experience, FS organisations do not always identify and log the cyber-element of economic crime experienced. This leaves the organisation exposed to cyber threats in spite of any existing cyber defence – if cybercrime is not being accurately tracked, the true risk of cybercrime for the organisation cannot be fully grasped and understood.

FS organisations need to recognise cybercrime as a risk type and establish proper cybercrime reporting.

## *Outsourcing risk*

In the Republic of Ireland, the funds industry services over €3 trillion of assets and the cross-border nature of the industry presents challenges when dealing with cybercrime. Service providers often deal with multiple IT systems and inconsistent organisational processes, which present integration challenges.

Furthermore, the prevalence of outsourcing in the Asset Management industry means that investment managers, service providers and other stakeholders must work closely in tandem in order to guard against cybercrime, as information is shared across a range of systems and organisations.

## *Old tricks, new methods*

On one hand, certain cyber threats do ebb and flow – for instance, the Middle Eastern cyber attacks that targeted several large U.S. banks in 2012/13 appear to have receded. Overall some 5% of FS respondents said that their risk perception (of cybercrime) had decreased, and this could be due to the cessation of such previous high-profile incidents.

On the other hand, cybercrime is growing and the methods are constantly evolving – we see no abatement in attacks on banks' infrastructure. Some recent attacks have installed hardware in bank branch systems to enable transactions to be manipulated via mobile networks. The U.S. has seen dramatic increases in FS economic crime – from outages created by Distributed Denial of Service (DDOS) attacks to massive ATM withdrawals effected by organised criminal groups. Credit card fraud has become more pervasive as the U.S. has yet to embrace the Chip and PIN system. In Japan, phishing scams have targeted bank customers' personal computers via virus, using fake pop-up windows or e-mails masquerading as legitimate internet banking interfaces to trick customers into inputting their personal information.

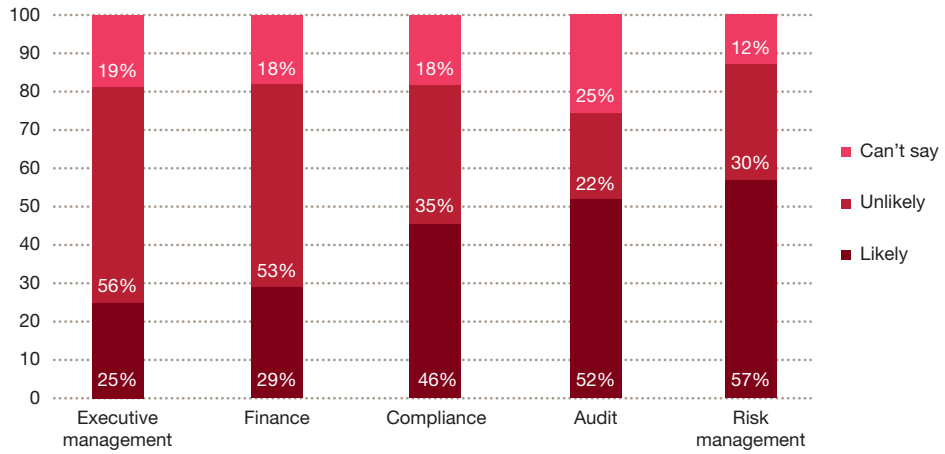
The landscape of cybercrime is also changing in a literal sense. For instance, our cybersecurity experts have perceived a rise in cybercrime from Africa, which correlates with big government initiatives to roll out broadband in that region. Industry sources also indicate that cybercriminals are relocating to South Africa from Europe (due to increased co-operation between law enforcement agencies in the EU).

## *Varying awareness of cybercrime*

It is concerning that 40%of all FS respondents believe that it is unlikely their organisations will experience cybercrime in the next 24 months. When we delved into the responses by respondent roles, an alarming 54% of CEO (or equivalent) and 49% of CFO (or equivalent) respondents declared that it is unlikely. 1 in 5 CEOs were unable to conclude whether it was likely or unlikely. And yet, cyber insecurity is seen as a key threat by CEOs – results from PwC's 17th Global CEO Survey show that more than 70% of Banking & Capital Markets CEOs see cyber insecurity as a threat to growth, more than any other sector.

There is a stark disconnect in the perception of cybercrime risk within FS organisations.FS respondents from the internal audit, compliance and risk functions thought it was more likely than unlikely that their organisations would experience cybercrime whilst the opposite was true for finance and executive management FS respondents.

**Fig 4: "Is your FS organisation likely to experience cybercrime in the next 2 years?"**



Clearly there is a mix of views amongst C-suite respondents, with CEOs and CFOs on the whole appearing less aware of the likelihood of cybercrime occurring in their organisation. It may be that within some FS organisations, cybercrime has not been materially reported to C-suite attention.

While the more risk-focussed functions like internal audit, compliance and risk management show greater awareness of the risk, a worrying percentage of respondents from those functions still conclude that cybercrime is unlikely.

It is widely recognised that the FS sector is very much at the forefront of fighting cybercrime. However, our survey results suggest that complacency still exists heavily within FS organisations – perhaps management feel comfortable that their organisations have better cybersecurity defences than ever before, without realising that threats are usually one step ahead. Or perhaps certain functions (including finance) still tend to perceive cybersecurity as more of an IT issue (rather than a significant business risk).

> ***"Today's incidents, yesterday's strategies – As the digital channel in financial services continues to evolve, cybersecurity has become a business risk, rather than simply a technical risk"***
>
> The Global State of Information Security® Survey (an annual, worldwide study by PwC, CIO magazine, and CSO magazine)

FS respondents should be aware that their organisations are increasingly likely to suffer cyber attacks regardless of whether proper defences are in place. When the findings above are linked up with survey results around fraud risk assessment (see further below), there is a sense that FS organisations still fail to see the importance of establishing fundamental IT security objectives and linking those with business objectives and risks.

## *Regulators fight back*

Meanwhile, regulators around the world are waking up to the fact that cybercrime poses systemic danger, especially when retail and commercial banks are concerned. FS organisations are custodians of monetary assets and sensitive information for companies and individuals in other industries, meaning the effects of cybercrime in the FS sector are seldom contained to FS organisations alone.

## *Regulatory pressure on cyber threats*

In the UK, the Bank of England has declared cybercrime a major risk to the FS sector and, along with other FS regulators in the UK, co-ordinated a major cyber attack in November 2013 to 'stress test' UK banks in an exercise known as 'Waking Shark II'. The Bank's report on this exercise cited a need both for greater co-ordination within the sector and for educating firms about the need to report major incidents to regulators. In the same month, the New York State Department announced that it would require the banks under its regulation to answer questions in a real-time online test in order to assess their cybersecurity policies and processes.

Additionally in the U.S., regulators have increased the visibility of cybercrime by requiring cyber incidents which have had material impact to be disclosed in registered public company filings. Several large FS organisations have thus been prompted to disclose within their 10K filings with the SEC that they have been targeted by cyber attacks.

Even in Lebanon, where online banking activities are less developed and banks therefore do not perceive the cybercrime risk as material, significant losses from cybercrime in the FS sector have emerged. The Banking Control Commission of Lebanon has initiated reviews of IT security in banks with a view to strengthening cyber defences.

Knowledge is power – FS organisations have been co-ordinating to share threat intelligence for years. Collaborating to share cyber threat data helps organisations deal quickly and proactively with cybercrime. In Luxembourg, where the FS sector is dominant, such collaboration is of strategic importance to the economy at large.

The largest FS organisations are also catching on to the need to deter (rather than just detect) cybercrime. At least one large global bank has established a zero-tolerance policy to combat all online banking fraud, regardless of materiality.

## *What can you do?*

- Educate employees at all levels (from C-suite to junior management) about cyber threats – cybercrime is not just the domain of the IT/network security function. There are different types of cybercrime, from hacktivism to data theft, which affect different functions of the bank in varying ways.
- Understand the potential culprits and their motivations to engage in a cyber attack on the organisation.
- Ensure that key fundamental safeguards for effective cyber security are in place – including ongoing monitoring, up-to-date personal or sensitive data inventory, a back-up policy and business continuity plans.
- Continue to engage with regulators to understand what other peer organisations are doing to counter cybercrime and adopt 'best in class' practices.
- Separate out the gross and net financial loss due to cybercrime for the FS organisation and report to executive management as meaningful indicators of activity and recovery levels.

# *Section 3 – Fraud*
## More than one way to lose

The FS sector is particularly exposed to certain types of economic crime (such as money laundering) and faces unique regulatory challenges as a result.

### *Money laundering*

Money laundering continues to be a hot topic in the FS sector. It is also distinct from other types of economic crime in that an FS organisation does not suffer direct financial loss through money laundering – instead, the effects are felt through a loss of reputation (in the eyes of both the public and the regulator), and increasingly compounded by colossal regulatory fines. At least 50% of FS respondents in Western Europe and Africa selected money laundering as their highest risk in doing business globally, compared to bribery andcorruption and anti-competition law.

Our survey showed that money laundering ranked next behind asset misappropriation and cybercrime in the types of economic crime experienced by FS organisations. It is almost five times as likely to occur in the FS sector compared to other industries.

FS organisations reported feeling particularly concerned about the impact of money laundering on their reputation (more so than operational disruptions or financial loss). Their focus on corporate reputation is in line with expectations given that many banks have had adverse press coverage regarding their Anti-Money Laundering ("AML") breaches.


***of FS respondents felt that the most severe impact of money laundering is on their organisation's reputation***

In the past few years, enforcement action across the globe has crystallised regulatory expectations in the AML space. The challenge for global FS organisations is how best to utilise Know Your Customer (KYC) information across the organisation, particularly in relation to customers that have multiple touch points with the organisation across more than one business unit and several jurisdictions. Regulators have made it clear that they expect institutions to have a consolidated picture of the client relationship, regardless of limitations presented by legacy IT systems and complexities of cross-border data privacy legislation.

There is a growing realisation that FS organisations need to invest in AML technologies in order to ensure they are operating as expected. The Financial Action Task Force (the inter-governmental body which sets AML standards) has recently indicated that its focus is shifting away from whether FS organisations can demonstrate compliance with AML requirements, to whether the AML arrangements in place are actually effective.

## *AML on the back foot*

**Many banks continue to struggle with AML remediation due to the size and complexity of their operations and customer base. Regulatory authorities – including central banks from Ireland to Israel – continue to push for greater accountability, creating challenges ahead.**

Regulators ranging from the UK's Financial Conduct Authority ("FCA") to Malaysia's Bank Negara Malaysia have recently published thematic reviews on financial institutions' AML systems and controls. The FCA's thematic review TR13/9 for Asset Management and Platform Firms sets out examples of 'good' and 'poor' practice, and also made the following comment on senior management oversight:

"We identified examples of recurring issues being reported to management committees, with no clear ownership for the closure and resolution of those issues, leading to a 'reactive' approach in managing money laundering and bribery and corruption risks. Some firms' senior management could not clearly articulate their money laundering and bribery and corruption risk management arrangements."

In South Africa, financial intelligence units were first established in the 1980s to identify and combat the laundering of illegal drug trade proceeds. Today, a much broader effort is under way – the Financial Intelligence Centre (FIC) monitors activity by globalised criminal syndicates operating in and through the country, large scale corruption and the influence of Politically Exposed Persons in the private sector, amongst other things. The FIC is increasingly confronted with the challenge of "big data" analysis and will need further investment in technology systems capable of handling massive data volumes and analytical functions.

### *What can you do?*

- Ensure that 'Know Your Customer' (KYC) procedures and Anti-Money Laundering processes are operating effectively across a 'single customer view' – making sure all relevant systems and records are joined up for consistency of data.
- Resolve legacy IT issues in order to keep pace with regulatory requirements and new tactics of money laundering syndicates.

## *Dealing with bribery and corruption abroad*

Of the FS organisations surveyed, 47% currently have operations in a market with high corruption risk.[5] At the same time, for each associated economic crime like bribery and corruption, money laundering and anti-competition law, around 40% of FS respondents were unable to provide an estimate of the financial loss suffered as a result.

Our survey results show that such risks remain hard to quantify in terms of financial loss. The results also indicate that FS organisations have not fully come to grips with the risks of operating in such territories. Regulators continue to take a strict view on money laundering, bribery and corruption – focusing on the corporate as well as the individual. In the UK, the Bribery Act emphasises personal liability ofboard members, while the 2013 Financial Services Act places the burden of proof on the individual (to demonstrate that reasonable steps have been taken to avoid bribery and corruption).

### *A number of forward-thinking FS organisations are seeking to get ahead of the pack.*

We recently worked with a global investment bank and with the cooperation of several peer organisations (competitors) sought to benchmark their anti-bribery, corruption and fraud management. This gave the FS organisation an external, objective view of their organisational structure and how roles, resources and areas of responsibility were geared towards dealing with such risks and incidents.

FS organisations need to remain wary of who they are "getting into bed with" in emerging markets. In June 2013, the U.S. Department of Justice announced that it had arrested the managing partner of a U.S. broker-dealer on felony charges arising from a conspiracy to pay bribes to a senior official in a South American state-owned economic development bank. More recently, certain global banks have come under investigation from UK and U.S. regulators for potential bribery and corruption due to their practice of making high-profile government-linked hires in Asia. While such occurrences are common among local entities, many foreign regulators may have a different view on such matters. It is far better for FS organisations to take a circumspect and informed approach to operating in emerging markets than to fall foul of regulators after the event – especially as recent regulatory releases and press reports seem to suggest that the FS sector is beginning to experience increased regulatory scrutiny with regards to the U.S. Foreign Corrupt Practices Act (FCPA) and other similar areas of compliance.

### *What can you do?*

- Carry out risk assessments for fraud, bribery and corruption in order to identify ways of improving the effectiveness of fraud detection mechanisms as well as to mitigate the risk of regulatory breach when operating in a territory with heightened corruption risk.
- Implement comprehensive due diligence programmes on third parties which would help to highlight potential "red flags" indicating vulnerability to bribery or corruption. These red flags may include issues such as engagement with Politically Exposed Persons, negative references in media or involvement in litigation.

5 Territory with high corruption risk is defined as one with a 2012 CPI score below 50 http://www.transparency.org/cpi2012/results

## *Whistleblowing – improving but underused and underrated*

Whistleblowing mechanisms remain underused in the FS sector. We attribute this in part to the greater dependencies placed on process-type detection methods in the industry – which may encourage complacency and diminish the perceived need for personal integrity and responsibility to come to the fore.Alternatively, it could be because whistleblowing does tend to be a 'last resort' option for employees to report concerns and issues.

Our survey shows significant improvement in some areas – only 19% of the FS respondents confirmed a complete lack of whistleblowing mechanism in place at their organisations (compared to 45% of the FS sector in 2011). Of those who do have a whistleblowing mechanism in place, over 1 in 2 (53%) reported effective or very effective whistleblowing mechanisms according to respondents – compared to 27% in 2011. However, doubts over the effectiveness of whistleblowing policies still remain – 16% still don't know whether their whistleblowing mechanism is effective or not. And a further 7% of FS respondents believe it is ineffective – including 10% from Western Europe and 6% from Asia Pacific and Africa.

In fact, tip-offs and whistleblowing helped to uncover only 16% of the most significant economic crime detected, compared to corporate controls which accounted for 57%. In other industries, tip-offs and whistleblowing helped to uncover 26% of economic crime.

### *A cautionary tale*

The LIBOR scandal has highlighted competition law violations that also saw individual employees from different banks implicated in wrongdoing, putting in the spotlight the need for whistleblowers to 'lift the lid' on malpractice and fraudulent behaviour.

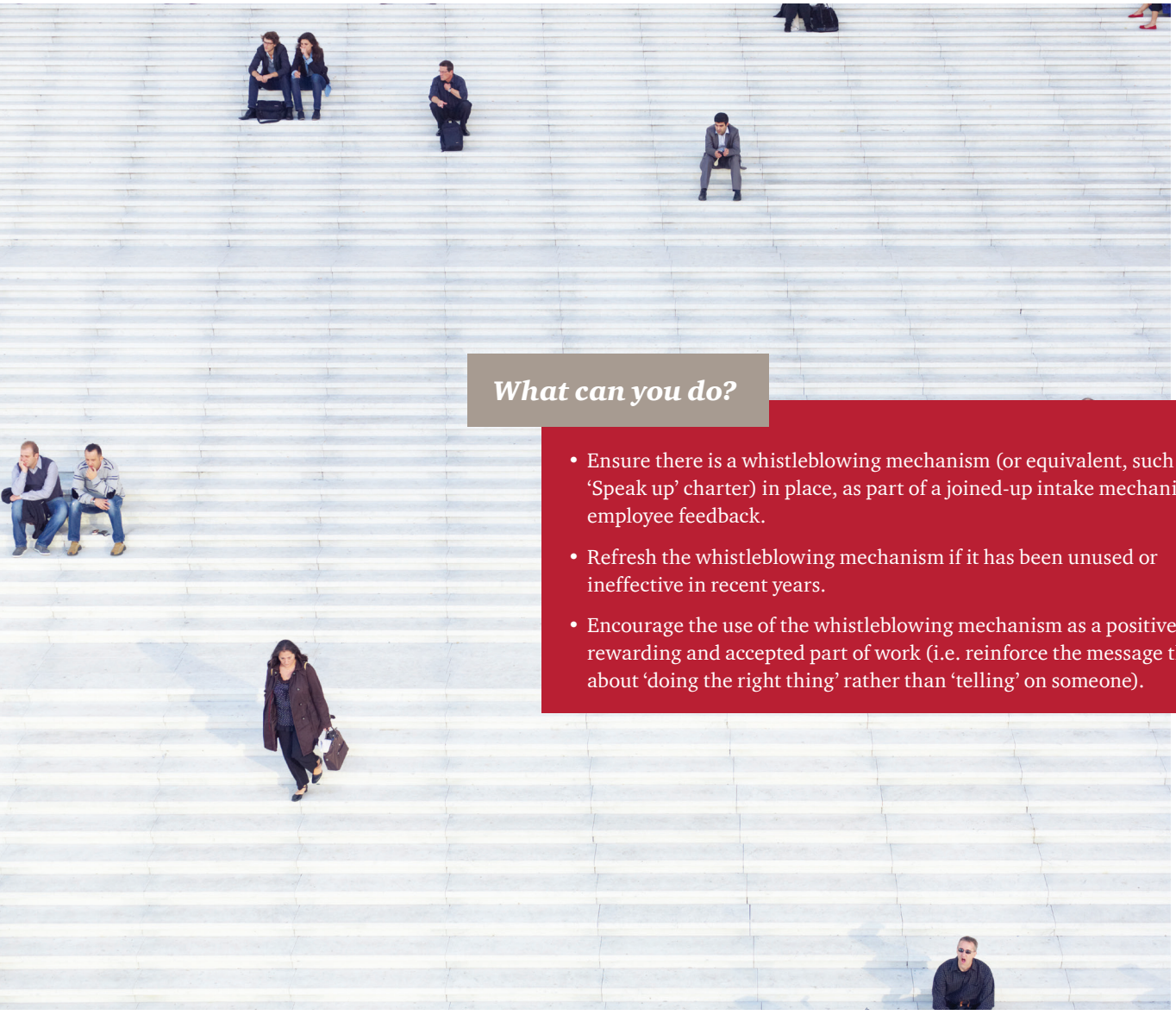
It is not enough to encourage the use of the whistleblowing mechanism if, as in the LIBOR case, employees are not encouraged to also challenge social conformity. It appears that many employees had not even realised or acknowledged that LIBOR manipulation equated to wrongdoing. A change in tone-from-the-top needs to take place in some FS organisations. Many banks have seen their reputation and public trust eroded in recent years; there needs to be a stronger culture of 'doing the right thing'.

Senior management need to lead from the front in this area, especially as accountability is now more heavily scrutinised by the regulators and potential criminal sanctions could be imposed if accountability is established.

Some FS regulators have taken significant measures to encourage whistleblowing. For example, people who provide original information that leads to a successful SEC enforcement action could be rewarded with a share of any sanction collected over $1m and a share of proceeds from any related regulatory action. In 2012, a former UBS banker was paid $104m by the U.S. Internal Revenue Service for revealing a tax evasion scheme. And in Germany, it has become a formal legal requirement for financial institutions to have an appropriate whistleblowing process (the effectiveness and appropriateness of which is subject to annual audit).

The magnitude of financial rewards available is being called into question by those worried about its distortionary effects on employee behaviour. It remains to be seen whether whistleblowing mechanisms will be abused as a result. Furthermore, whistleblowing is not seen as positive behaviour in certain territories for historical and cultural reasons. FS organisations may need to reflect on how whistleblowing concerns and outcomes are fed back into the business, as well as on the visibility of any such output, and ensure that the whistleblowing mechanism is sufficiently joined up with other feedback processes in the organisation.

On the whole, FS regulators are emphasising recognition of positive whistleblowing behaviour. A balanced approach is required - financial incentives and positive recognition need to be coupled with penalties for clear misuse of the whistleblowing mechanism. Moreover, employees should be empowered to identify and report issues before matters escalate to a stage where whistleblowing remains the only way forward.



### *What can you do?*

- Ensure there is a whistleblowing mechanism (or equivalent, such as a 'Speak up' charter) in place, as part of a joined-up intake mechanism for employee feedback.
- Refresh the whistleblowing mechanism if it has been unused or ineffective in recent years.
- Encourage the use of the whistleblowing mechanism as a positive, rewarding and accepted part of work (i.e. reinforce the message that it is about 'doing the right thing' rather than 'telling' on someone).

## *Fraud risk assessment*

In certain jurisdictions, FS regulatory requirements exist for risk areas like money laundering and fraud. Our survey asked about fraud risk assessments ("FRAs") and the results reveal a surprising number of FS organisations still do not carry any out. It is possible that if FRAs took place more regularly additional economic crime would have been detected. Other economic crime areas such as bribery, corruption and money laundering also benefit from thorough enterprise-wide risk assessments.

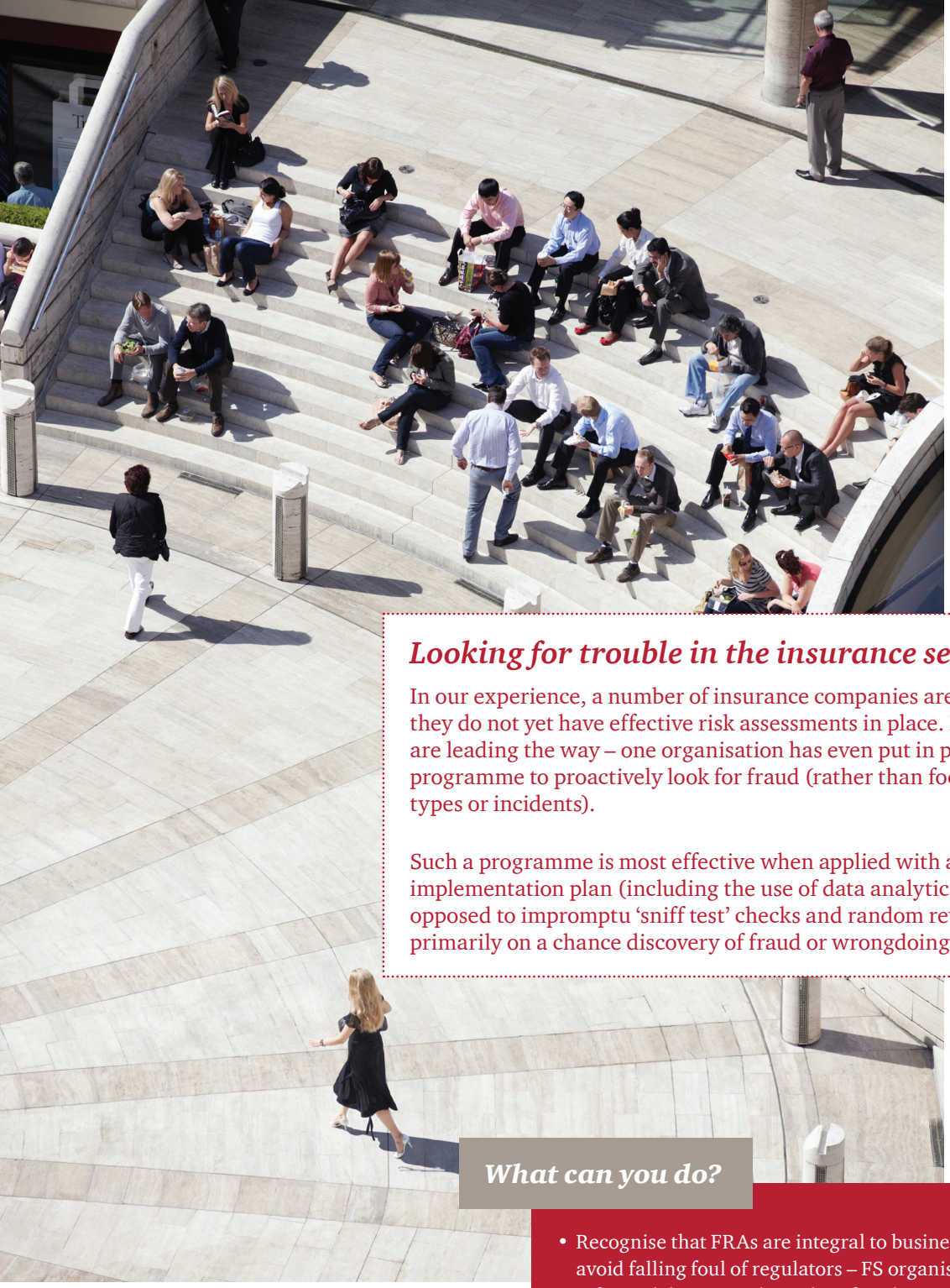
The percentage of FS respondents whose organisations did not perform annual FRAs has increased from 18% to 25%, This appears to be better than other industries (where 43% do not have annual FRAs), but is considered to be relatively high taking into account that FS regulators tend to expect or even fully require such a risk assessment in many jurisdictions.

A further 12% of FS respondents do not know whether any FRAs were performed in their organisation during the survey period. When asked why, 32% noted they did not know what an FRA involves (compared to 30% in other industries in 2014, 36% of FS respondents in 2011). Another 27% perceived a lack of value in FRAs.

It appears that over 50% of respondents from FS organisations that did not carry out any FRAs during the survey period fail to see the correlation between fraud, working conditions, organisational culture and the effectiveness of corporate controls. And yet, almost one in all 5 serious frauds was detected by Fraud Risk Management ("FRM"). FRM remains the most effective method in fraud detection (17% of serious frauds experienced by FS respondents were detected this way). Only 13% of frauds were detected through suspicious transaction reporting (compared to 19% in 2011). 6% were detected through data analytics (an option not offered in the 2011 survey) – which is likely to become a more important detection tool in the future. Surprisingly,1 in 5 FS respondents did not confirm a method of fraud detection ("Don't know") compared to only 8% in 2011.

**Fig 5: Economic crime detection methods in FS organisations**


% FS respondents



## *Looking for trouble in the insurance sector*

In our experience, a number of insurance companies are starting to realise that they do not yet have effective risk assessments in place. However, some insurers are leading the way – one organisation has even put in place a fraud detection programme to proactively look for fraud (rather than focussing on specific known types or incidents).

Such a programme is most effective when applied with a clear methodology and implementation plan (including the use of data analytics if appropriate), as opposed to impromptu 'sniff test' checks and random reviews which seek to rely primarily on a chance discovery of fraud or wrongdoing.

### *What can you do?*

- Recognise that FRAs are integral to business and often necessary to avoid falling foul of regulators – FS organisations need to be making informed decisions about their fraud prevention and detection mechanisms.
- Consider new ways of fraud detection – data analytics capabilities are helping FS organisations identify fraud based on 'outlier' criteria (e.g. unlikely transaction or payment dates).

# Contacts

For more information on the Global Economic Crime Survey and the survey methodology, please refer to Economic crime: A threat to business globally at www.pwc.com/crimesurvey.

If you would like to find out more about the information contained within this report, or to discuss any issues around economic crime and how our team can help you, please get in touch with your local PwC contact or the sector report team:

## Contact team

**Andrew Clark (Sector report lead partner)**
+44 (0) 20 7804 5761
andrew.p.clark@uk.pwc.com

**Tien Tien Tan (Sector report project manager)**
+44 (0)20 7212 1133
tien.tien.t.tan@uk.pwc.com

## Forensic Service Leaders

**Chris Barbee**
Partner, USA, Global Leader
+1 (267) 330 3020
chris.barbee@us.pwc.com

**John Donker**
Partner, Hong Kong, East Cluster Leader
+852 2289 2411
john.donker@hk.pwc.com

**Andrew Palmer**
Partner, United Kingdom, Central Cluster Leader
+44 (0) 20 7212 8656
andrew.palmer@uk.pwc.com

**Erik Skramstad**
Partner, USA, West Cluster Leader
+1 (617) 530 6156
erik.skramstad@us.pwc.com

## Editorial team acknowledgements

In preparing this report, assistance was gratefully received from PwC teams in Germany, the Republic of Ireland, Israel, Lebanon, Qatar, Luxembourg, Malaysia, New Zealand, Nigeria, South Africa, the United Kingdom and the U.S.

## *Forensic Services*

The PwC forensic services network is comprised of forensic accountants, economists, statisticians, former regulators and law enforcement, fraud examiners, forensic technologists and corporate intelligence specialists. We help organisations tackle the major financial and reputational risks associated with economic crime. We identify financial irregularities, analyse complex business issues, and mitigate the future risk of fraud.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2014 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

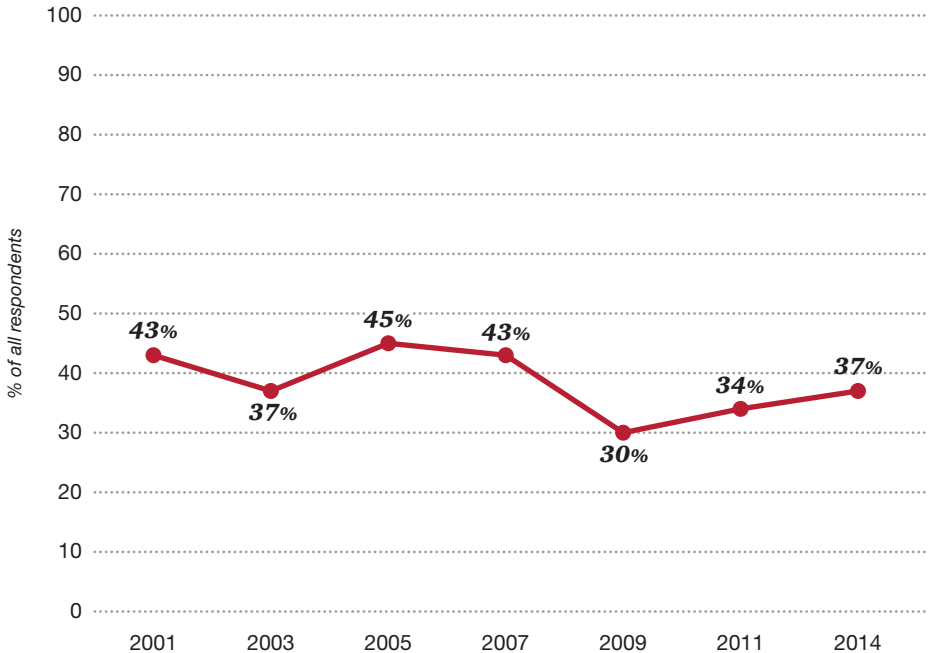
The Design Group 21991 (02/14)

*Economic crime threatens a wide variety of business processes, including:*

**Figure 1: Business processes threatened by economic crime**

| | |
|---|---|
| • Sales (or selling) | • Customer "on-boarding" |
| • Marketing | • International expansion |
| • Bidding | • Tax compliance |
| • Procurement | • Facilities construction, leasing and operations |
| • Payments | • Hiring and recruiting |
| • Vendor selection | • Suspicious transaction reporting |
| • Distribution | • IP development and deployment |
| • Logistics | • Data security and privacy |
| • Access to commodities and resources | • IT network operations |
| • Supply chain operations | • Employee expense reimbursement |

## Figure 2: Evolution of reported rate of economic crime (GECS)



## Figure 3: Types of economic crime reported

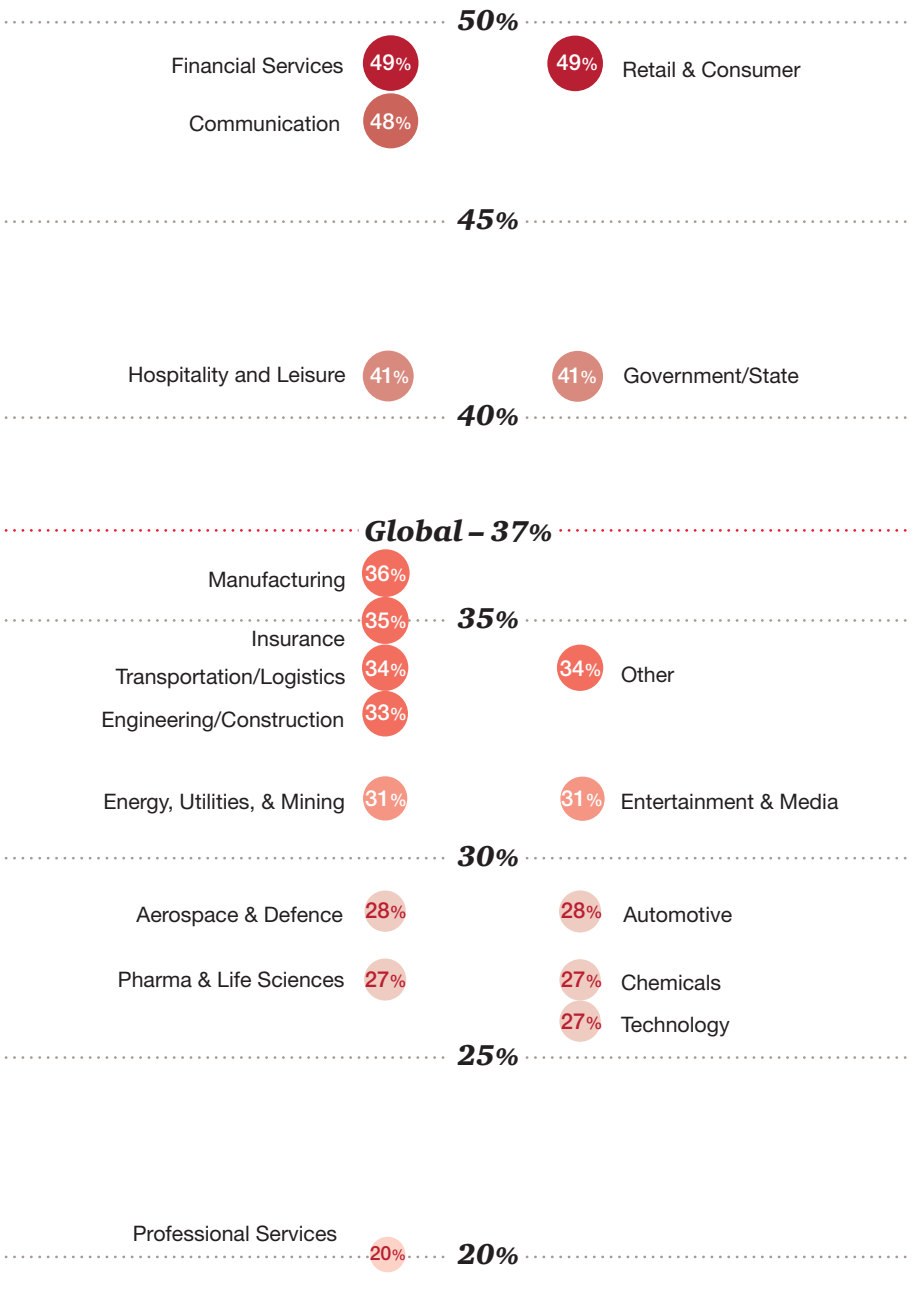

*% of all respondents who experienced economic crime over the survey period*

## Figure 4: Economic crime reported by region

| Territory | Reported Fraud 2014 | Reported Fraud 2011 |
|---|---|---|
| Africa | 50% | 59% |
| North America | 41% | 42% |
| Eastern Europe | 39% | 30% |
| Latin America | 35% | 37% |
| Western Europe | 35% | 30% |
| Asia Pacific | 32% | 31% |
| Middle East | 21% | 28% |
| Emerging Eight* | 40% | 35% |
| **Global** | **37%** | **34%** |

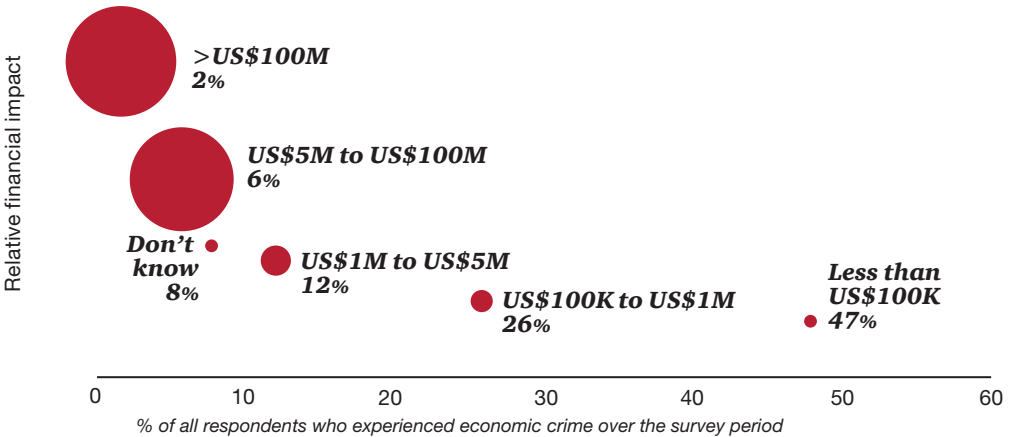
**Emerging Eight include Brazil, China, India, Indonesia, Mexico, Russia, Turkey, and South Africa*

## Figure 5: Economic crime reported by industry

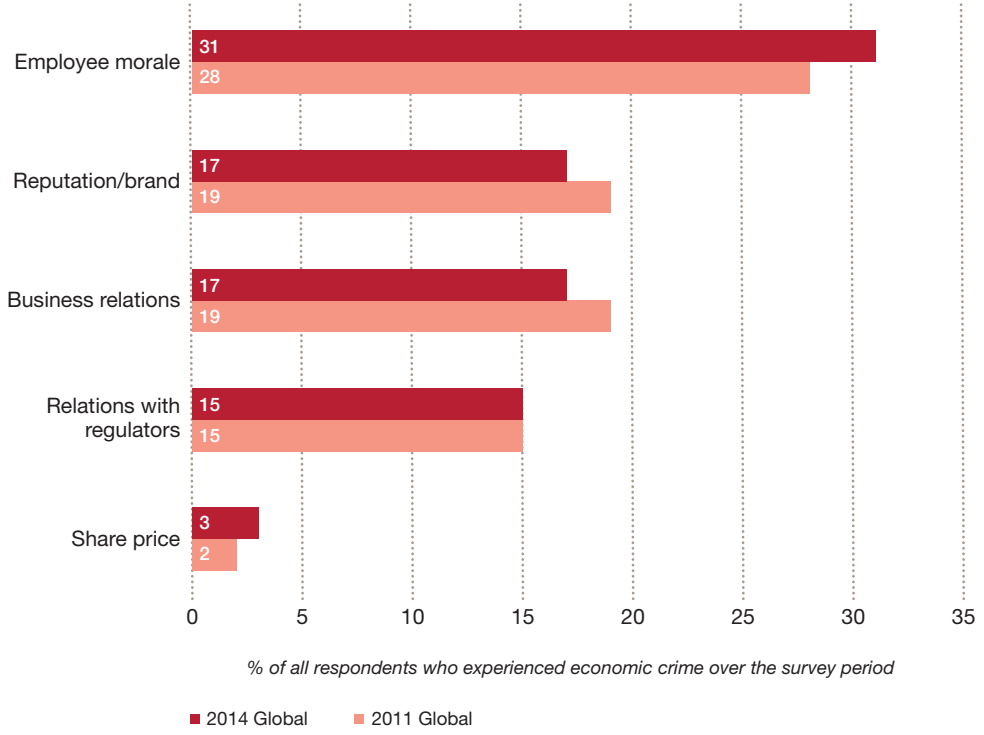



*% of all respondents who experienced economic crime over the survey period*

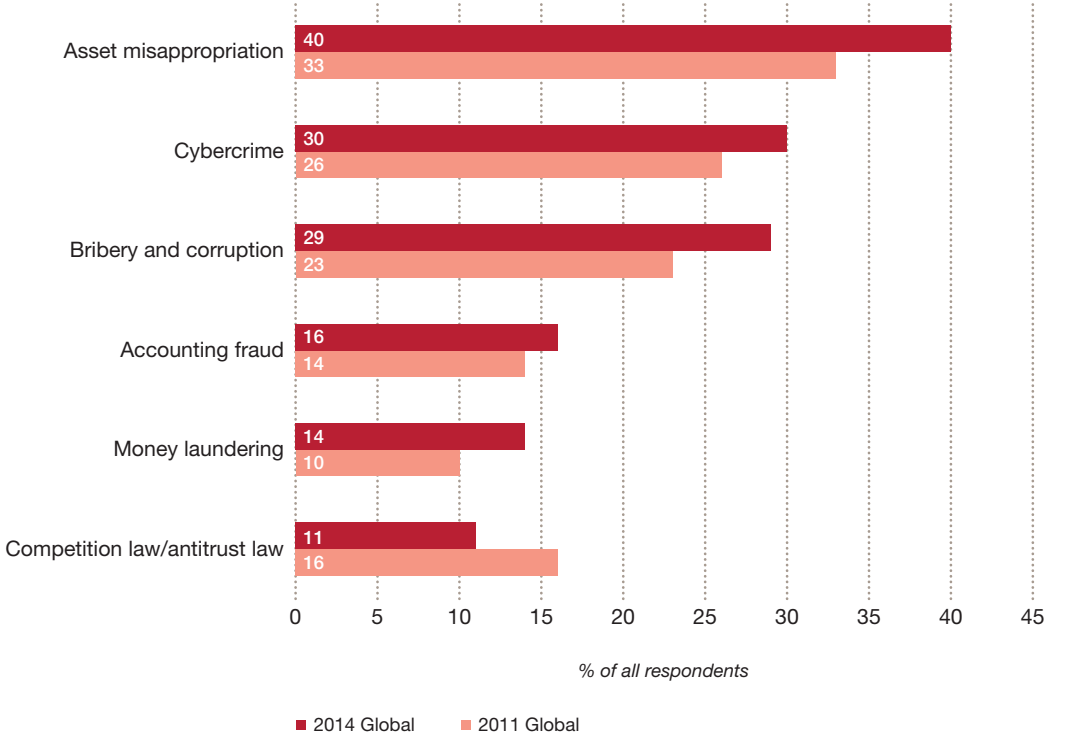
## Figure 6: Relative financial impact of economic crime on organisations



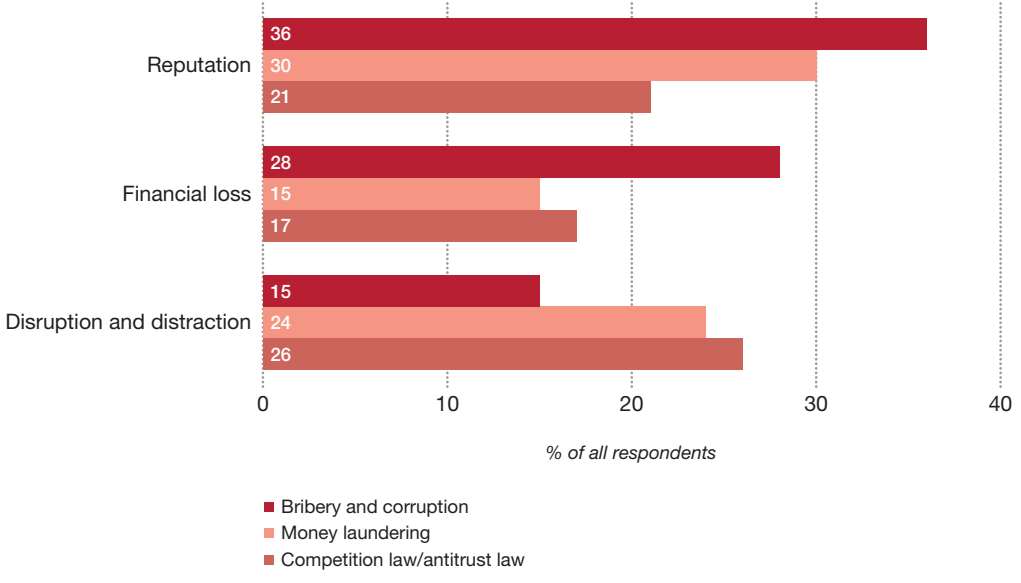
## Figure 7: Collateral effects of economic crime



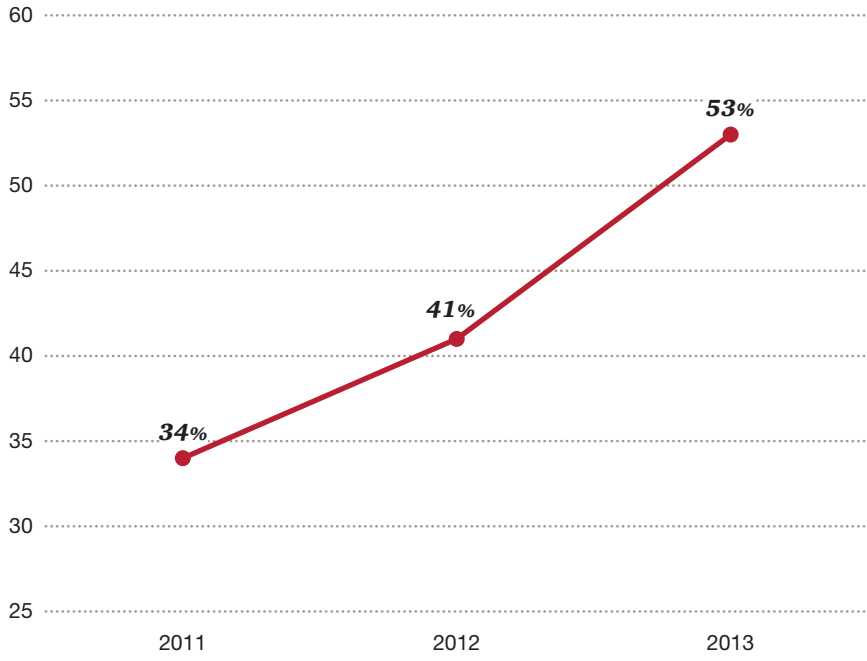
## Figure 8: Trends in expectations of economic crime



## Figure 9: Perceived most severe impact, by highlighted economic crime



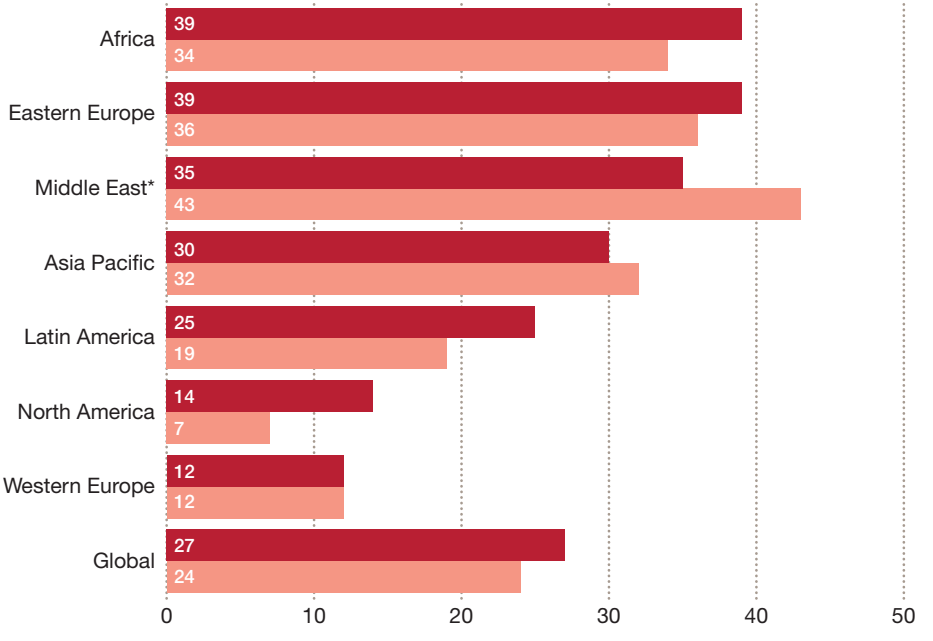
## Figure 10: Rising CEO concern regarding bribery and corruption




*% of all respondents in PwC's Annual Global CEO Survey*

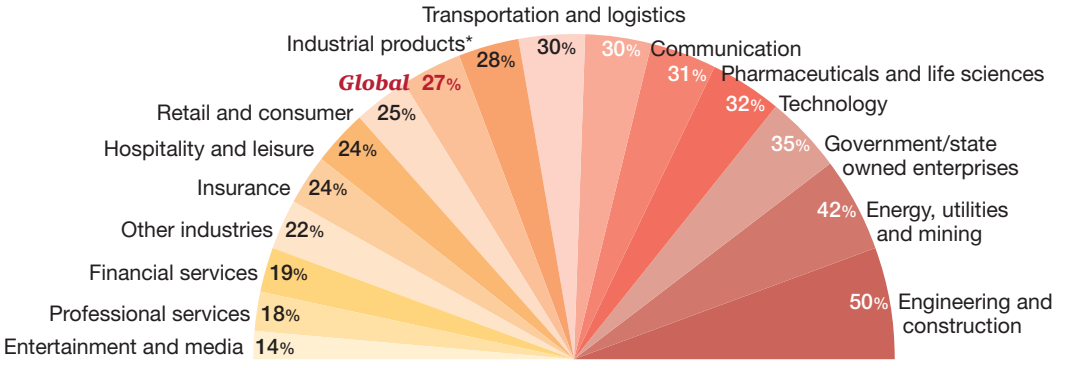
## Figure 11: Losses over US$5M considering bribery and corruption, by company size

## Figure 12: Reported bribery and corruption, by region



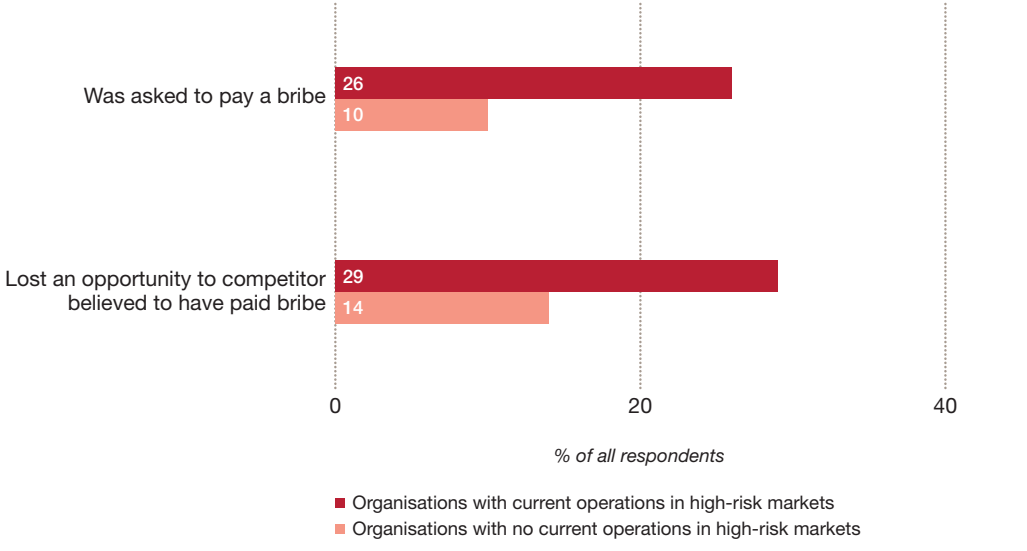

*Middle East was included in the "Asia Pacific" region in 2011

## Figure 13: Reported bribery and corruption, by industry

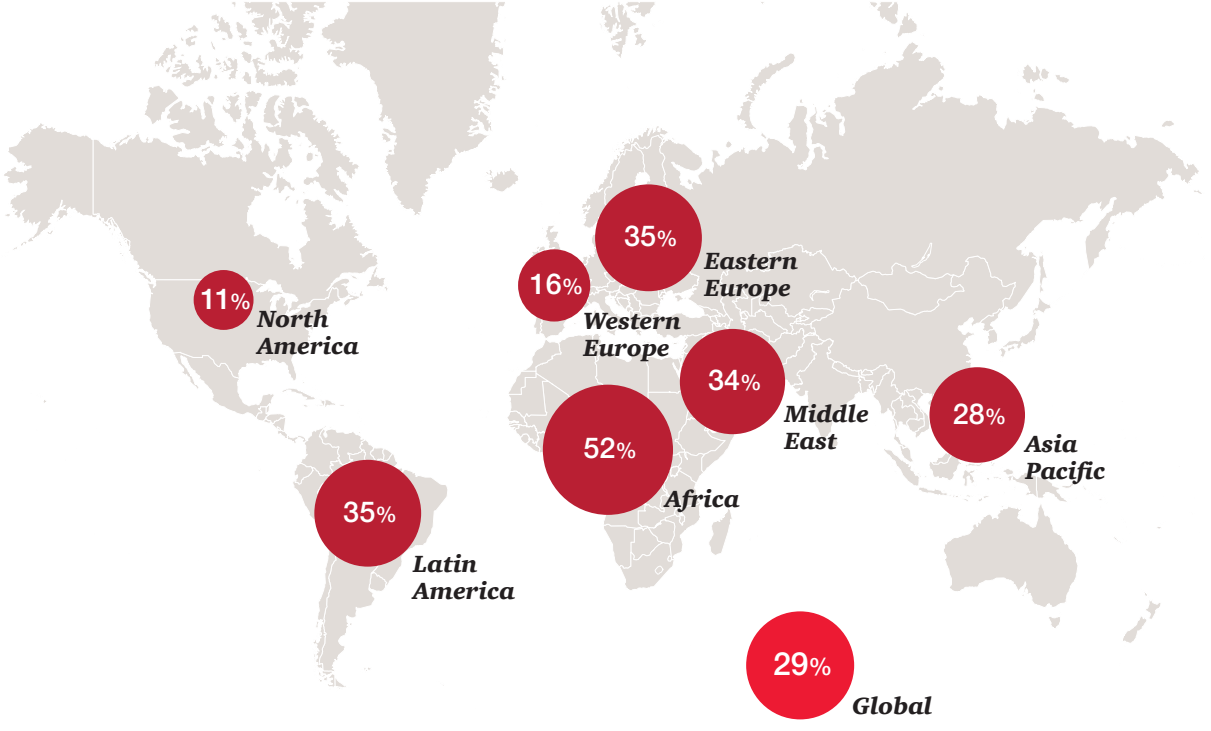



*% of all respondents who experienced economic crime over the survey period*

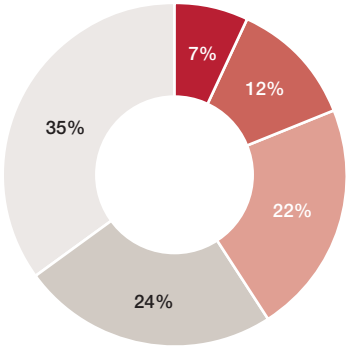
## Figure 14: Bribery and lost opportunities



## Figure 15: Perception of future bribery and corruption, by region



## Figure 16: Organisations affected by collusion

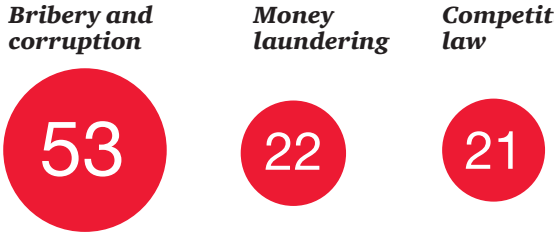



***41% indicate that more than 10% of revenues were affected by collusion***

Results of 2013 survey on economic crime conducted by PwC Germany
*Reported % of revenues affected by collusion*

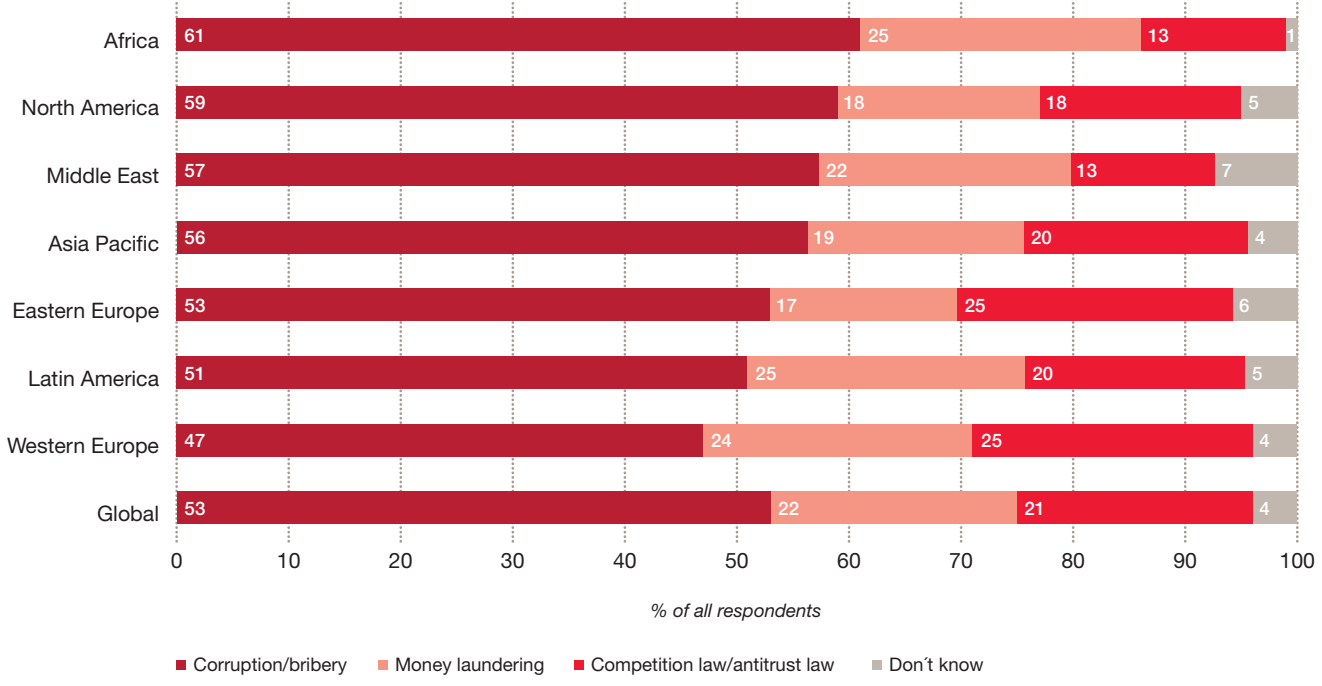
Over 30% | 20-29% | 10-19% | 5-9% | Below 5%

## Figure 17: Perceived greatest relative economic crime risk

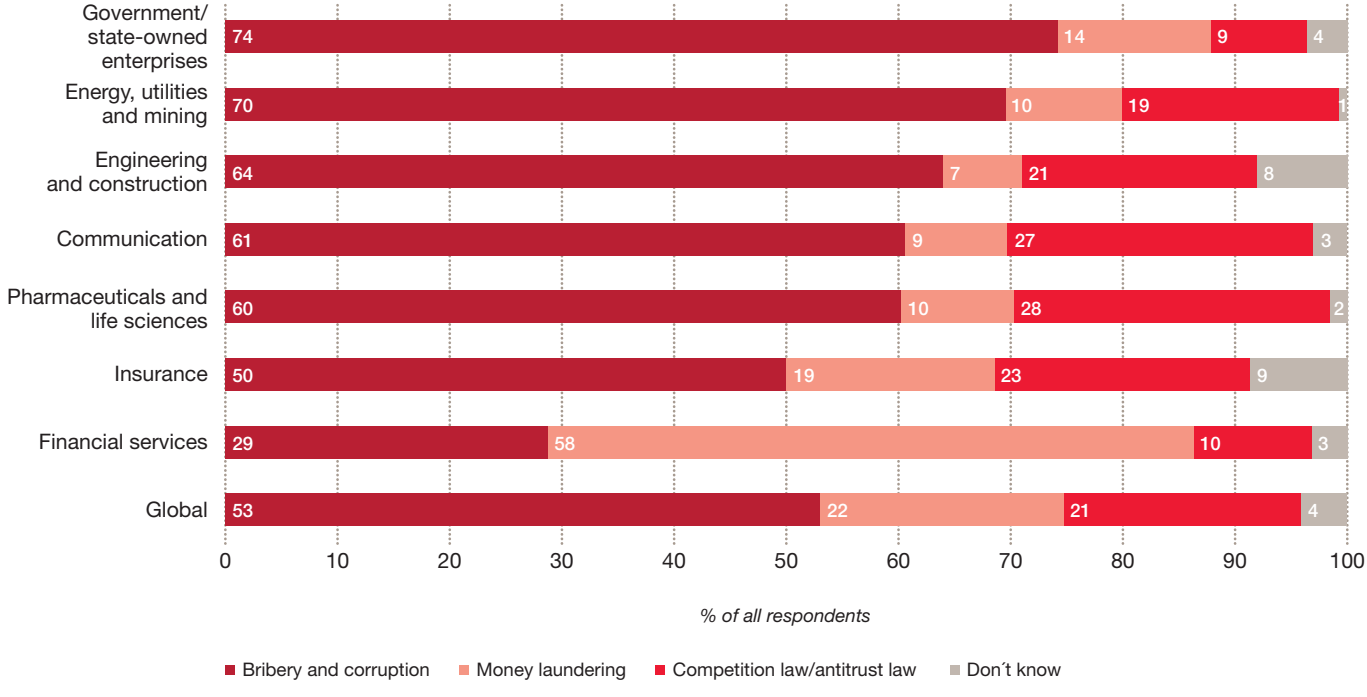



*% of all respondents*

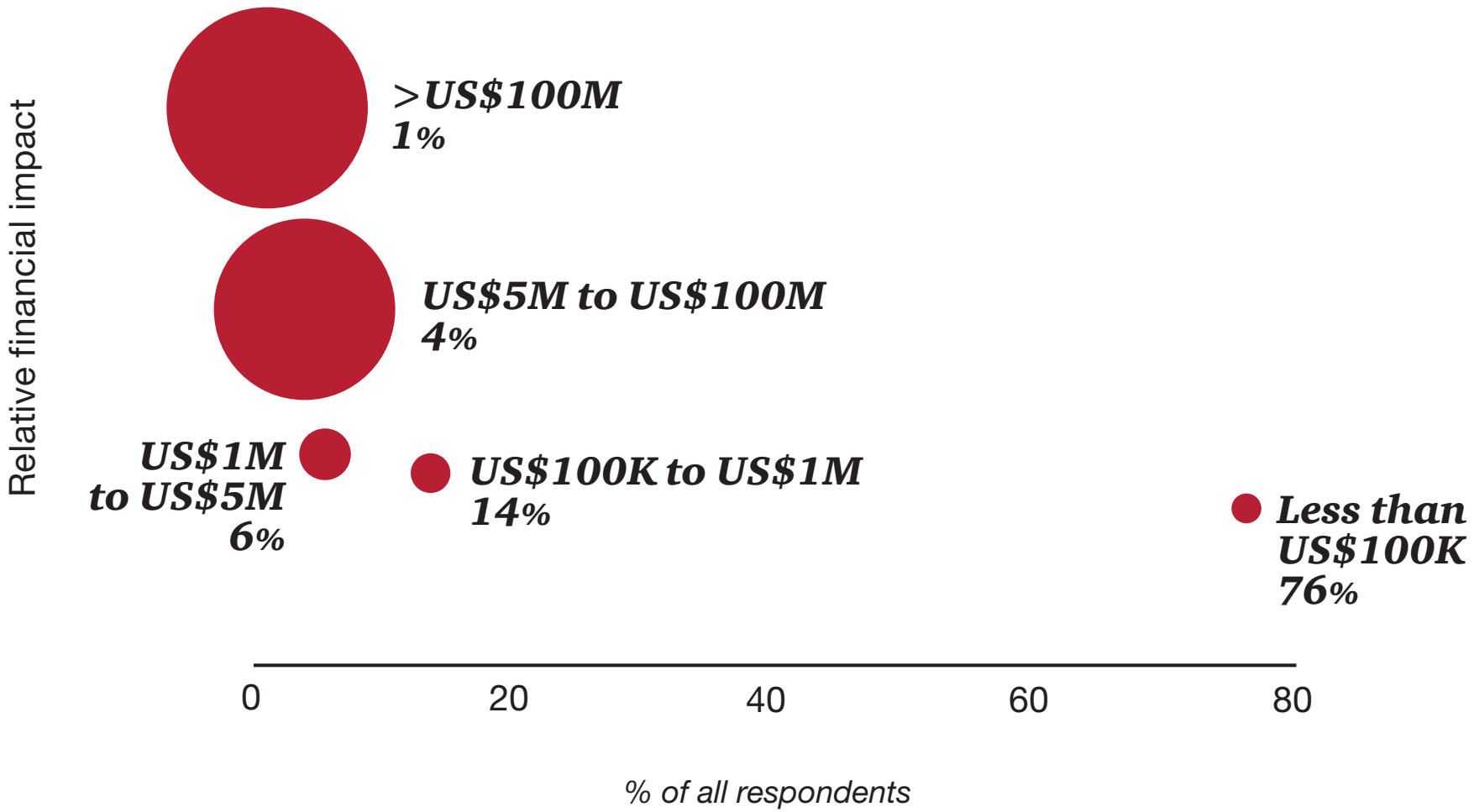
## Figure 18: Perceived greatest relative economic crime risk, by region



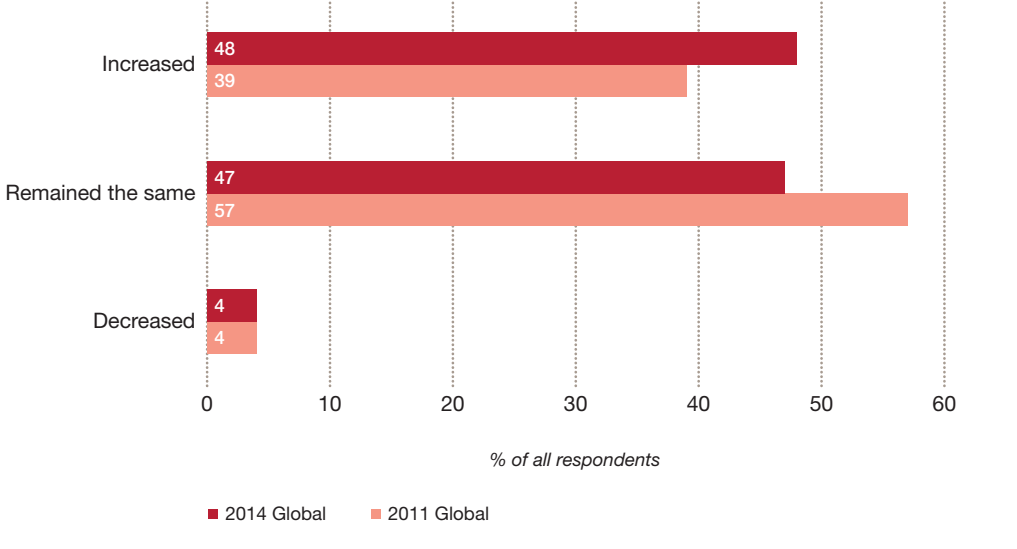
## Figure 19: Perceived greatest relative economic crime risk, by industry



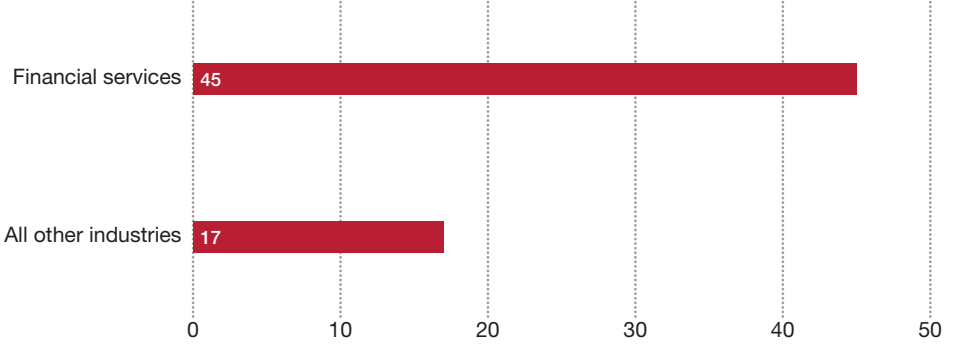
## Figure 20: Relative financial impact of cybercrime on organisations



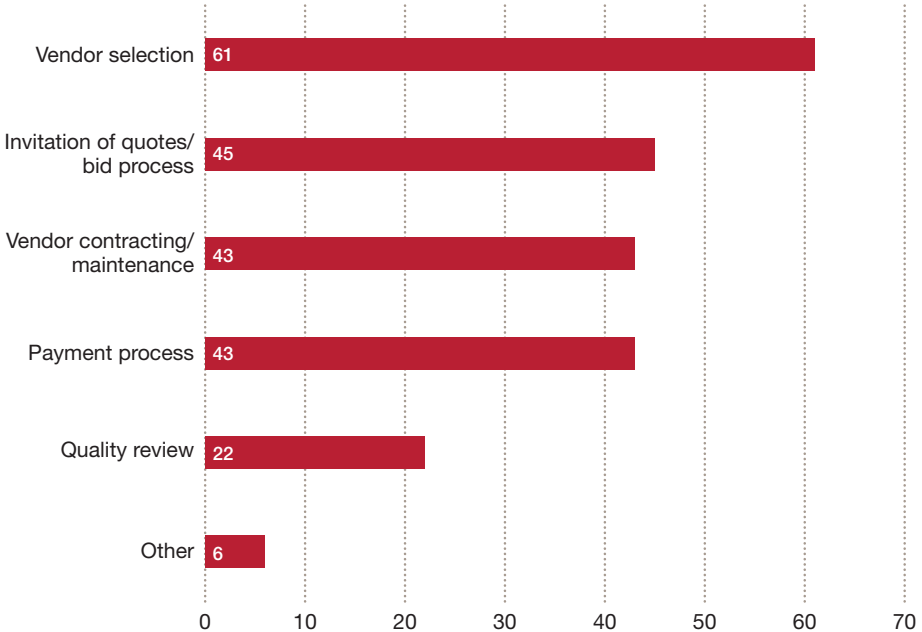
## Figure 21: Perception of the risk of cybercrime



## Figure 22: Cybercrime and financial services

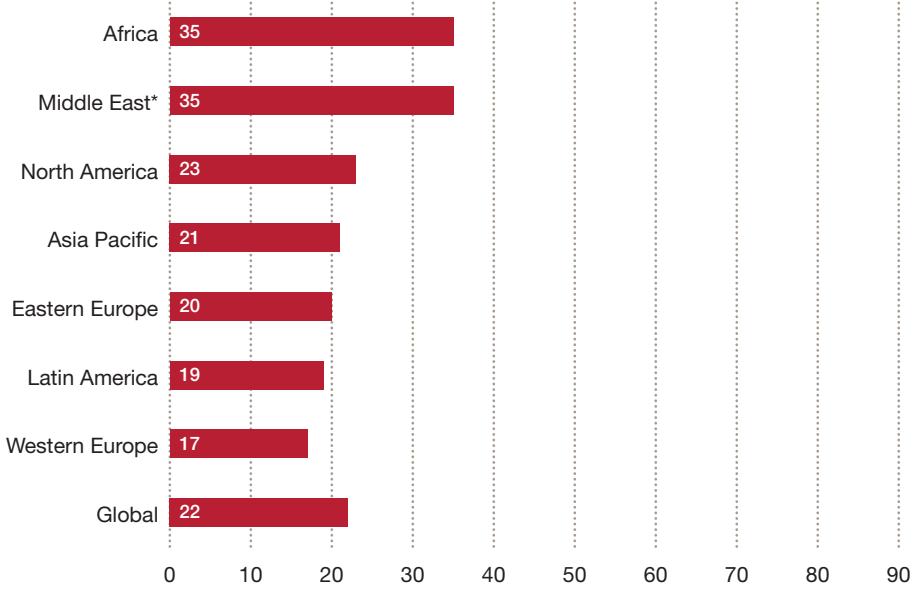


## Figure 23: Procurement fraud ocurrence by stage



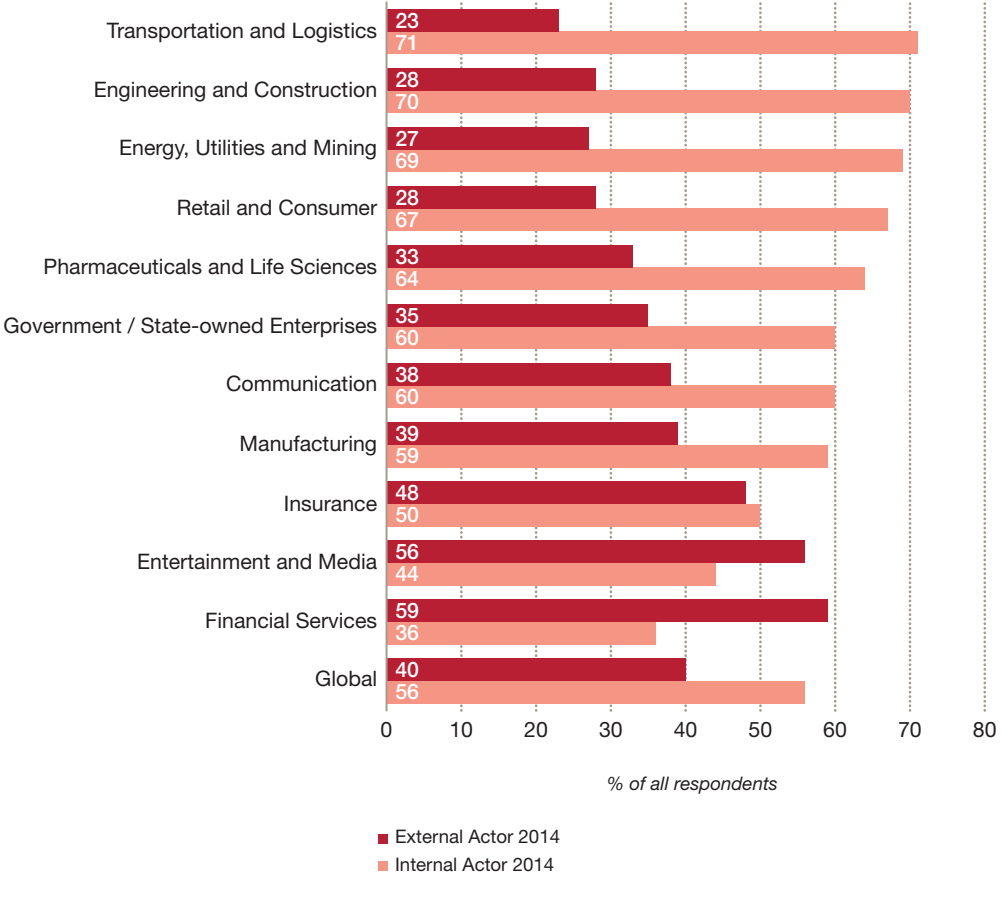

*% of all respondents who experienced procurement fraud over the survey period*

## Figure 24: Reported accounting fraud, by region

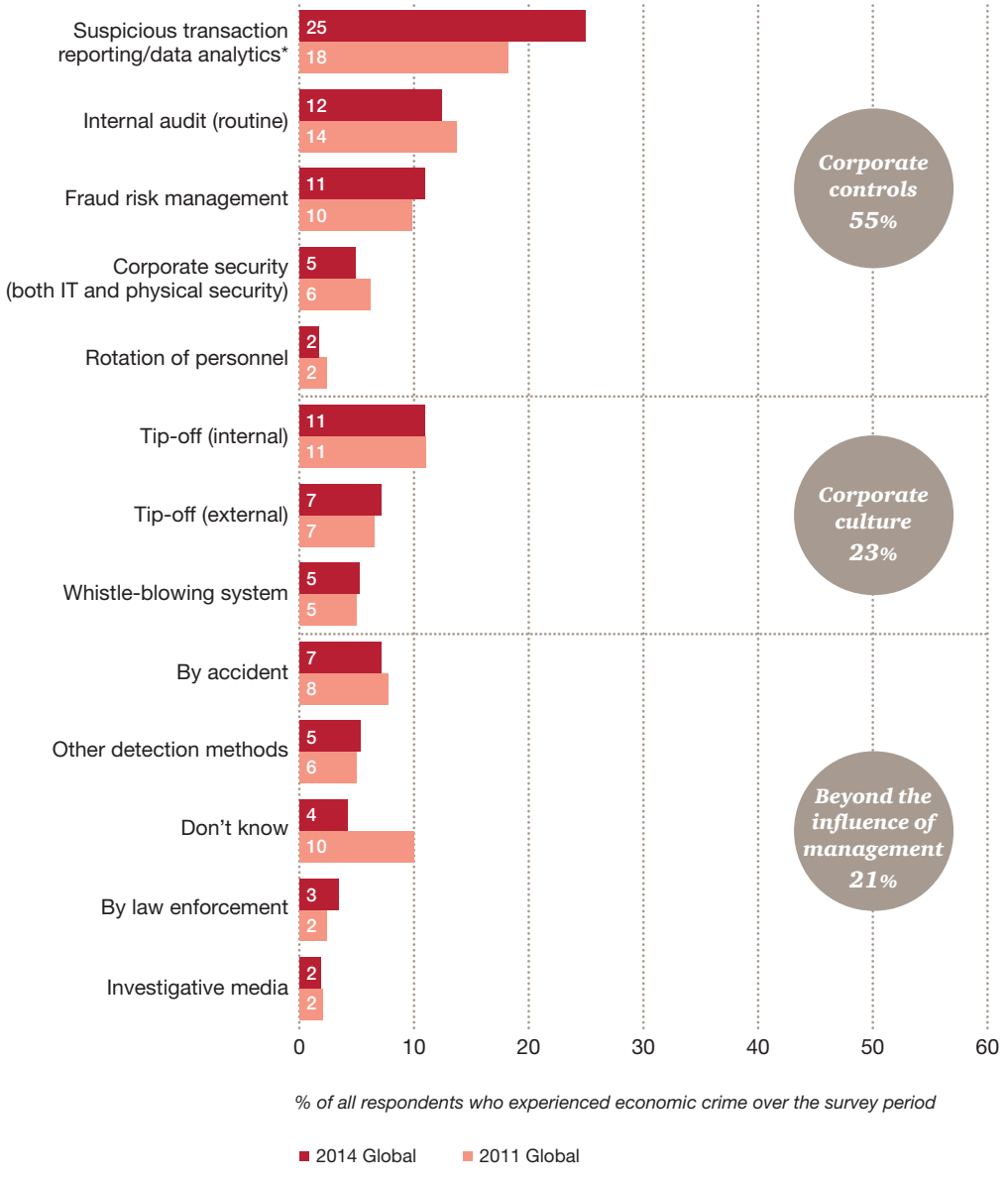



*Middle East was included in the "Asia Pacific" region in 2011

## Figure 25: Internal vs. external perpetrator, selected industries

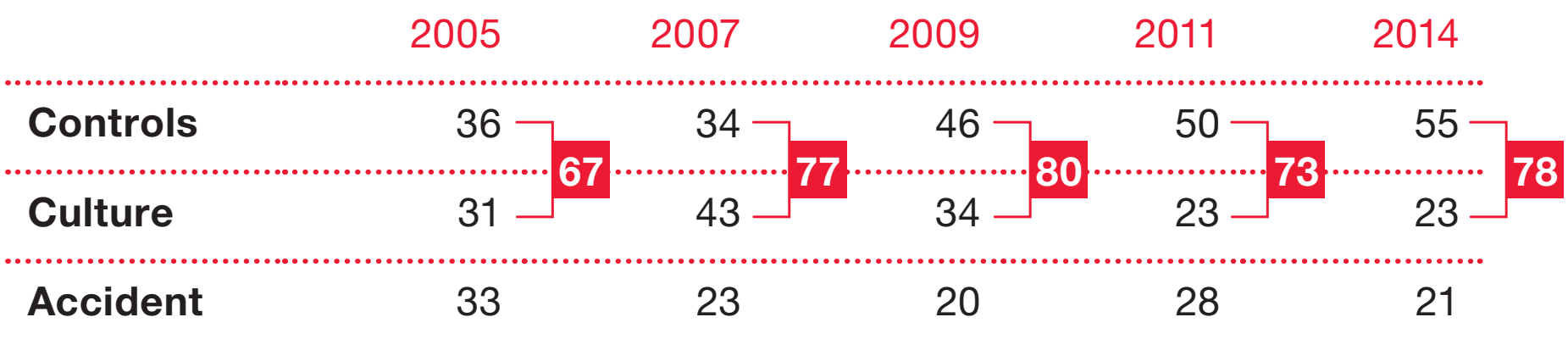


## Figure 26: Method of detection of most serious economic crime experienced



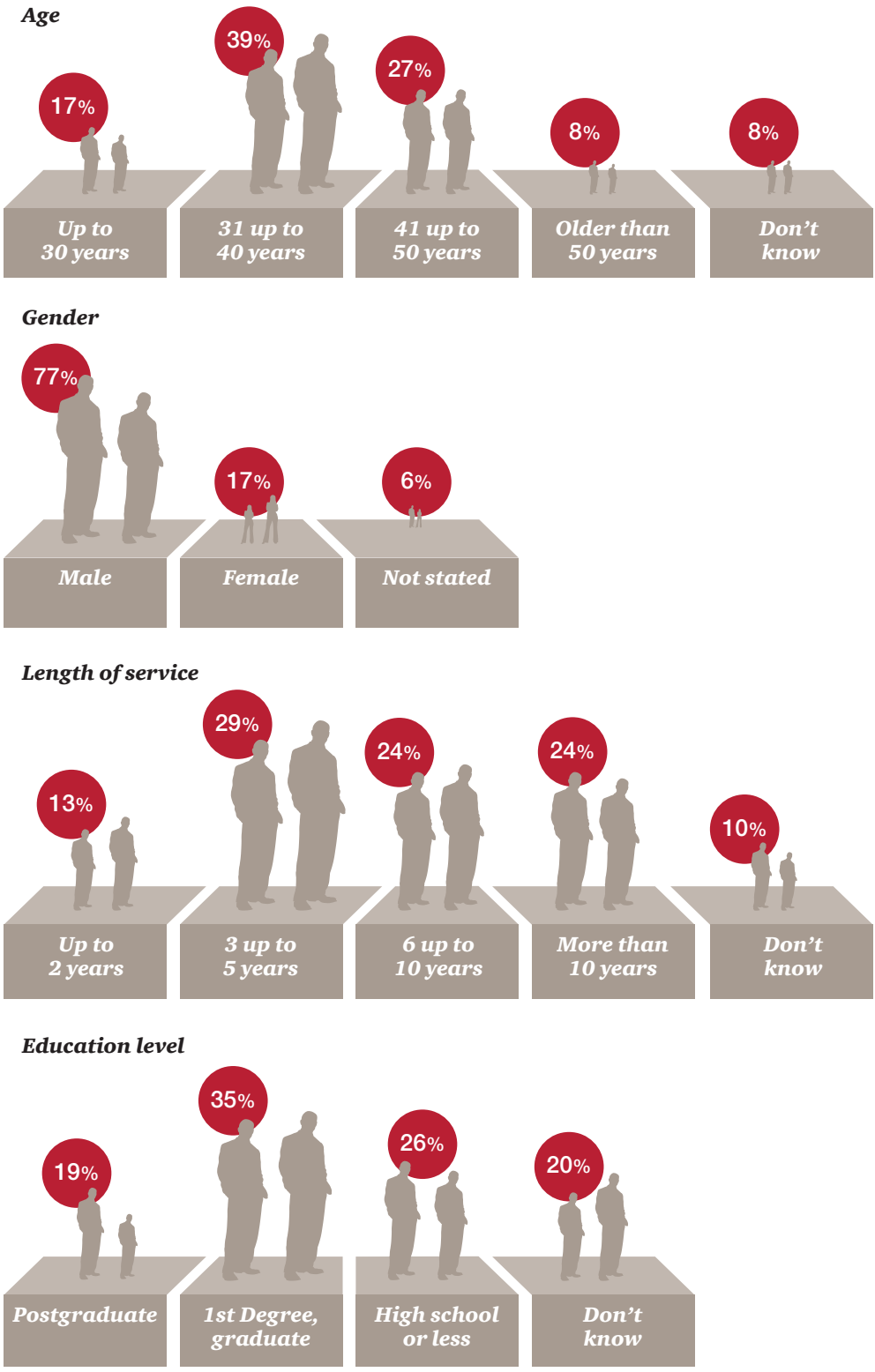

*Data Analytics was added as a category in the 2014 survey.

## Figure 27: Economic crime detection methods




*Historical % reported, how economic crime was detected*

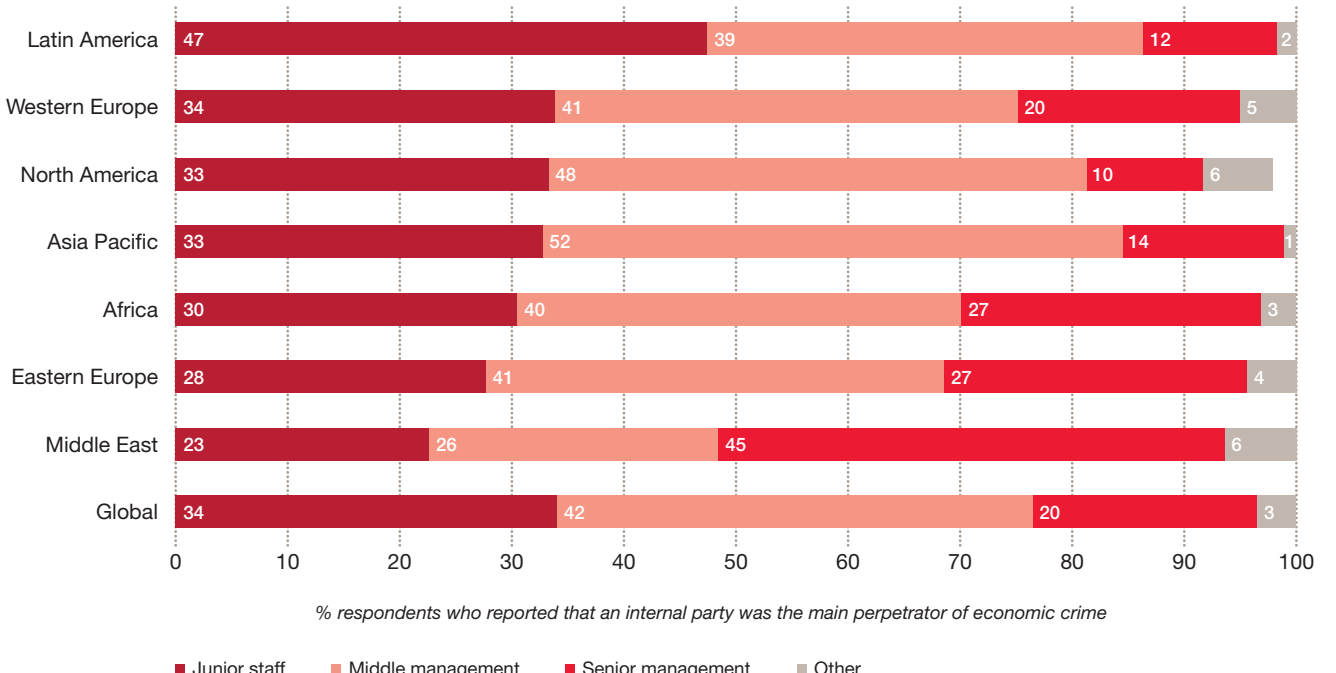
## Figure 28: Age, gender, length of service and education level of internal perpetrator




*% respondents who reported that an internal party was the main perpetrator of economic crime*

● 2014 Global

## Figure 29: Profile of internal perpetrator, by region



## Figure 30: Territories with highest percentage of economic crime

| Territory | Reported Fraud 2014 | Reported Fraud 2011 |
|---|---|---|
| South Africa | 69% | 60% |
| Ukraine | 63% | 36% |
| Russia | 60% | 37% |
| Australia | 57% | 47% |
| Papua New Guinea | 57% | NA |
| France | 55% | 46% |
| Kenya | 52% | 66% |
| Argentina | 51% | 45% |
| Spain | 51% | 47% |
| **Global** | **37%** | **34%** |

## Figure 31: Territories with lowest percentage of economic crime

| Territory | Reported Fraud 2014 | Reported Fraud 2011 |
|---|---|---|
| Malaysia | 24% | 44% |
| Italy | 23% | 17% |
| Turkey | 21% | 20% |
| Peru | 20% | 35% |
| Hong Kong/ Macau* | 16% | n/a |
| Japan | 15% | 5% |
| Portugal | 12% | n/a |
| Denmark | 12% | 29% |
| Saudi Arabia** | 11% | n/a |
| **Global** | **37%** | **34%** |

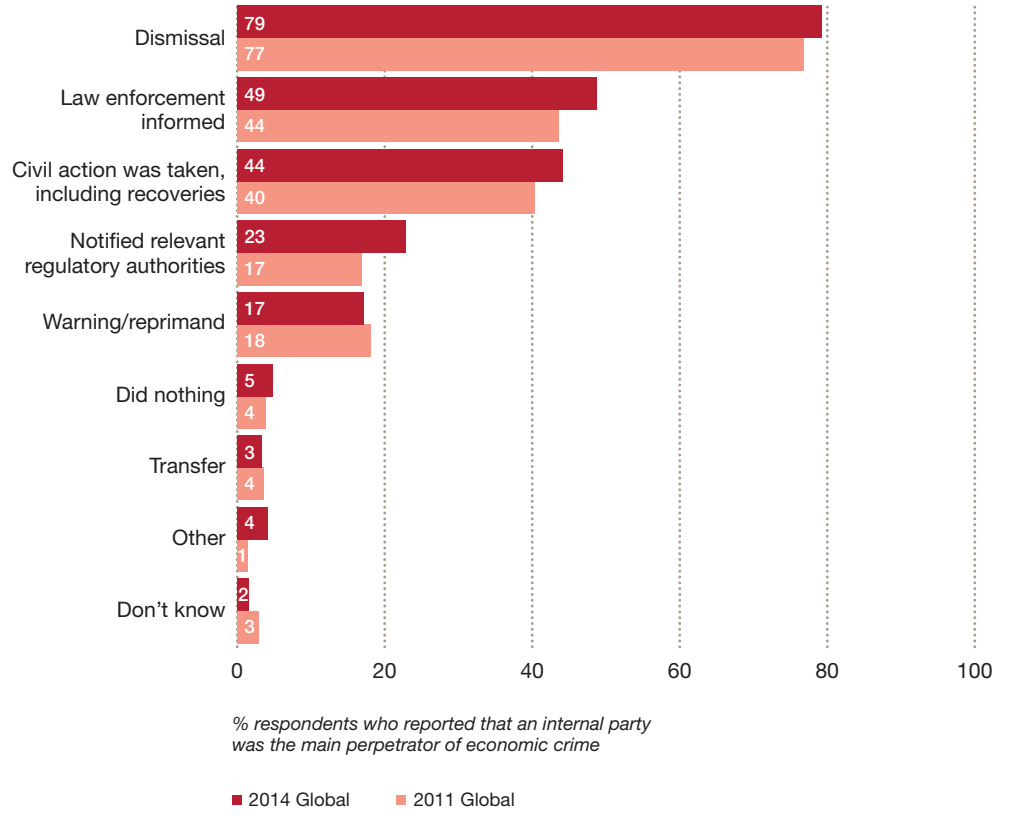
* Part of greater China in 2011; ** Part of greater Middle East in 2011

## Figure 32: Emerging 8 percentage of economic crime

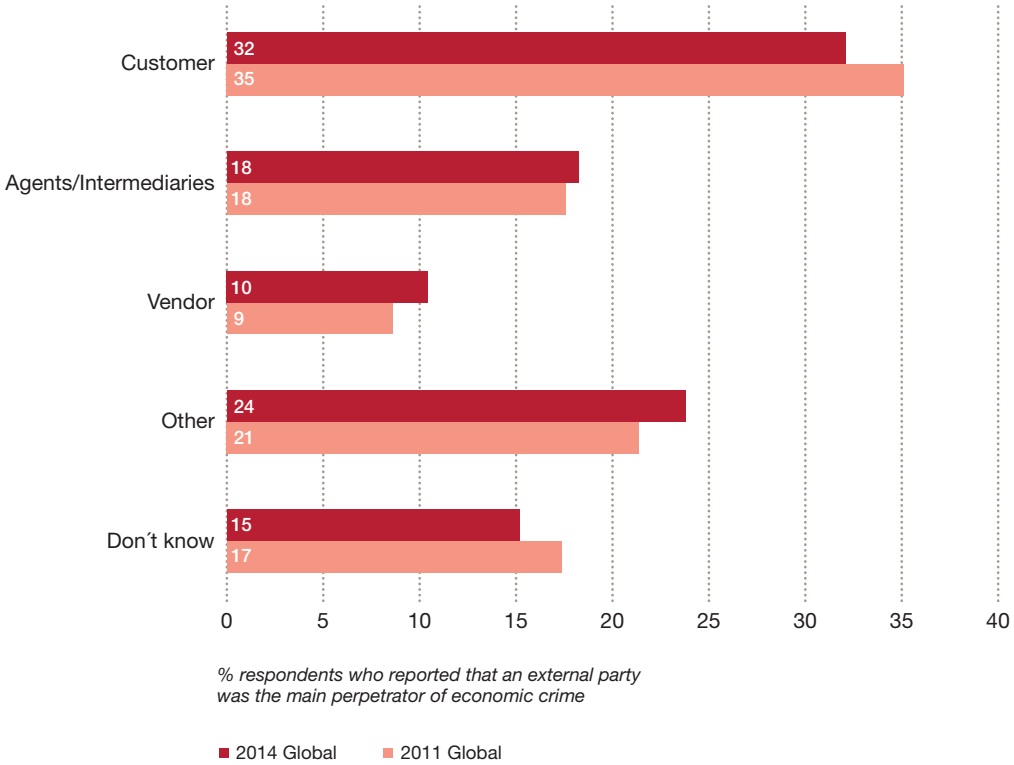
| Territory | Reported Fraud 2014 | Reported Fraud 2011 |
|---|---|---|
| Brazil | 27% | 33% |
| Russia | 60% | 37% |
| India | 34% | 24% |
| China* | 27% | NA |
| South Africa | 69% | 60% |
| Turkey | 21% | 20% |
| Mexico | 36% | 40% |
| Indonesia** | NA | 16% |
| **Global** | **37%** | **34%** |

* 2014 statistic for China excluding Hong Kong/Macau—figures unavailable for 2011; ** Figures unavailable for 2014

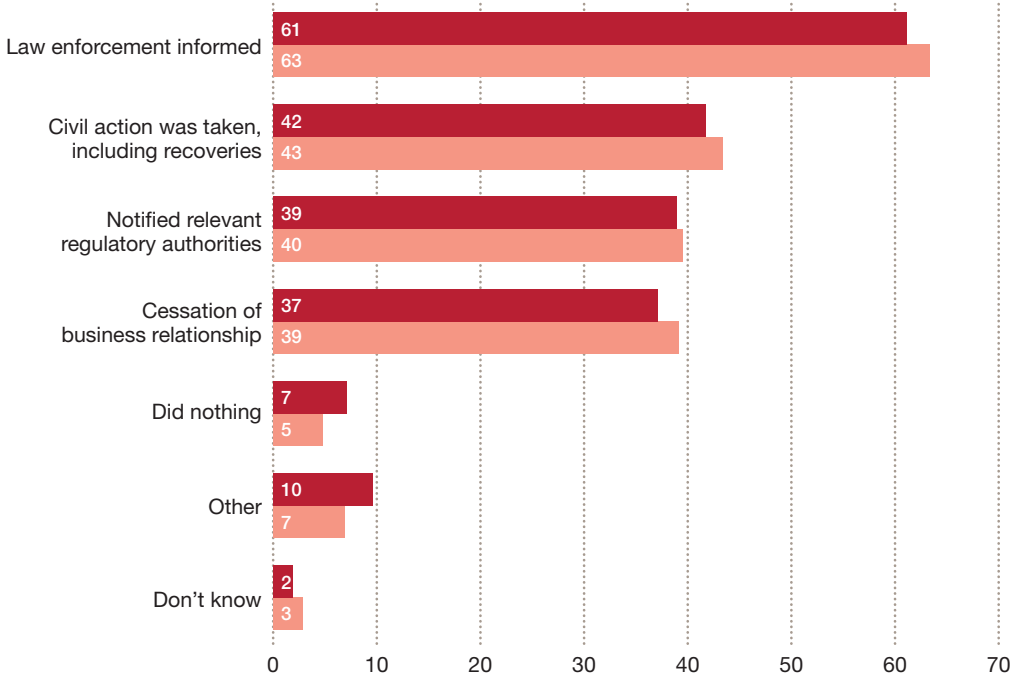
## Figure 33: Actions taken against internal perpetrator



## Figure 34: Profile of external perpetrator



## Figure 35: Actions taken against external perpetrator



## Figure 36: Participating territory counts

| Territory | 2014 | 2011 |
|---|---|---|
| **Asia Pacific** | **906** | **669** |
| Australia | 79 | 79 |
| China including Hong Kong[1] | N/A | 22 |
| Hong Kong / Macau | 116 | N/A |
| China (excluding Hong Kong) | 85 | N/A |
| India | 115 | 106 |
| Indonesia | 4 | 84 |
| Japan | 75 | 73 |
| Malaysia | 110 | 93 |
| New Zealand | 82 | 93 |
| Papua New Guinea | 81 | 1 |
| Singapore | 82 | 18 |
| Taiwan | 0 | 2 |
| Thailand | 76 | 79 |
| Vietnam | 1 | 19 |
| **Africa** | **604** | **259** |
| Algeria | 2 | 0 |
| Angola | 22 | 1 |
| Botswana | 5 | 1 |
| Cameroon | 6 | 0 |
| Democratic Republic of Congo | 1 | 0 |
| Ghana | 3 | 29 |
| Guinea | 2 | 0 |
| Ivory Coast | 3 | 0 |
| Kenya | 124 | 91 |
| Lesotho | 1 | 0 |
| Liberia | 0 | 5 |
| Malawi | 1 | 0 |
| Morocco | 17 | 0 |
| Mozambique | 4 | 0 |
| Namibia | 26 | 2 |
| Nigeria | 82 | 3 |
| Sierra Leone | 1 | 0 |
| South Africa | 134 | 123 |
| Swaziland | 4 | 1 |
| Tanzania | 12 | 0 |
| Tunisia | 17 | 2 |
| Uganda | 12 | 0 |
| Zambia | 83 | 1 |
| Zimbabwe | 42 | 0 |

| Territory | 2014 | 2011 |
|---|---|---|
| **Middle East[2]** | **232** | **128** |
| Unspecified Middle East Countries | N/A | 127 |
| Bahrain | 2 | N/A |
| Egypt | 7 | N/A |
| Jordan | 9 | N/A |
| Lebanon | 8 | N/A |
| Oman | 1 | N/A |
| Qatar | 12 | N/A |
| Saudi Arabia | 74 | N/A |
| Sudan[3] | 1 | 1 |
| Syria | 1 | N/A |
| UAE | 117 | N/A |
| **Western Europe** | **1,555** | **1,317** |
| Andorra | 0 | 1 |
| Austria | 6 | 8 |
| Belgium | 68 | 84 |
| Cyprus | 88 | 5 |
| Denmark | 118 | 116 |
| Finland | 34 | 61 |
| France | 131 | 112 |
| Germany[4] | 10 | 38 |
| Greece | 11 | 92 |
| Ireland | 78 | 80 |
| Israel | 31 | - |
| Italy | 101 | 127 |
| Luxembourg | 12 | 3 |
| Netherlands | 75 | 41 |
| Norway | 92 | 67 |
| Portugal | 75 | 0 |
| Spain | 79 | 85 |
| Sweden | 91 | 79 |
| Switzerland | 83 | 140 |
| UK[5] | 372 | 178 |
| **North America** | **215** | **209** |
| Canada | 100 | 53 |
| USA | 115 | 156 |

*1) China and Hong Kong/Macau were combined from 2005-2011. They were separated in the 2014 survey.*

*2) Middle East was previously part of Asia Pacific region totals.*

*3) Sudan was previously part of Africa region totals.*

*4) PwC Germany conducted a separate survey which captured 603 respondents from Germany in 2013.*

*5) UK includes instances when the survey responder indicated Guernsey as territory.*

## Figure 36: Participating territory counts (continued)

| Territory | 2014 | 2011 |
|---|---|---|
| **Central & Eastern Europe** | **877** | **804** |
| Bulgaria | 79 | 58 |
| Croatia | 0 | 1 |
| Czech Republic | 94 | 84 |
| Estonia | 0 | 1 |
| Hungary | 91 | 85 |
| Kazakhstan | 1 | 0 |
| Lithuania | 1 | 7 |
| Moldavia | 0 | 1 |
| Montenegro | 0 | 1 |
| Poland | 94 | 79 |
| Romania | 77 | 76 |
| Russia | 111 | 126 |
| Serbia | 52 | 14 |
| Slovakia | 76 | 84 |
| Slovenia | 33 | 48 |
| Turkey | 78 | 55 |
| Ukraine | 90 | 84 |

| Territory | 2014 | 2011 |
|---|---|---|
| **Latin America** | **711** | **483** |
| Argentina | 82 | 77 |
| Bahamas | 2 | 0 |
| Barbados | 1 | 0 |
| Bolivia | 0 | 3 |
| Brazil | 132 | 115 |
| Chile | 75 | 1 |
| Colombia | 1 | 1 |
| Cuba | 2 | 0 |
| Dominican Republic | 1 | 0 |
| Ecuador | 22 | 11 |
| Mexico | 211 | 174 |
| Peru | 82 | 17 |
| Venezuela | 100 | 84 |
| **No primary country specified** | **28** | **8** |
| **Total** | **5,128** | **3,877** |

## Figure 37: Participating industry groups

| Industry | % respondents 2014 | 2011 |
|---|---|---|
| Aerospace and defence | 1% | 1% |
| Automotive | 4% | 4% |
| Chemicals | 2% | 2% |
| Communication | 3% | 3% |
| Energy, utilities and mining | 7% | 7% |
| Engineering and construction | 6% | 5% |
| Entertainment and media | 2% | 3% |
| Financial services | 19% | 18% |
| Government/state-owned enterprises | 5% | 5% |
| Hospitality and leisure | 2% | 2% |
| Insurance | 7% | 5% |
| Manufacturing | 9% | 12% |
| Pharmaceuticals and life sciences | 5% | 5% |
| Professional services | 6% | 6% |
| Retail and consumer | 7% | 8% |
| Technology | 5% | 5% |
| Transportation and logistics | 5% | 4% |

## Figure 38: Principal function of participants

*% respondents*

| Industry | 2014 | 2011 |
|---|---|---|
| Audit | 14% | 16% |
| Advisory/Consultancy | 4% | 3% |
| Compliance | 6% | 5% |
| Customer service | 1% | 1% |
| Executive management | 18% | 17% |
| Finance | 28% | 29% |
| Human resources | 1% | 1% |
| Information technology | 2% | 4% |
| Legal | 4% | 4% |
| Marketing and sales | 3% | 2% |
| Operations and production | 2% | 3% |
| Procurement | 1% | 0% |
| Research and development | 1% | 1% |
| Risk management | 6% | 6% |
| Security | 3% | 4% |
| Tax | 1% | 1% |
| Other (please specify) | 6% | 2% |

## Figure 39: Job title of participants

| | % respondents | |
|---|---|---|
| | 2014 | 2011 |
| **Senior Executives** | **50%** | **53%** |
| Board Member | 4% | 4% |
| Chief Executive Officer/President/ Managing Director | 12% | 10% |
| Chief Operating Officer | 2% | 2% |
| Chief Financial Officer/Treasurer/ Comptroller | 23% | 23% |
| Chief Information Officer/ Technology Director | 1% | 3% |
| Chief Security Officer* | 2% | |
| Other C-level Executive (please specify) | 6% | 10% |
| **Non-Senior Executives** | **49%** | **47%** |
| Senior Vice President/Vice President/ Director | 7% | 8% |
| Head of Business Unit | 4% | 7% |
| Head of Department | 15% | 15% |
| Head of Human Resources* | 1% | |
| Manager | 22% | 17% |
| Others (please specify) | 2% | 0% |

**Option added in the 2014 survey*

# Figure 40: Organisation types participating

| | % respondents | |
|---|---|---|
| | 2014 | 2011 |
| Listed on a stock exchange | 35% | 36% |
| Private | 50% | 51% |
| Government/state-owned enterprises | 9% | 10% |
| Other (please specify) | 6% | 3% |

## Figure 41: Size of participating organisations

| | % respondents | |
|---|---|---|
| | 2014 | 2011 |
| Up to 1,000 employees | 44% | 43% |
| 1,001–5,000 employees | 20% | 20% |
| More than 5,000 | 34% | 34% |

# *Delitos económicos: Una amenaza a los negocios que sigue creciendo*

**51%**
Más de la mitad de los encuestados fueron víctimas de un delito económico.

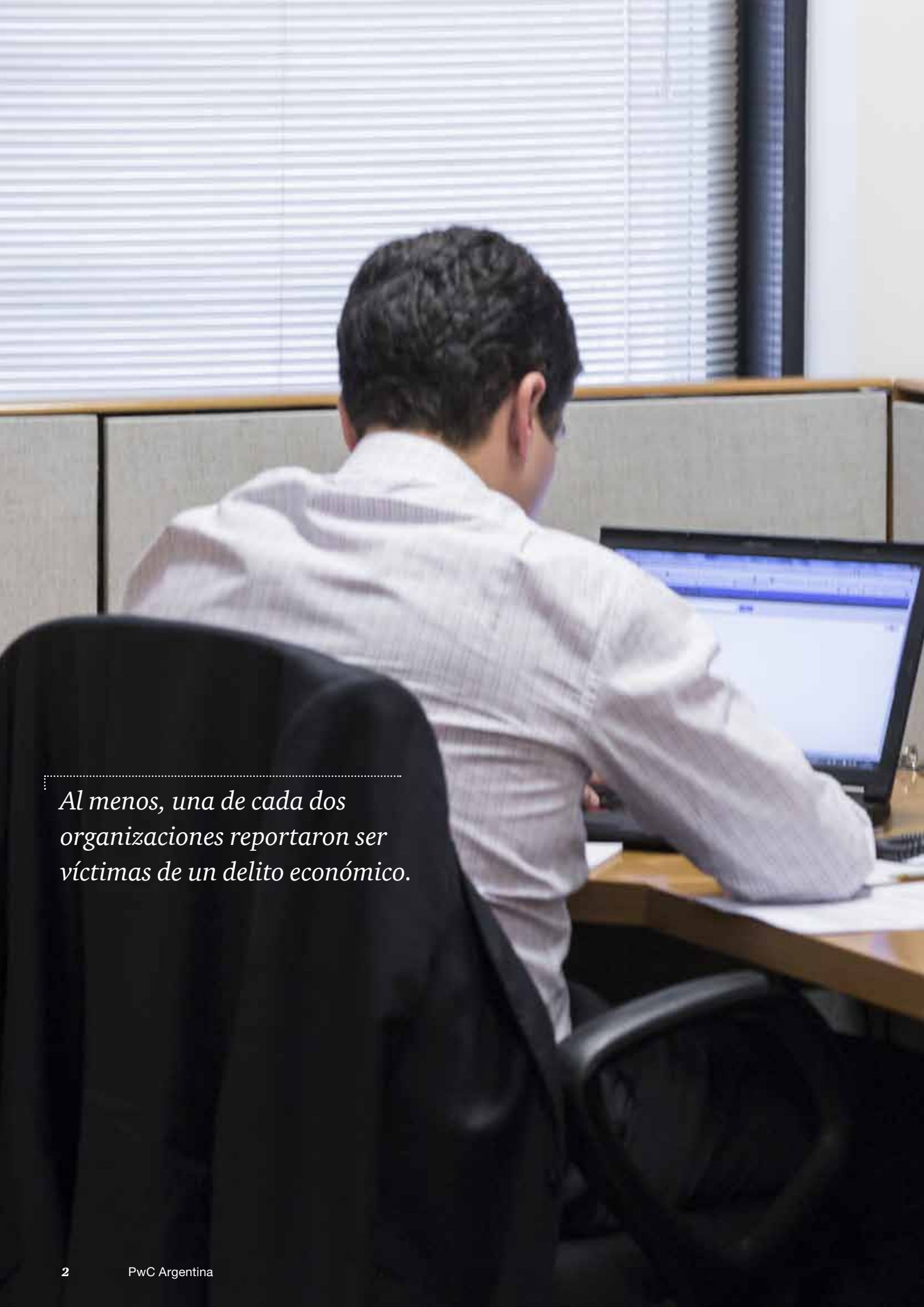
**64%**
Casi 2 de cada 3 CEOs informaron estar preocupados por el soborno y la corrupción.

**33%**
1 de cada 3 informó que el riesgo de delito informático ha aumentado casi el 50% con respecto a 2011.

pwc

*Los delitos económicos siguen siendo una preocupación importante para las organizaciones de todos los tamaños, en todas las regiones y en prácticamente todos los sectores.*

# Contenido



*Al menos, una de cada dos organizaciones reportaron ser víctimas de un delito económico.*

# *Prólogo*

Preocupará a más de uno, pero no sorprenderá, que la Argentina continúe siendo uno de los 10 países que proporcionalmente mayor cantidad de fraudes reportó en los últimos 24 meses.

Este mensaje encabeza el capítulo argentino de la Encuesta Global sobre Delitos Económicos 2014, una de las más amplias y exhaustivas encuestas, con más de 5.000 encuestados en casi 100 países y con récord de participación de empresas argentinas (más de 80).

Es cierto que los fraudes son una amenaza ya conocida por los directivos empresarios, el problema que se suscita en Argentina es que los delitos económicos continúan creciendo año tras año, atacando cada proceso de negocios, erosionando la integridad de los empleados y empañando la reputación de las empresas. El propósito, en esta 7ma. edición, es explicar cómo está siendo afectada la organización y reflexionar sobre cómo afrontar esta amenaza y revertir esta tendencia. Tendencia que, también ubica al país como el más atacado de toda América Latina, ya que 51% de las organizaciones argentinas encuestadas respondieron haber sufrido un fraude en los últimos 24 meses.

Cada uno de los procesos básicos comunes a toda organización –ventas y cobranzas, compras y pagos, altas y bajas de empleados- está bajo amenaza. Es inherente a toda empresa, que tenga que interactuar con diferentes actores económicos para desarrollar su actividad (clientes, distribuidores, agentes, consultores, contratistas, proveedores), exponerse diariamente a diversas formas de fraude en diferentes dimensiones.

Al mismo tiempo, los riesgos continúan evolucionando y –al igual que un virus- los delitos económicos se adaptan a los cambios que experimentan las organizaciones. Así como la tecnología adopta cada vez más un rol protagónico en toda transacción y las compañías se apoyan en la tecnología para desarrollar su actividad, no sorprende que los delitos informáticos escalen posiciones en frecuencia, impacto y sofisticación: es el segundo tipo de fraude más recurrente (en 2011 ocupaba el quinto lugar), después de la malversación de activos.

Asimismo, no resultará novedoso que esta encuesta haya arrojado que los fraudes en compras y contrataciones sean un tema no menor. Sin embargo, esta edición nos permite tomar conciencia de la dimensión de este padecimiento como así también del fraude en los recursos humanos: dos males difíciles de erradicar.

Ante semejante escenario, no es de extrañar que los delitos económicos estén instalados en la agenda de la alta dirección de las empresas. En Argentina, dos de cada tres CEOs –según nuestra reciente **Encuesta Global Anual de CEOs 2014**- respondieron estar preocupados por la corrupción.

Esperamos este informe sea de utilidad a todos sus *stakeholders*, tanto como punto de referencia así como también una herramienta estratégica para la lucha contra el fraude.

Jorge C. Bacher
Socio de PwC Argentina

# *Resultados destacados*

- **Más de la mitad** de los encuestados fueron víctimas de un delito económico en los últimos 24 meses.
- Argentina persiste entre los diez países que proporcionalmente **mayor cantidad de delitos económicos** reportaron en los últimos 24 meses y el más atacado de América Latina.
- El 40% de las organizaciones que reportaron un delito económico sufrieron un **impacto financiero** de más de cincuenta mil dólares.
- La **malversación de activos** fue el delito económico más recurrente durante los últimos 24 meses, con el 67% de fraudes reportados.
- Continúan creciendo los **delitos informáticos**, se convirtieron en el segundo tipo de fraude más reportado (21%). En el 2011, solo 8% de los casos reportados se correspondía con este delito.
- No sorprende, pero preocupa, que el fraude en las **compras y contrataciones** se ubique como el tercer tipo de delito económico más común, habiendo sido esta la primera edición que incluyó esta categoría.
- A casi 20% de los encuestados le pidieron un **soborno** en los últimos 24 meses. Similar porcentaje de encuestados reportó haber perdido una oportunidad de negocio frente a un competidor que ha pagado un soborno.
- La **evaluación del riesgo de fraude** continúa siendo una asignatura pendiente para las organizaciones. Argentina se encuentra entre los 10 países cuyas empresas informaron desconocer o no haber realizado ninguna evaluación del riesgo de fraude en los últimos 24 meses.
- Preocupa que **auditores internos** desconozcan si su organización sufrió un delito económico en los últimos 24 meses.
- El **perpetrador interno** continúa siendo la principal amenaza de la organización (69%).
- La **tolerancia cero** predomina en las organizaciones: 24 de las 29 organizaciones que sufrieron un delito económico perpetrado por un actor interno, informaron que despidieron al empleado involucrado.
- En 2013, la Securities Exchange Commission de los Estados Unidos (SEC) penalizó a 8 compañías por cometer actos de corrupción alrededor del mundo. 2 de esas 8 compañías, fueron **sancionadas por sus delitos cometidos** en Argentina por una suma total de casi 14 millones de dólares.

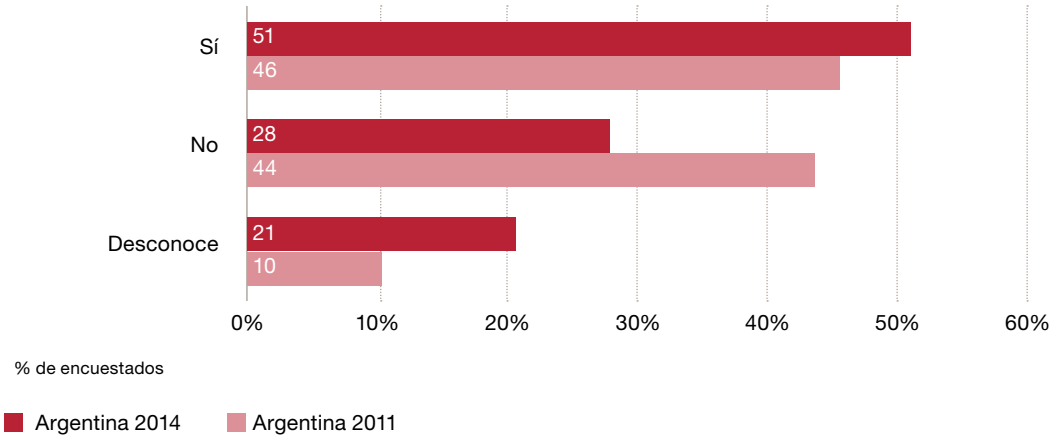
El **futuro** no parece ser prometedor: 33% de los encuestados temen ser víctima de un fraude en los próximos 12 meses. Esta percepción se incrementó 16 puntos porcentuales en comparación con 2011 (17%).

*Argentina persiste entre los diez países que proporcionalmente mayor cantidad de delitos económicos reportaron en los últimos 24 meses.*

# *Delitos económicos en el año 2014*
## Una foto de Argentina

A pesar de los esfuerzos de las organizaciones y de los profesionales que combaten el fraude, la delincuencia económica continúa creciendo en Argentina. Más de la mitad de los encuestados informaron que su organización ha experimentado un delito económico durante los últimos 24 meses, un incremento de 5 puntos porcentuales en comparación con nuestra encuesta del 2011. Además, vale resaltar que más del 48% de las organizaciones que reportaron delitos económicos fueron víctimas de más de un incidente.

**Gráfico 1. Organizaciones argentinas que reportaron delitos económicos**




Los resultados arrojados posicionan a Argentina entre los 10 países que proporcionalmente mayor cantidad de delitos económicos reportaron en los últimos 24 meses.

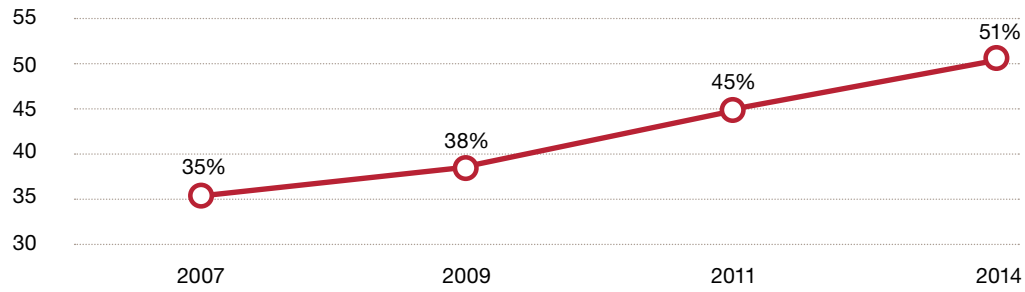
**Gráfico 2. Países que proporcionalmente reportaron mayor cantidad de fraudes**

| País | 2014 | 2011 |
|---|---|---|
| Sudáfrica | 69% | 60% |
| Ucrania | 63% | 36% |
| Rusia | 60% | 37% |
| Australia | 57% | 47% |
| Papúa Nueva Guinea | 57% | N/A |
| Francia | 55% | 46% |
| Kenia | 52% | 66% |
| **Argentina** | **51%** | **46%** |
| España | 51% | 47% |

N/A: no se obtuvo la cantidad de respuestas mínimas requeridas.

Analizando la tendencia de nuestras últimas encuestas, notamos que la cantidad de víctimas crece año tras año. En 2007, 35% de las organizaciones reportaron un fraude. En 2014, esa cifra llegó al 51%. En otras palabras, los delitos económicos han aumentado casi un 50% desde 2007.

**Gráfico 3. Evolución del fraude en Argentina 2007 - 2014**




% de encuestados

¿A qué responde este incremento de fraudes? ¿Las organizaciones mejoraron sus métodos de detección? ¿Es un problema puntual de una industria? ¿Depende del tamaño? ¿El fraude afecta por igual a toda la región? ¿Cómo frenar esta escalada que Argentina experimenta desde el 2007?

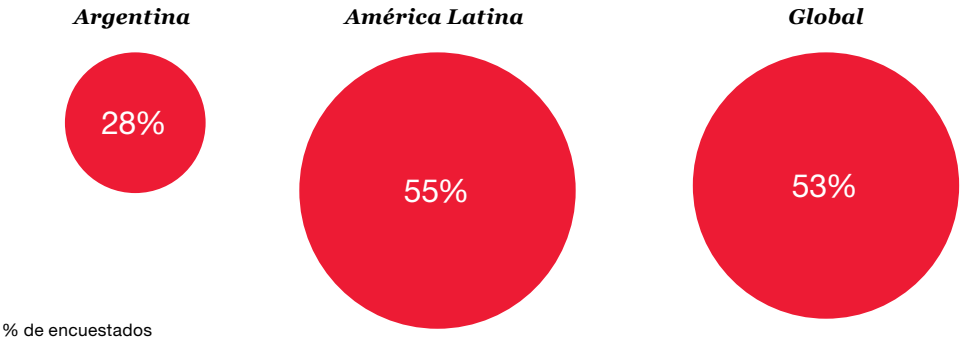
En las páginas siguientes intentaremos ensayar algunas posibles respuestas a esto y otros interrogantes de los delitos de cuello blanco en nuestro país.

## Prevenir a partir de la experiencia

Llamó la atención que el 28% de los argentinos encuestados respondió no haber sufrido un delito económico y el 21% reportó desconocerlo. Estas cifras resultan muy lejanas a las de América Latina (55% y 10% respectivamente) y el resto del mundo (53% y 10% respectivamente). Dicho 21%, al compararlo con otras latitudes nos sugiere que la comunicación de los delitos económicos no es frecuente en las organizaciones argentinas.

El primer paso para prevenir y disuadir un hecho delictivo es conocer los incidentes sufridos. No es alentador que de ese 21% que respondió desconocer si su organización fue víctima de un delito económico, poco menos de un tercio de ellos desempeñan funciones dentro del área de **auditoría**.

## Gráfico 4. Organizaciones que no reportaron delitos económicos

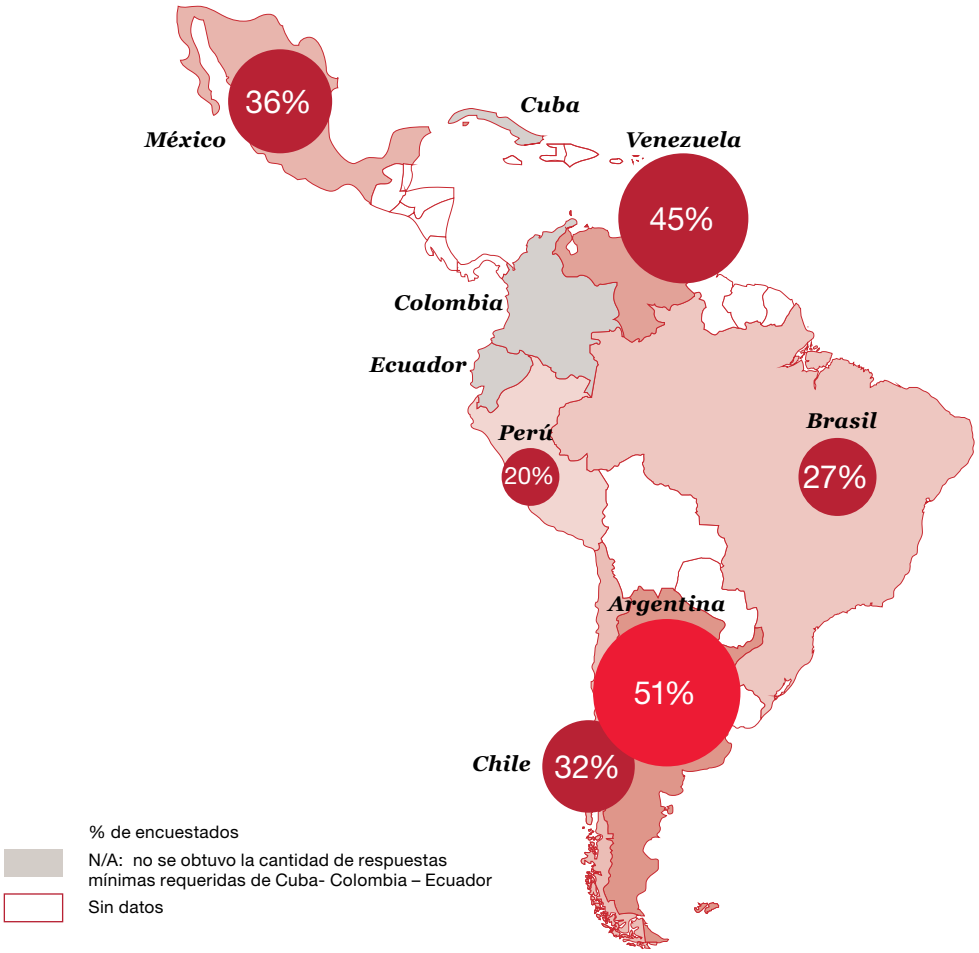



% de encuestados

## Argentina y la región

En esta 7ma. edición de la encuesta, 707 organizaciones de 9 países de Latinoamérica respondieron las preguntas. 250 de las empresas en la región sufrieron un delito económico, siendo Argentina el país que proporcionalmente mayor cantidad de delitos económicos reportó. Este lugar que ocupa no es nuevo, también en nuestra encuesta de 2011 las empresas argentinas fueron las que ocuparon la primera posición.

## Gráfico 5. Países en América Latina que reportaron delitos económicos en 2014

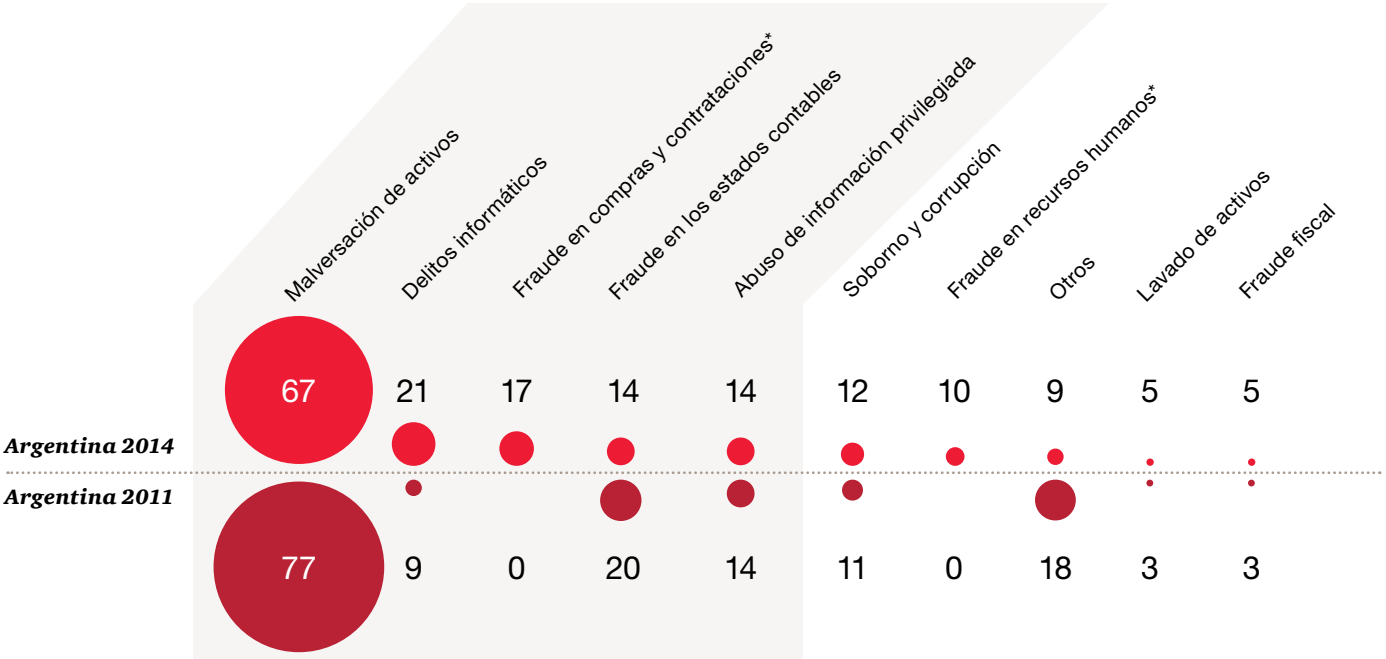


*El fraude en compras y contrataciones se posicionó como el tercero más reportado en nuestro país.*

# ¿A qué nos enfrentamos?

Los delitos económicos pueden presentarse en diversas modalidades, cada uno con sus propias características, amenazas y consecuencias.

**Gráfico 6. Tipos de delitos económicos reportados por las organizaciones**




*No fueron inluidos en la Encuesta de 2011
% sobre los encuestados que sufrieron un delito económico los últimos 24 meses
Nota: Se permitió la selección de respuestas múltiples

Nuestras últimas encuestas (desde el 2007) ubican por un amplio margen a la **malversación de activos** como el fraude más reportado. Sin embargo, este año la tasa disminuyó al 67% (77% en 2011), seguramente dada la incorporación de dos nuevas categorías de delitos económicos en la presente edición: el fraude en compras y contrataciones (17%) y el fraude en recursos humanos (10%).

Al respecto de estas nuevas categorías, los resultados no fueron alentadores; el **fraude en compras y contrataciones** se posicionó como el tercero más reportado en nuestro país (segundo en América Latina y el mundo). Esta ubicación podría estar impulsada por la tendencia global a la subcontratación de servicios y la interconectividad entre las organizaciones.

*En los próximos 12 meses, el 32% de las compañías cree que sufrirá fraude en compras y contrataciones y un 21% en torno a recursos humanos.*

Es importante mencionar que las industrias que reportaron, al menos un hecho de fraude en compras y contrataciones, fueron aquellas que dependen de una estrecha colaboración con una amplia variedad de proveedores, en toda su cadena de valor:

- Telecomunicaciones.
- Manufactura.
- Energía, Servicios Públicos y Minería.
- Servicios Financieros.
- Venta Mayorista y Minorista.

En lo que se refiere al **fraude en recursos humanos**, si bien no disponemos de datos históricos, surge como una amenaza de la cual no hay que descuidarse. Las organizaciones deberían replantearse qué actividades de control se realizan en procesos tales como la contratación de empleados y la liquidación de novedades (ejemplo: horas extras).

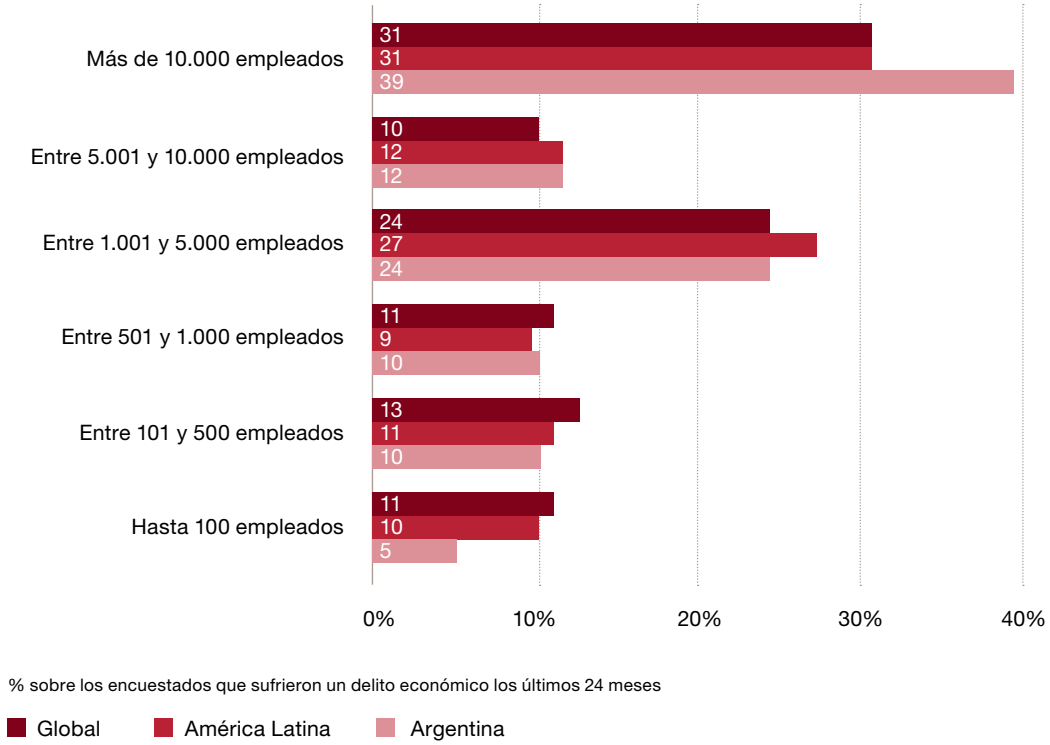
Seguramente, deberán prestar mayor atención aquellas organizaciones que emplean a muchos trabajadores y/o experimentan un significativo y rápido crecimiento de la nómina. La amenaza de sufrir este tipo de fraude crece en relación a la nómina de empleados: en Argentina y en el mundo, las principales víctimas de este tipo de fraude fueron empresas con más de 500 empleados.

Como lo inferíamos al decidir incorporar ambas categorías a la encuesta, son amenazas con entidad propia y requieren una rápida respuesta de las organizaciones. En los próximos 12 meses, el 32% de las compañías espera sufrir un fraude en compras y contrataciones y un 21% un fraude en recursos humanos.

## El tamaño y la industria

No es el tamaño o la industria donde opera una compañía razón suficiente para ser víctima de un fraude, sino cómo se prepara para afrontar un ataque. Hoy en día, las organizaciones están expuestas a los delitos económicos de igual manera, sin importar sus características. Sin embargo, podemos afirmar que, en comparación con las pymes, las compañías más grandes disponen de más recursos y, en consecuencia, tienen la posibilidad de invertir en mecanismos más eficaces de prevención, detección y disuasión de fraudes.

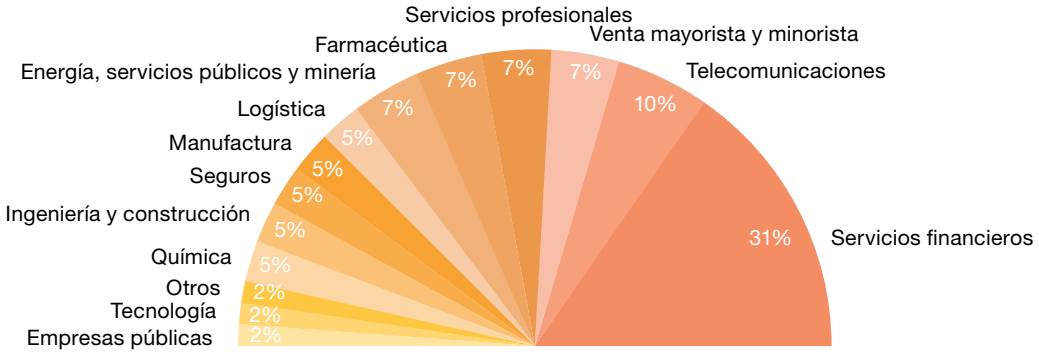
**Gráfico 7. Tamaño de la organización**




En tal sentido, la encuesta nos dice que las compañías argentinas con más de 500 empleados reportaron mayor cantidad de fraudes (85%) que las compañías con menos de 500 (15%). Estas cifras confirman la tendencia de la región y del resto del mundo.

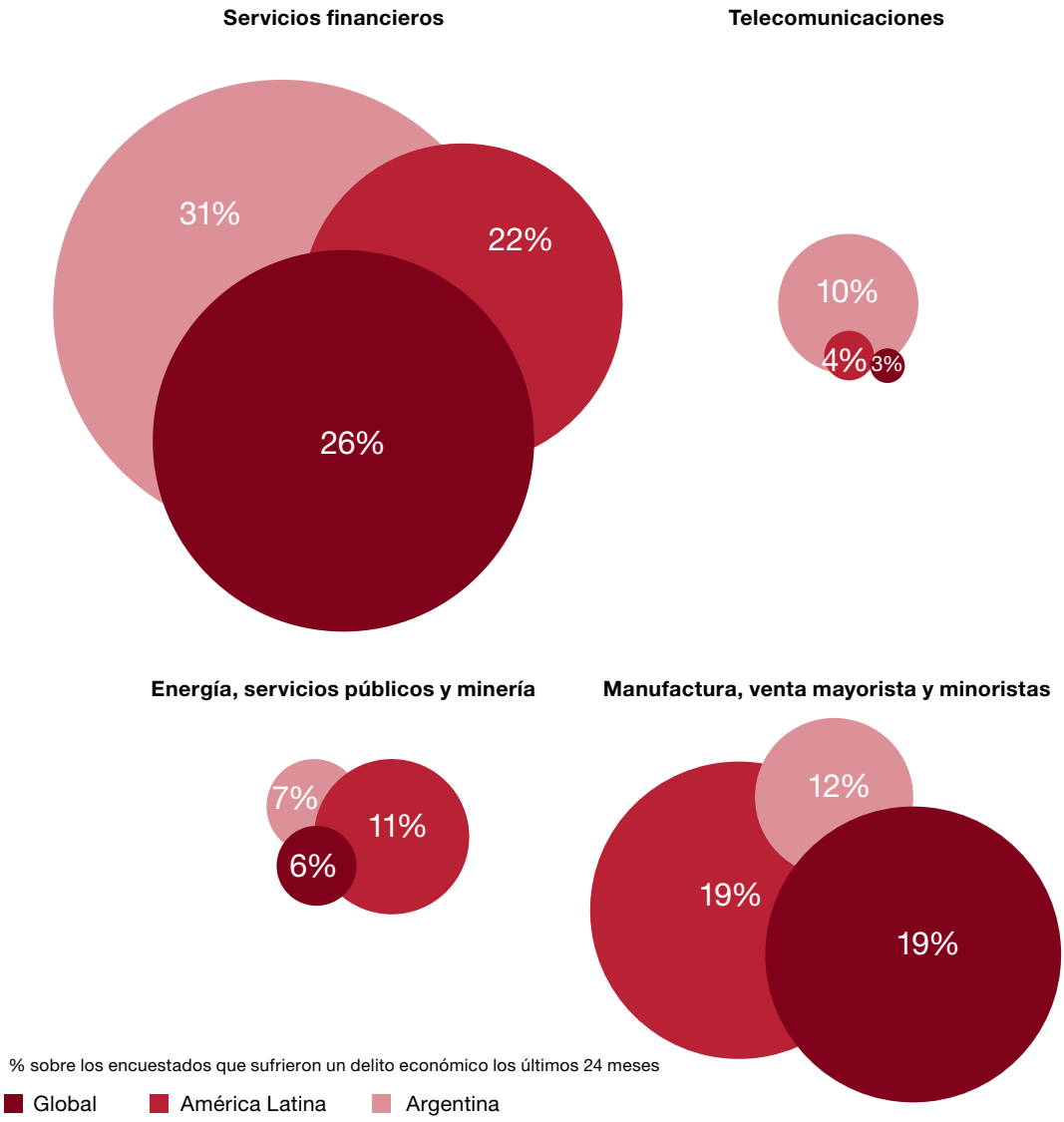
Con respecto a la industria, los **servicios financieros** continúan a la cabeza de las más atacadas a nivel local y global. El perpetrador tiende a preferir cometer el delito que le permita hacerse del efectivo del modo más sencillo posible. Es decir, va a preferir clonar una tarjeta de débito y extraer dinero de un cajero automático, que apropiarse de mercadería la cual después tendrá que venderla en algún mercado informal. Más allá de este factor, observamos que los fraudes se encuentran diseminados en todos los sectores de la economía.

## Gráfico 8. Delitos económicos reportados por industria en Argentina




% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

## Gráfico 9. Industrias más atacadas



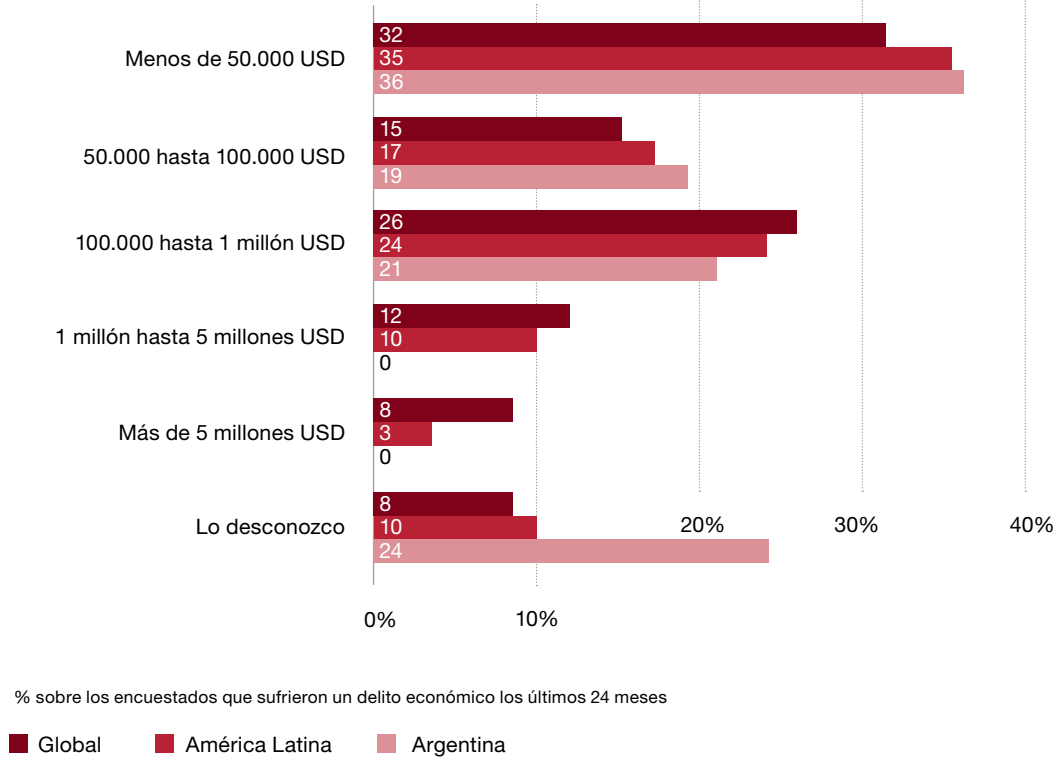

% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

Global América Latina Argentina

## El daño

Las organizaciones a menudo no logran comprender el verdadero daño de un delito económico. Como en años anteriores, nuestro estudio pone en relieve que el costo del fraude en las organizaciones es un factor que ninguna empresa puede desestimar y que el impacto total de los daños no puede ser medido únicamente de manera monetaria.

**Gráfico 10. Cuantificación del perjuicio económico causado directamente por los delitos económicos reportados (en USD)**




Como indica el gráfico, un 40% de las organizaciones argentinas víctimas de un incidente tuvieron un impacto financiero que osciló los 50.000 y el millón de dólares. Además, la edición de este año arrojó un dato más que interesante, casi el 24% de los encuestados que sufrió un delito económico en los últimos 24 meses en Argentina no sabe cuál fue el impacto financiero que éste originó a la compañía, más del doble que en Latinoamérica (10%) y el mundo (8%).

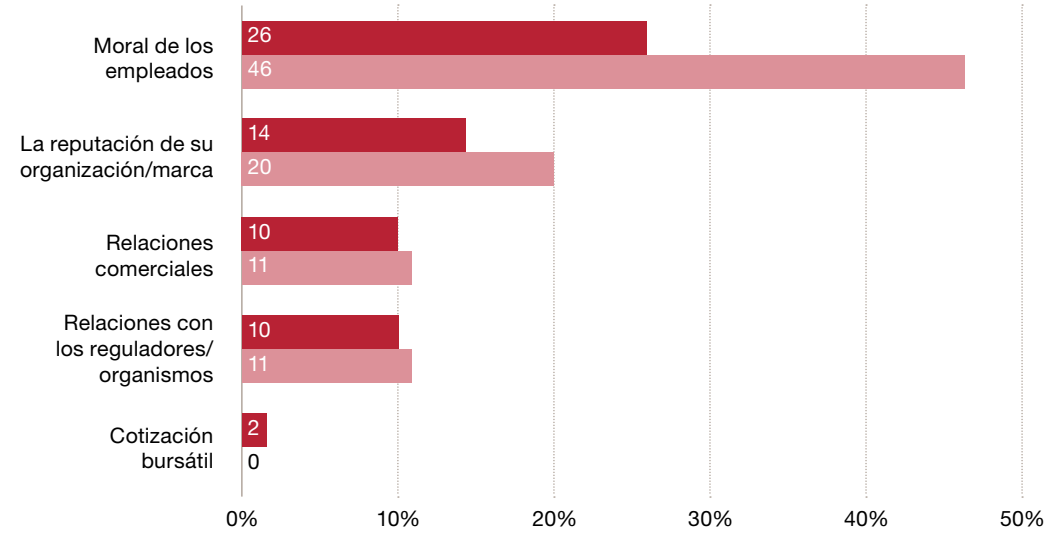
Este último factor, junto a la inexistencia de organizaciones que han reportado algún caso de fraude con un impacto mayor a los 5 millones de dólares en Argentina, nos indicaría que en nuestro país es más difícil poder cuantificar la incidencia de un delito económico cuando éste es de mayor magnitud en términos monetarios.

## Daño colateral: difícil de cuantificar, difícil de ignorar

La pérdida económica no es la única preocupación que las empresas enfrentan en la lucha contra el fraude. Al igual que en ediciones anteriores, nuestros encuestados señalaron como algunos de los daños colaterales más graves causados por los delitos económicos:

- la moral de los empleados;
- la reputación de la organización y de la marca; y
- las relaciones comerciales.

**Gráfico 11. Daños colaterales causados por los delitos económicos**




% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

Argentina 2014 Argentina 2011

Al tomar en cuenta los daños colaterales, el costo real de un delito económico puede provocar un impacto de larga duración. Si bien es difícil cuantificar este tipo de pérdidas en términos estrictamente financieros, hay un hecho que es claro: si el fraude implica perder clientes o proveedores (porque se niegan a continuar la relación comercial), empleados que prefieren cambiar de trabajo o talentosos recursos que deciden no aplicar a un puesto en la organización, definitivamente el impacto se sentirá en el mediano plazo en los resultados de la compañía.

En otras palabras, la larga cadena de efectos adversos que conlleva sufrir un delito económico, tales como la pérdida de ingresos, la pérdida de clientes, la baja en el precio de las acciones, la disminución de la productividad, el aumento del costo de la mano de obra y el daño en la moral de los empleados, no sólo pueden ser difíciles de valorar de forma individual, sino que también son imposibles de ignorar.

Afortunadamente, la alta dirección parece haber comprendido ésto. Nuestra 17° Encuesta Anual Global de CEOs informa que el 55% de los directores ejecutivos locales, ve "la falta de confianza en las empresas" como una problemática, por lo cual atacar esta cuestión se ha transformado en algo clave. Una mayoría significativa reconoce que las empresas tienen un papel más amplio en la sociedad que la mera construcción de valor para los accionistas.

## ¿Qué nos depara el futuro?

Así como aumentó la cantidad de fraudes reportados, también creció la preocupación de sufrir un fraude en los próximos 12 meses. En particular, 5 tipos de delitos económicos sobresalen como los más temidos por las organizaciones:

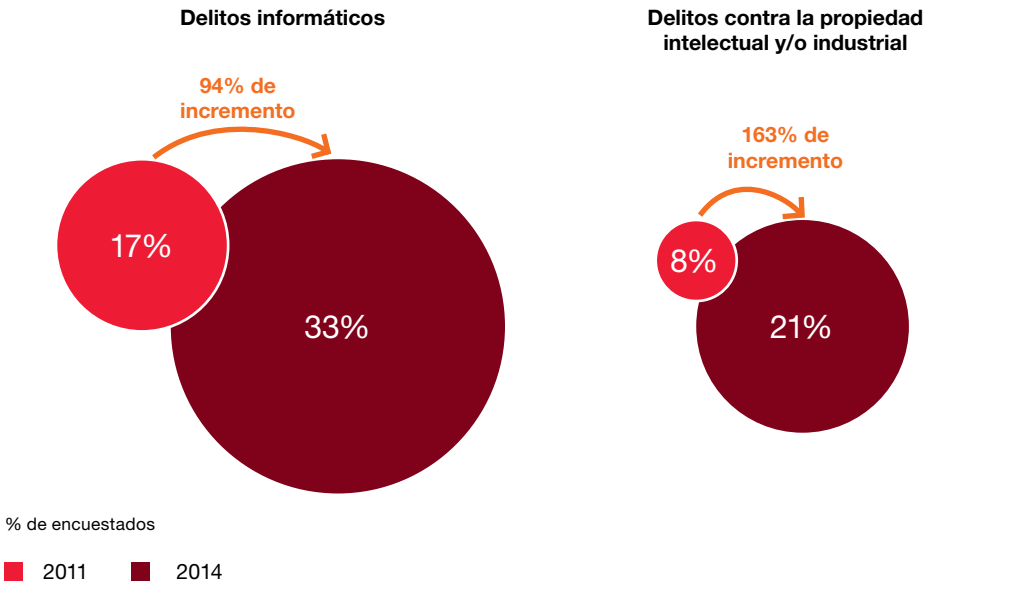
**Gráfico 12. Las mayores amenazas**

| 2014 | | 2011 |
|---|---|---|
| 1. | Malversación de Activos | 1. |
| 2. | Delitos informáticos | 5. |
| 3. | Fraudes en compras y contrataciones | S/D |
| 4. | Abuso de información privilegiada | 3. |
| 5. | Fraude en los estados contables | 2. |
| 6. | Soborno y corrupción | 4. |

S/D: nueva categoría agregada en 2014

Más allá de lo expuesto, no queremos que el lector pierda de vista que ha crecido exponencialmente la preocupación de las empresas por dos tipos de delitos económicos: delitos informáticos y delitos contra la propiedad intelectual y/o industrial.

**Gráfico 13. Las amenazas que toman protagonismo**



## ¿Cómo podemos defendernos?

Analizando la cantidad de compañías que efectuó una evaluación de riesgo de fraude al menos una vez al año, podemos mencionar las siguientes aseveraciones:

- Así como Argentina se posiciona entre los 10 países que proporcionalmente mayor cantidad de fraudes reportó, también se ubica en la cima de los países que respondieron no haber realizado una evaluación del riesgo de fraude en los últimos 24 meses o desconocerlo (55% de las empresas encuestadas).

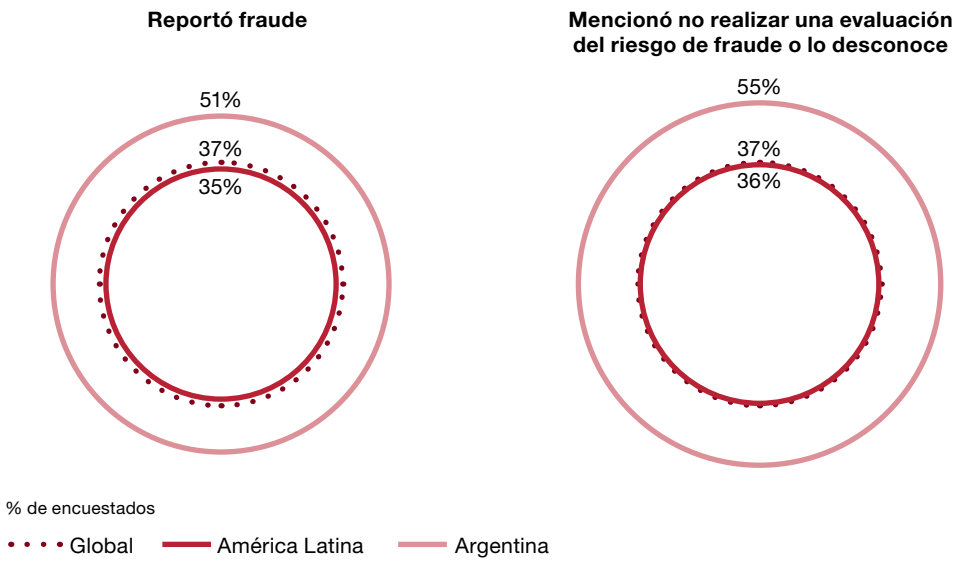
**Gráfico 14. Países que proporcionalmente mayor cantidad de encuestados desconocen o no han realizado una evaluación de riesgo de fraude en los últimos 24 meses**

| | |
|---|---|
| Botsuana | 80% |
| Angola | 77% |
| Túnez | 65% |
| Namibia | 62% |
| Turquía | 55% |
| **Argentina** | **55%** |
| Suecia | 52% |
| Argelia | 50% |
| Bahréin | 50% |
| **Latinoamérica** | **36%** |
| **Global** | **37%** |

% de encuestados

- Desde la perspectiva local y regional, también Argentina se encuentra por encima de la media. En Latinoamérica solo el 36% de las organizaciones mencionó no realizar una evaluación de riesgo de fraude o desconocerlo.

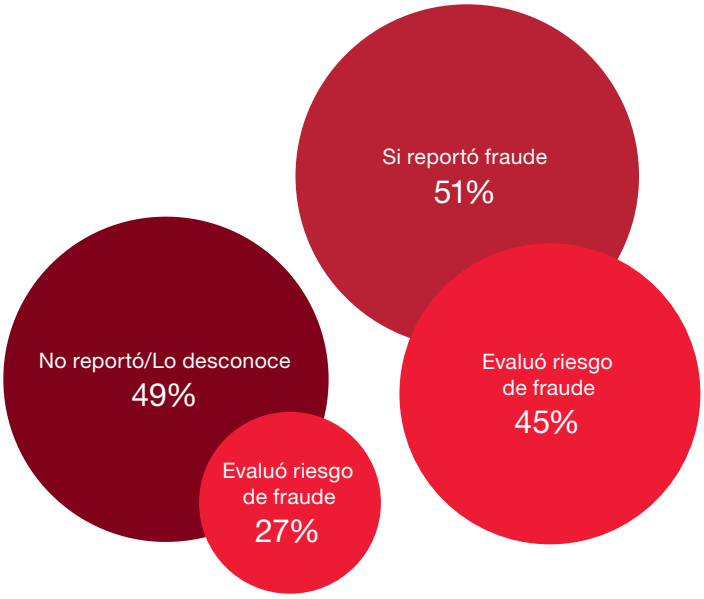
**Gráfico 15. Evaluación de riesgo de fraude**



## ¿Por qué una evaluación de riesgo de fraude?

Nuestra experiencia indica que uno de los primeros pasos en la lucha contra el fraude, es conocer a qué riesgos de fraude está expuesta la organización. Haciendo esta evaluación, facilitaremos la detección de un incidente y estaremos mejor preparados para afrontar nuevas amenazas.

**Gráfico 16. La evaluación del riesgo de fraude y el porcentaje de casos reportados**




% de encuestados

*Al igual que en nuestras últimas dos ediciones, observamos que continúa existiendo una correlación entre la cantidad de fraudes reportados y las evaluaciones del riesgo de fraude llevadas a cabo por las organizaciones.*

*En 2013 la SEC sancionó a 2 compañías por un total de 14 millones de USD por delitos cometidos en Argentina.*

# ***Bajo la lupa de los organismos regulatorios***

## Soborno, corrupción y lavado de activos en primera plana

Problemas como el soborno y la corrupción o el lavado de activos son temas ya conocidos en el ámbito de los negocios. Sin embargo, siguen planteando amenazas importantes a las organizaciones globales, más en un mundo interconectado como el actual. En ese contexto, gobiernos y organismos internacionales incrementaron la regulación y los controles para combatirlas. En nuestro país existen organismos que combaten el fraude y la corrupción tales como la recientemente creada PROCELAC (Procuraduría de Criminalidad Económica y Lavado de Activos) y las ya conocidas UIF (Unidad de Información Financiera) y la Oficina Anticorrupción. Durante 2012, estos organismos iniciaron 352[1] investigaciones (Oficina Anticorrupción) y abrieron 17[2] nuevos sumarios (UIF). Asimismo en la región, se están realizando algunas de las siguientes acciones:

- Brasil aprobó en 2013 una nueva ley anticorrupción que impone nuevas responsabilidades a las personas jurídicas del sector privado. Esta ley prohíbe aquellas prácticas corruptas cometidas por estas compañías ante la administración pública tanto local como extranjera, y plantea sanciones administrativas y judiciales, que no son excluyentes.
- En México, en 2012 entró en vigencia la Ley Federal Anticorrupción en Contrataciones Públicas. El objetivo de la ley, en este caso, es el establecimiento de responsabilidades y sanciones para personas físicas y jurídicas en lo que respecta a las infracciones en las que incurran, en su participación en las contrataciones públicas tanto domésticas como en el exterior.

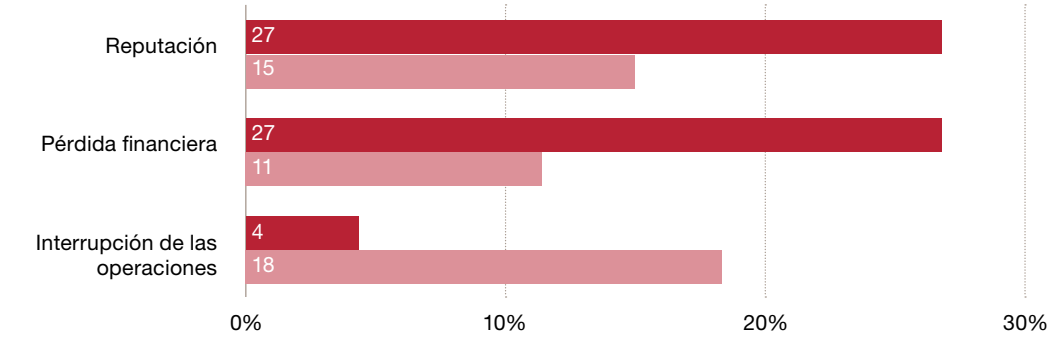
En el resto del mundo, entre las acciones que se están llevando a cabo en países como Estados Unidos en su lucha contra el fraude y la corrupción, vale la pena mencionar las sanciones aplicadas por la Securities Exchange Commission de los Estados Unidos (SEC). En 2013, este organismo penalizó a 8 compañías por cometer actos de corrupción alrededor del mundo. **El dato importante aquí es que 2 de esas 8 compañías fueron sancionadas por sus delitos cometidos en Argentina, por una suma total de casi 14 millones de dólare**s.

Además de las multas y acusaciones criminales, estas violaciones pueden ser vistas como emblemas de problemas para las organizaciones más grandes, y desencadenar daños en la reputación (incluyendo la desaprobación pública, opiniones no deseadas en los medios, litigios y/o reacciones adversas en el precio de las acciones), pérdidas financieras, interrupciones en los planes de negocio y fugas de talento.

Considerando todo lo comentado y conforme se exhibe en el siguiente gráfico, el daño a la reputación, la interrupción de las operaciones y la pérdida financiera son los impactos que más preocupan a las organizaciones argentinas.

1. Informe anual de gestión 2012 – Oficina Anticorrupción, Ministerio de Justicia y Derechos Humanos.
2. Informe de gestión 2012 – Unidad de Información Financiera, Ministerio de Justicia y Derechos Humanos.

**Gráfico 17. Impacto más preocupante**




% sobre los encuestados que sufrieron un delito económico los últimos 12 meses

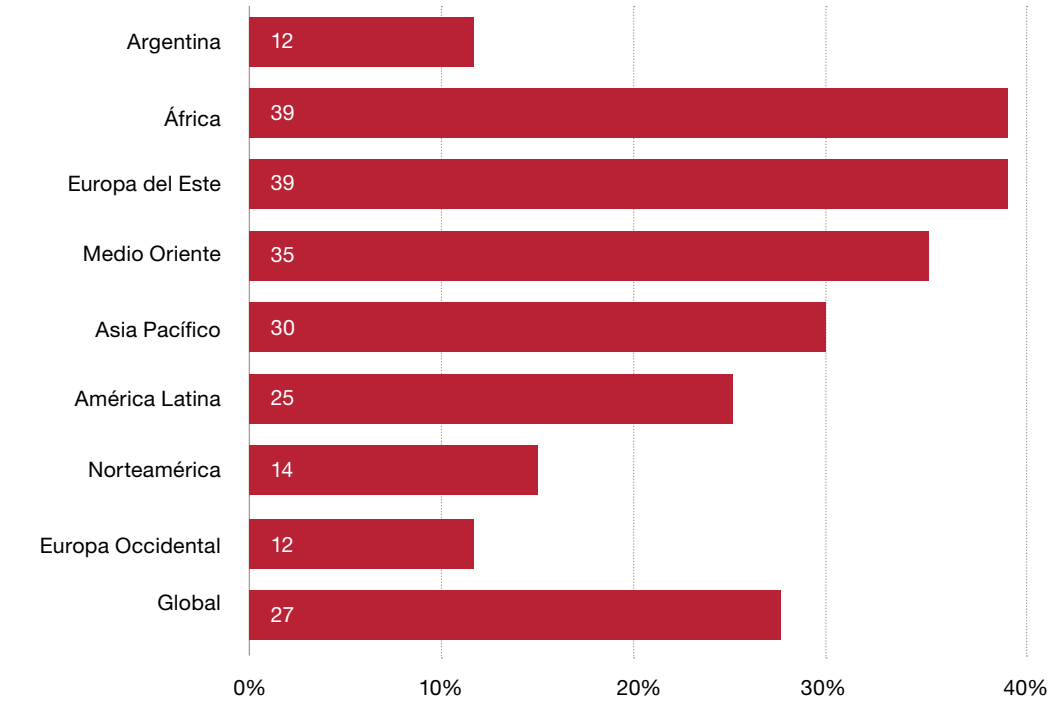
Soborno y corrupción  Lavado de activos

# El desafío de Argentina

*34% de las organizaciones argentinas ubican al soborno y corrupción como una de las amenazas de los próximos 12 meses.*

El soborno y la corrupción ocupa el tercer lugar (27%) entre los delitos económicos sufridos por las organizaciones a nivel global en los últimos 24 meses. Sin embargo, en el caso de Argentina, la tasa de casos no supera el 12%, muy por debajo inclusive de la media de la región.

**Gráfico 19. Soborno y corrupción por región**




% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

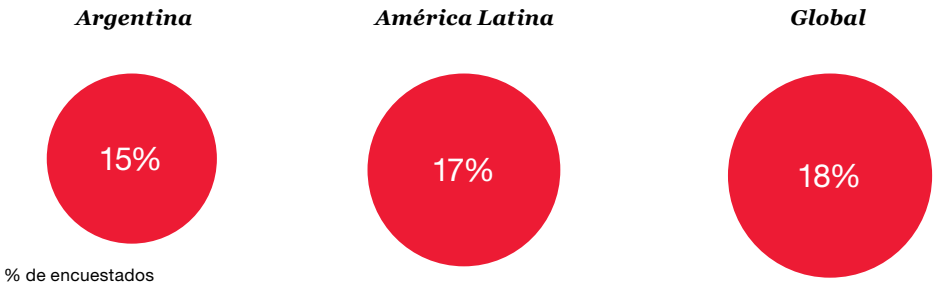
3. Escala del 0 al 100. El número más alto corresponde a un país mas transparente.

En cambio, cuando nos referimos al futuro, 34% de las compañías argentinas ubican al soborno y la corrupción como una de las amenazas de los próximos 12 meses, en línea con América Latina (35%) y el resto del mundo (29%). ¿Será que Argentina percibe que hay mayor cantidad de casos de soborno y corrupción de los que realmente suceden? ¿O será que los casos de soborno y corrupción son más difíciles de detectar, porque generalmente involucran a personas que ocupan altos cargos y tienen las atribuciones suficientes para ocultar el delito más tiempo?

Como mínimo podemos plantear que las organizaciones se encuentran seriamente expuestas a ser víctimas de este tipo de delitos.

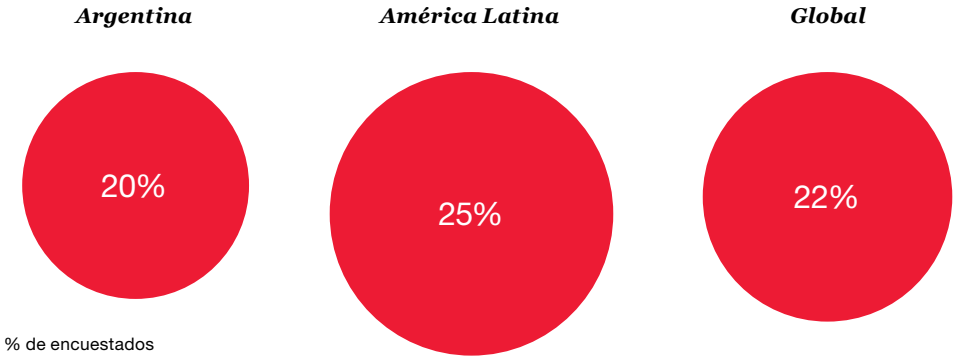
*20% de los encuestados locales perdió una oportunidad de negocio con un competidor que ha pagado un soborno, tendencia que Argentina comparte con el resto de los países.*

**Gráfico 20. Porcentaje de empresas que se les fue solicitado un soborno**




% de encuestados

**Gráfico 21. Porcentaje de empresas que perdieron una oportunidad de negocios por no pagar un soborno**




% de encuestados

# El lavado de activos preocupa especialmente a las entidades financieras

En términos de delitos económicos, los servicios financieros son una industria diferente a las demás. El lavado de activos es una de sus principales preocupaciones, ya que presenta un riesgo para la entidad que no lo reporta. De hecho, las entidades financieras encuestadas creen que existe un mayor riesgo de lavado de activos que de corrupción y soborno. Más de un cuarto (27%) de las encuestadas a nivel global manifestaron un evento de lavado de activos en los últimos 24 meses.

Si bien los artilugios para lavar dinero varían en sofisticación y complejidad, el propósito no varía: tener acceso a las prestaciones y servicios de una entidad financiera. Para ello, siempre existe un factor común: la debilidad humana, ya sea por la incompetencia, por la corrupción o el dolo.

El desafío que impone esta amenaza sistémica es que no puede evitarse completamente -al menos sin tomar medidas irracionales como salir del mercado en cuestión- y los procesos de negocio deben afrontarla día a día en distintas etapas:

- ***Conozca a su cliente (KYC).*** Buscar potenciales clientes e integrar nuevos se ve directamente afectado por la amenaza de lavado de activos.
- ***Cumplimiento.*** Con la misma importancia, el lavado de activos amenaza los procesos de la entidad en materia de cumplimiento respecto de las operaciones: en la ventanilla de caja, en la sala de transferencia de dinero y en el procesamiento y cobro de cheques.
- ***Gestión del riesgo.*** El lavado de activos también amenaza los procesos de due diligence, de información de operaciones sospechosas y gestión del riesgo de una entidad, en particular cuando el riesgo se concentra en grupos de cuentas bajo control común o préstamos utilizados por personas que lavan dinero o cuando la capacidad de los sistemas de monitoreo está atrasada respecto de las plataformas de servicio utilizadas.

Considere la dificultad que enfrenta una entidad financiera internacional para administrar sus operaciones en distintos ámbitos culturales y legales -que está sujeta a las normas legales estrictas de una economía occidental desarrollada-. Se debería capacitar a los cajeros, por ejemplo, para que puedan identificar e informar lo que podrían ser ***"operaciones sospechosas"*** ya sea por **la suma, moneda y frecuencia de los depósitos, la identidad del depositante o la naturaleza inexplicable del negocio**.

La entidad podría estar operando en una cultura conocida por la violencia o intimidación a las personas no dispuestas a colaborar, por la deferencia a los pedidos de las personas adineradas, o en una cultura en la que la corrupción es habitual. Podría estar operando en un ámbito donde existen relativamente grandes diferencias entre la situación económica de los clientes y la de los empleados bancarios, lo que genera que existan regalos o amenazas para allanar el camino para el uso inadecuado del sistema financiero por parte de quienes realizan estas operaciones, las aprueban o denuncian.

El lavado de activos tiene amenazas colaterales. Este delito daña a la reputación y otorga publicidad negativa. Las cargas adicionales incluyen el costo operativo de cumplir con nuevas regulaciones de cumplimiento, vigilancia y la actualización que surja de otros procesos de negocio.

Por otro lado hoy en día existe otro desafío que enfrentan los sistemas operativos y de cumplimiento en los bancos: las redes de pago alternativas que utilizan monedas ***"virtuales"***. Si bien las operaciones en estos sitios pueden ser "virtuales", están respaldadas por depósitos reales en entidades financieras de todo el mundo.

Por lo tanto, operar en ámbitos que generan una amenaza sistémica de lavado de activos a los procesos de negocio de las entidades financieras constituye un **desafío crucial**. Los artilugios de lavado de activos no sólo son numerosos y sofisticados sino que además crean una tensión significativa entre metas tan loables como ***conseguir y prestar servicios a un cliente rentable y operar con una entidad que acate totalmente las normas de múltiples jurisdicciones.***

*Puede que muchas organizaciones ni siquiera se percaten que están en la mira, o se enteren mucho tiempo después, cuando el daño ya está hecho.*

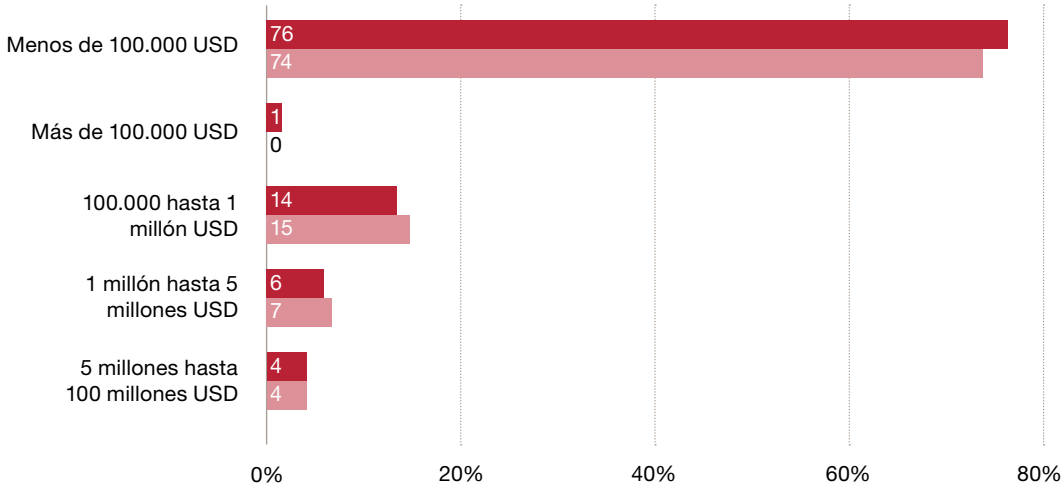
# *Delitos informáticos*
## Los riesgos de un planeta interconectado

El avance de la tecnología, combinado con el explosivo crecimiento de las redes sociales y la conectividad de datos alteró definitivamente las relaciones entre las empresas y los consumidores.

Desafortunadamente, esta conectividad tiene un lado oscuro. El delito informático opera en las sombras y puede que muchas organizaciones ni siquiera se percaten que están en la mira, o se enteren mucho tiempo después, cuando el daño ya está hecho.

Este solo factor convierte a los delitos informáticos en uno de los delitos más peligrosos.

**Gráfico 22. Pérdida financiera por delitos informáticos**




% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

Global América Latina

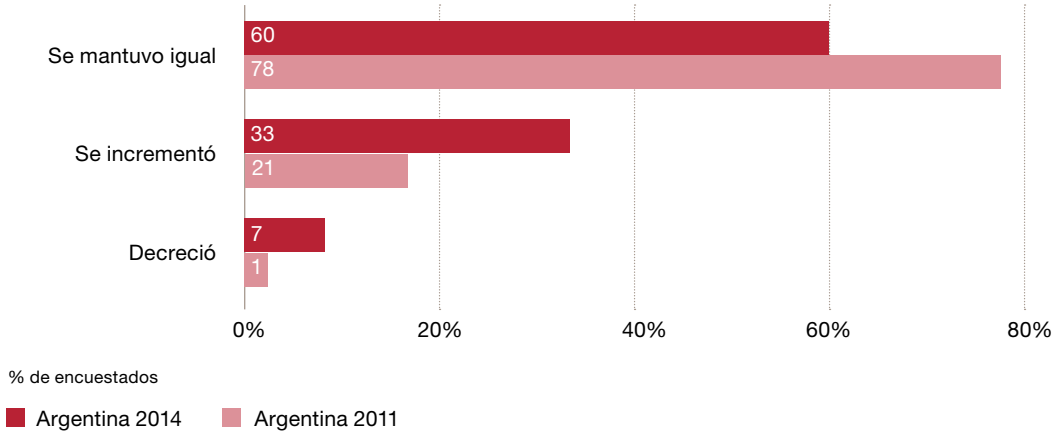
*Aumentó 16 puntos porcentuales la percepción de ser víctima de un fraude en los próximos 12 meses.*

# Una seria amenaza para las compañías argentinas

Nuestro informe de 2011 fue el primero de la serie en destacar los delitos informáticos como una amenaza que exigía la atención de las organizaciones: un 9% de los encuestados en Argentina reportaron ser víctimas de este tipo de delito. Ahora, en el 2014, el porcentaje de casos saltó al 21% (20% en Latinoamérica y 24% a nivel global). Es decir, los delitos informáticos se convirtieron en el segundo tipo de fraude más reportado por las empresas en Argentina.

Esta tendencia también se confirma con la creciente percepción de sufrir un delito informático. Este año, **el 33% de los encuestados sostiene que su empresa se encuentra más expuesta a ser víctima** de un delito informático en los próximos 12 meses, casi un 50% más con respecto al 2011 (21%).

**Gráfico 23. Percepción de sufrir un delito informático en los próximos 12 meses**




## Lo que no sabe y puede causarle daño

Aquellos que informaron no haber sufrido un delito informático pueden ser víctima y ni siquiera saberlo. Esto es un verdadero motivo de preocupación.

Este panorama se complica, en muchas ocasiones cuando es detectado el delito informático, éste no se denuncia. A menudo (como en los casos de robo de propiedad intelectual), puede haber razones de competitividad para que las organizaciones mantengan silencio.

La conclusión es que gran parte de los daños causados por este tipo de ataques no se dan a conocer, ya sea porque desconocen su existencia, porque son difíciles de cuantificar, o bien porque no se desean compartir. Naturalmente, este tipo de comportamientos plantea riesgos para un ecosistema global de negocios, cada vez es más dependiente de la tecnología y de la propiedad intelectual.

Es un entorno peligroso aquél donde puede ser más fácil robar un activo intangible vital, que cuantificar, revelar o al menos darse cuenta de una pérdida de este tipo.

## *Un objetivo en movimiento*

En un contexto tecnológico cambiante, los adversarios sofisticados sacan ventaja atacando nuevas debilidades. Este es el motivo por el cual las compañías tratan al menos de no perderles el ritmo a los delincuentes que las acechan.

Incluso cuando las organizaciones están al tanto de los tipos de ciber-amenazas que enfrentan, muchas no comprenden realmente la capacidad de los ciber-delincuentes, cuáles pueden ser sus objetivos y cuál será el valor de esos objetivos. Las compañías continúan poniendo su información crítica a disposición de la gerencia, los empleados, proveedores y clientes a través de una gran cantidad de plataformas, que pueden ser de alto riesgo, como los dispositivos móviles y la "nube", dado que los beneficios económicos y competitivos parecen ser convincentes.

Si bien nadie espera que los beneficios de la tecnología disminuyan ni que las entidades reduzcan su huella digital, resulta claro que –con más información accesible en más plataformas- la información valiosa estará amenazada, y el costo de las violaciones de seguridad continuará siendo elevado. De hecho, en cada región, entre un cuarto y un tercio de las compañías manifestaron creer que sufrirán delitos informáticos en un futuro cercano.

### Los delitos informáticos son un problema estratégico

Creemos que los delitos informáticos no son un problema de la tecnología estrictamente hablando. Sino que son un problema estratégico, humano y de procesos.

Las organizaciones no están siendo atacadas por computadoras, sino por personas que intentan aprovecharse tanto de la fragilidad humana como de la vulnerabilidad técnica. Motivo por el cual, dicha problemática requiere una respuesta en los procesos de negocio, accesos, autoridad, delegación, supervisión y conciencia, y no solamente en herramientas y tecnologías.

Esto se puede ilustrar al menos de cuatro maneras. En primer lugar, las personas son el vínculo más débil en la cadena de seguridad. Los **hackers**, con frecuencia, **se aprovechan de la ingenuidad humana** a través de ataques tales como "spear phishing" (suplantación de identidad) – es un abuso informático realizado a través de un correo electrónico de una fuente confiable, como un banco - para tomar ventaja sobre el usuario distraído. Los hackers pueden tratar de desencriptar códigos de datos, o pueden adivinar, robar o sobornar para conseguir una contraseña. La encriptación se duplica cada 18 meses, pero la habilidad del cerebro humano para recordar una contraseña compleja, sin escribirla, no ha mejorado.

En segundo lugar, **los hackers pueden innovar tanto sus procesos tecnológicos como los no tecnológicos**. Por ejemplo, puede identificar una falla en el sistema de cajeros automáticos y coordinar que varias personas, al mismo tiempo, en diferentes cajeros, extraigan dinero, aprovechándose de la debilidad. Ello refleja cómo la "productividad" del hacker ha multiplicado su eficacia en magnitud; no porque emplee nuevas tecnologías, sino por el mejor uso organizado de las "mulas".

En tercer lugar, **las soluciones de seguridad informática generalmente requieren del uso de herramientas y procesos no tecnológicos:** capacitación y concientización, involucramiento de expertos en asuntos privados o legales, relación con los medios, manejo de crisis y planes de remediación de soluciones para descubrir el delito cibernético.

Finalmente, una seguridad efectiva requiere que la gente **esté concentrada en sus datos más importantes**. Las empresas que realizan un inventario de sus activos de información y priorizan los datos de sus redes, son capaces de concentrarse en sus bienes más preciados, y usarán de manera astuta sus limitados presupuestos para combatir delitos informáticos.

La seguridad informática es una cuestión de negocios para la alta gerencia. El equipo de TI tiene que conocer cuáles son las mejores herramientas y tecnologías para la compañía, pero no podrán ayudar mucho si la **protección de los activos está erróneamente enfocada**.

## *Los delitos informáticos amenazan los procesos de negocio que utilizan tecnología.*

El creciente uso de procesos de negocio que utilizan tecnología hace que los delitos informáticos sean una verdadera amenaza para una amplia gama de operaciones comerciales. En nuestra experiencia reciente, los sistemas más amenazados son aquellos que contienen datos personales, o que se relacionan de manera directa con activos financieros que pueden ser robados. Las amenazas son:

- ***Puntos de venta*** de compras cotidianas por medio de tarjeta de débito o crédito.
- ***Transacciones bancarias*** en cajeros automáticos.
- ***Privacidad de los clientes***. Debe ser preservada y respetada. Esto es particularmente importante en la industria del cuidado de la salud, donde los proveedores por lo general tienen sistemas con información crítica de pacientes, incluyendo identidad, posición financiera, plan de seguro médico y estado de salud.
- ***Comercio electrónico o procesos de venta en línea***. Igual que la penetración de los sistemas de puntos de venta en los comercios minoristas o en bancos, excepto que éstos se producen en línea.
- ***Comunicaciones de negocio electrónicas (correo electrónico)***. Los ciber-delincuentes externos pueden acceder a los sistemas de comunicación corporativos y robar información –crítica- comercial, propiedad intelectual y comunicaciones ejecutivas confidenciales.
- ***Puntos débiles de la infraestructura*** para perpetrar algunos de los delitos expresados anteriormente. Por ejemplo, accediendo a puntos de acceso WIFI o interceptando las comunicaciones de otras personas a través de estos puntos de acceso, o atacando los entornos de servidores que son mantenidos por un prestador de servicios en la "nube".
- ***Incentivos a los consumidores***. La lealtad y otros programas de incentivo que retienen datos de los clientes y sus hábitos/preferencias de gastos, ofrecen un gran volumen de datos que pueden ser utilizados para el robo de identidad y para convertirse en blanco de otros delitos informáticos.
- ***Fusiones y Adquisiciones***. Luego de realizada una fusión o adquisición, la compañía podría demorar la integración completa de las políticas de seguridad de la información, procesos y herramientas. Esto conlleva vulnerabilidades en el ambiente de TI a nivel corporativo, que puede ser aprovechado por hackers, accediendo a bases de datos que contienen propiedad intelectual y demás información confidencial valiosa.
- ***Cadena de abastecimiento***. Los proveedores, contratistas y distribuidores son parte del ecosistema de una compañía - con frecuencia, el personal está autorizado a acceder a datos y sistemas confidenciales. El riesgo de ellos, es su propio riesgo, y una ruptura en la cadena de abastecimiento puede tener efectos en cascada en la seguridad de las redes o, peor aún, permitir el acceso directo a información confidencial.
- ***Investigación, desarrollo e ingeniería***. Las tecnologías propias, los secretos comerciales y la propiedad intelectual son blancos de países, empresas gubernamentales y corporaciones poco éticas. Las empresas han perdido miles de millones de dólares a través del robo, por parte de hackers o personal interno, de propiedad intelectual para beneficiar a los competidores.
- ***Expansión a nuevos mercados***. Cuando una empresa ingresa en un mercado geográficamente nuevo, puede convertirse en el blanco del gobierno o de los competidores locales que quieren robarle su tecnología, listado de clientes o planes de comercialización. Si la empresa está literalmente de "visitante", el problema del personal interno se extiende más allá de los empleados, alcanzando a proveedores de instalaciones, consultoras, servicios de mantenimiento e inclusive organismos gubernamentales.

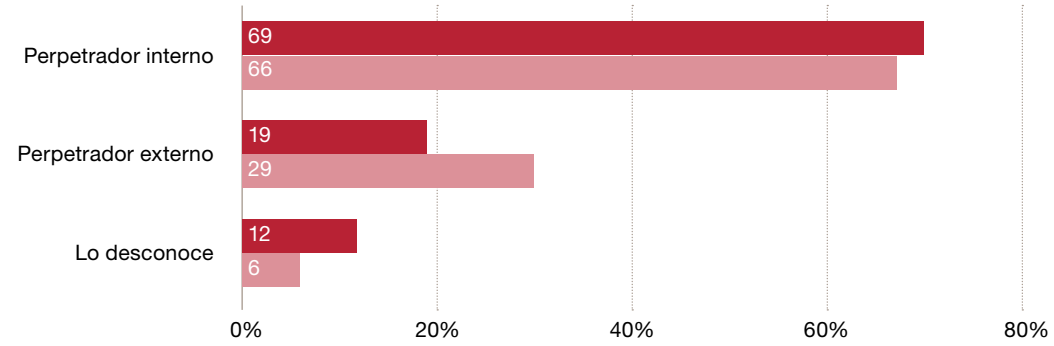
*La amenaza de sufrir un fraude continua siendo mayormente interna.*

# *Defraudador: conociendo a su enemigo*

Al igual que cualquier batalla, **una regla de oro en la lucha contra los delitos económicos es conocer al enemigo**. En este sentido, es interesante que el 69% de los encuestados señaló como interno al principal perpetrador, continuando la tendencia de nuestra anterior encuesta (66%).

Sin embargo, pareciera ser que no todas las organizaciones están convencidas de esta "regla de oro", o todavía no la lograron aplicar eficazmente. El 12% de los encuestados desconoce si el perpetrador fue interno o externo. Esta cifra no sólo dobla la del 2011, sino que también es superior a la de América Latina (7%) y el resto del mundo (4%).

**Gráfico 24. Perpetrador del fraude**




% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

Argentina 2014 Argentina 2011

Conocer de dónde proviene la amenaza nos permite distribuir mejor los esfuerzos: si la amenaza es externa, entonces reforzaremos en primer lugar aquellos procesos donde la participación de terceros es relevante.

**Gráfico 25. Procesos de negocio bajo amenaza**

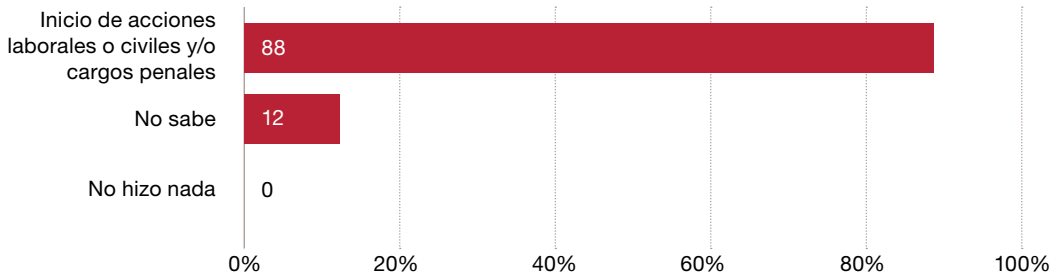
| Industria | ¿Qué procesos/áreas reforzar? |
|---|---|
| Servicios financieros | Alta de clientes |
| | Otorgamiento de préstamos |
| | Transacciones a través de home-banking |
| Energía, servicios públicos y minería | Contratación de servicios, contratistas y locaciones |
| Productos industriales y consumo masivo | Venta canal mayorista |
| | Transporte de mercadería |
| Seguros y Salud | Pago a prestadores de servicio |
| | Reintegro de gastos a beneficiarios |
| | Pago de siniestros |

Al contrario, si el perpetrador es interno, en principio todo proceso es vulnerable, y más que nunca debemos enfocarnos en la cultura de la organización:

- predicando con el ejemplo por parte de la alta dirección,
- transmitiendo los principios y valores de la organización con un código de ética,
- implementando una línea de denuncias independiente, confidencial y anónima donde un empleado pueda denunciar una situación irregular y, sobre todo,
- teniendo tolerancia cero cuando un incidente ocurre.

Analizando los tipos de fraude cometidos, de 28 organizaciones argentinas que reportaron haber sufrido un delito de malversación de activos, 23 identificaron que el delito fue cometido por un perpetrador interno. Sabiendo que el perpetrador más frecuente trabaja en la propia empresa, las **organizaciones disponen de un amplio abanico de herramientas para prevenirlo y disuadirlo**, desde mejorar las actividades de control de cada proceso de negocio expuesto a un siniestro, hasta la aplicación de sanciones ejemplificadoras a los empleados infieles. Justamente, nuestra encuesta nos muestra que el 83% de las organizaciones víctimas de un delito iniciaron acciones laborales, civiles y/o penales contra el perpetrador.

**Gráfico 26. Acciones realizadas por las empresas argentinas para con el perpetrador**




% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

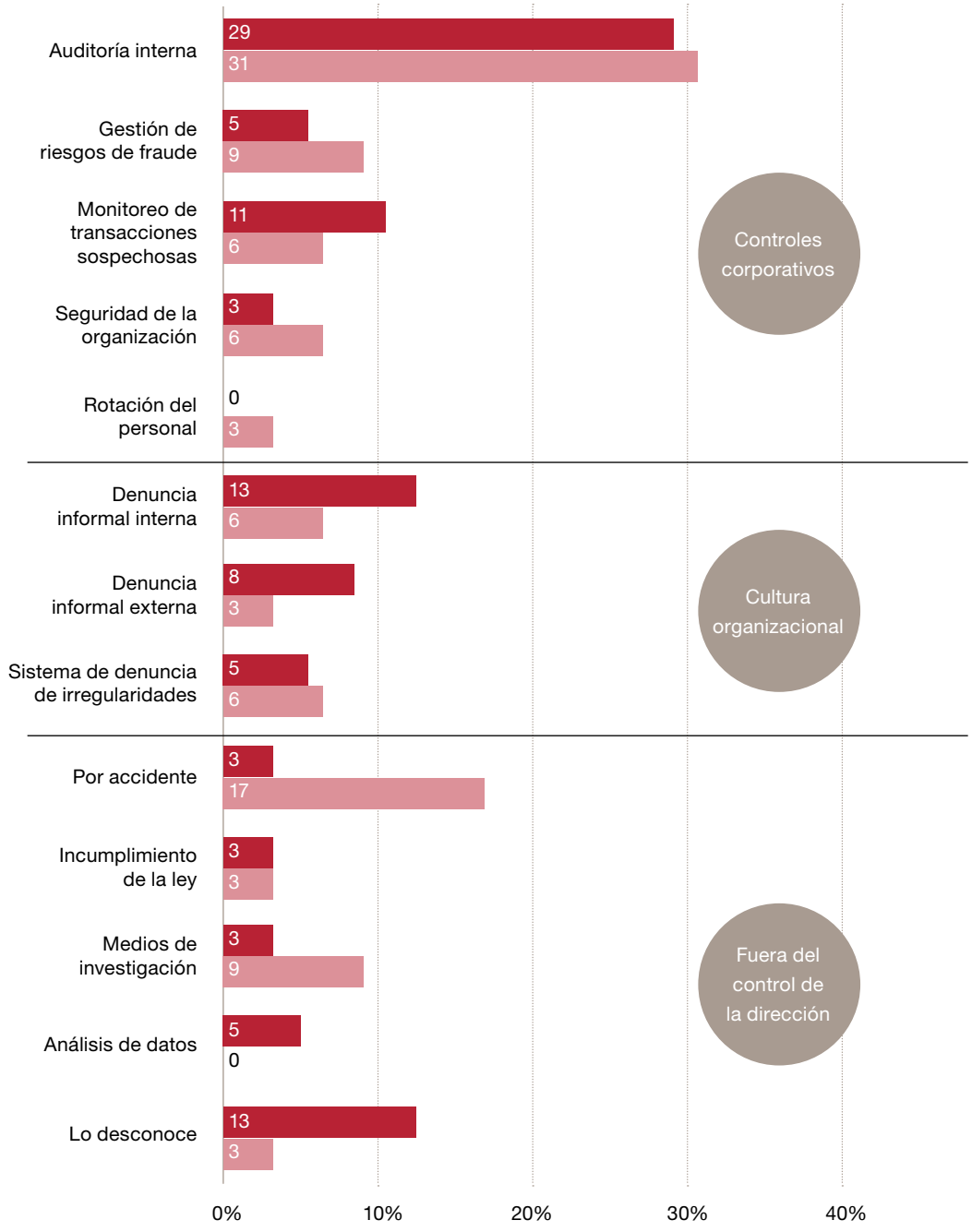
Argentina 2014

# Capturar al ladrón

Entonces, ¿cómo prevenir y/o detectar un delito económico antes que suceda o, por lo menos, mientras está ocurriendo?

Los métodos de detección de fraude por lo general se encuadran en una de estas tres categorías: controles corporativos, cultura organizacional o eventos fuera del control de la dirección. El siguiente gráfico muestra los métodos mediante los cuales se detectó al defraudador.

**Gráfico 27. Métodos de detección de fraude utilizados**




% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

Argentina 2014 Argentina 2011

Al igual que 2011, **auditoría interna** continúa siendo el método que más casos de fraude detectó en nuestro país, mientras que a nivel global el monitoreo de transacciones sospechosas se consolida como el más utilizado. Igualmente, este año podemos observar un leve cambio en ciertas categorías de detección, empezando a **imitar las tendencias globales**. Notamos un crecimiento tanto en el monitoreo de transacciones sospechosas como en el análisis de datos.

**Gráfico 28. Métodos de detección más utilizados**

| | Argentina | América Latina | Global |
|---|---|---|---|
| 1° | Auditoría interna | Auditoría interna | Monitoreo de transacciones sospechosas |
| 2° | Denuncia informal interna / Lo desconoce | Análisis de datos | Auditoría Interna |
| 3° | Monitoreo de transacciones sospechosas | Monitoreo de transacciones sospechosas | Evaluación del riesgo de fraudes |

Por último y no menos importante, llama la atención el incremento en el número de encuestados que indicaron desconocer cómo fue detectado el fraude con respecto a las cifras de la encuesta de 2011. Ante este dato, hay que recordar que no hay método más eficaz que la **"sensación de control"** o la de **"ser descubierto"**.

## Sistema de denuncia de irregularidades

En términos de implementación de una línea de denuncias, 52 % de las compañías argentinas respondieron tenerla implementada. Si bien el porcentaje es considerable, aún se encuentra por debajo de la tendencia regional y global (66% y 62% respectivamente). Un dato relevante es que el 16% de los encuestados en Argentina desconoce si su compañía posee un mecanismo de línea de denuncias, 8% a nivel global y 7% en Latinoamérica. Que los empleados desconozcan si su empresa aplica esta herramienta, revela que **la difusión** de este mecanismo, de haberse implementado, **no fue del todo efectiva**.

## Fraude interno: el enemigo escondiéndose de la vista de todos

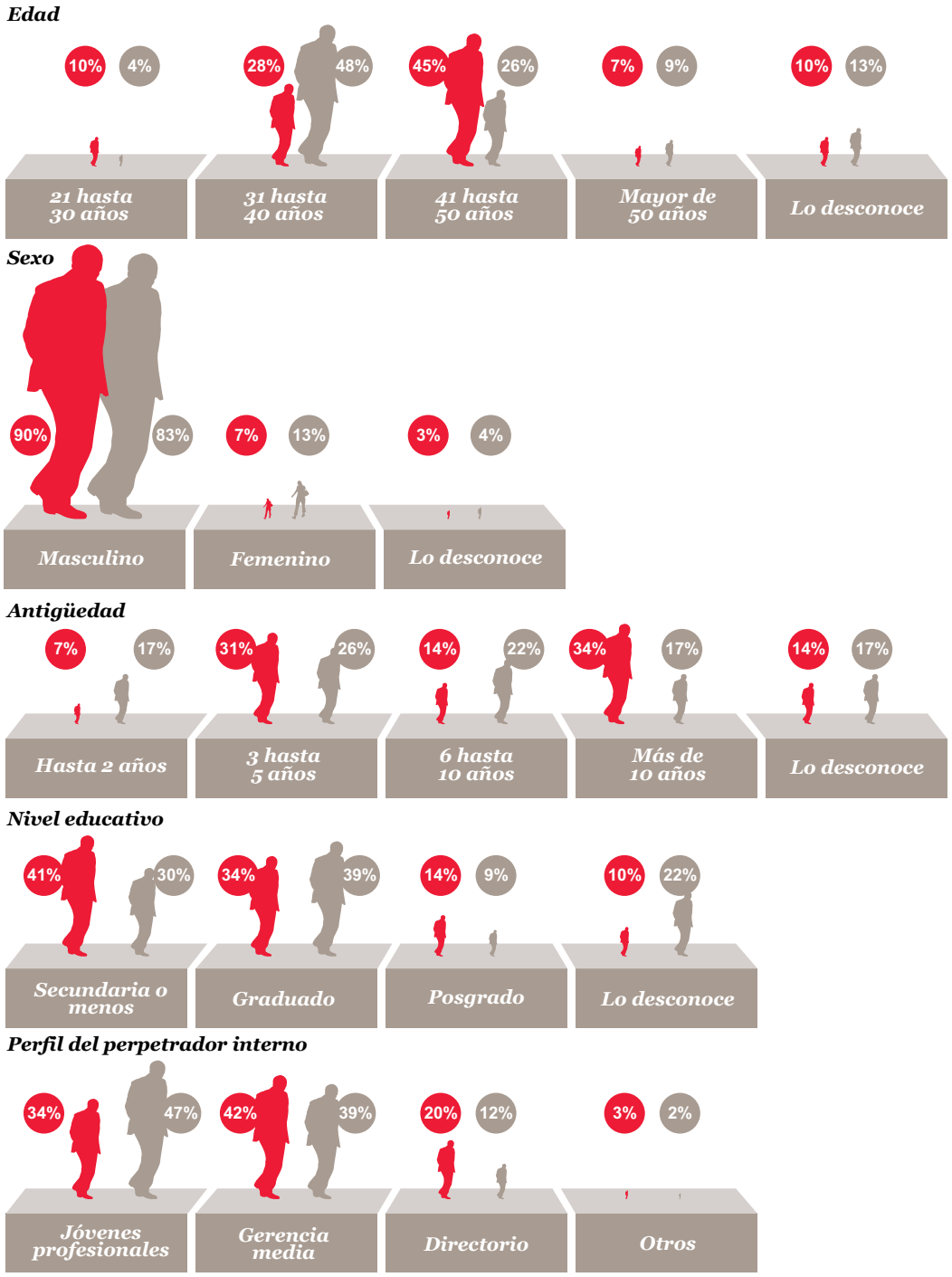
Los profesionales de la práctica contra el fraude se refieren comúnmente al "Triángulo del Fraude", haciendo referencia a tres elementos que a menudo están presentes cuando un perpetrador comete un delito económico: **la presión, la oportunidad y la racionalización**.

En nuestro país, 23 de 29 encuestados indicaron que la **oportunidad** fue el factor desencadenante para que el perpetrador cometa un fraude. Si bien esta noticia puede parecer decepcionante a primera vista, es importante tener en cuenta que, de los tres factores, la oportunidad es el más controlable por la organización. Mientras que las **presiones** y la **racionalización** pueden girar en torno a los empleados, si una organización puede limitar las oportunidades (ejemplo: mitigar el riesgo que un control falle), puede ser capaz de detener el fraude antes que éste comience.

Por otro lado, si bien no podemos especificar cuál fue la presión específica o la racionalización detrás de cada acto de fraude interno, al menos podemos describir el perfil del perpetrador más común: **gerente, de sexo masculino, de entre 41 y 50 años, con estudios secundarios y que ha trabajado en la organización por más de 10 años**.

Comparando con el 2011, este año el perpetrador resultó más grande de edad, con mayor antigüedad en la empresa y menor preparación académica. Ésto, nos confirma que el fraude es una amenaza latente, que atraviesa a la organización en todos sus estamentos, y quien lo comete es aquél que tuvo la capacidad de **identificar la oportunidad para poder cometerlo**.

**Gráfico 29. Edad, sexo, antigüedad, nivel educativo y perfil del perpetrador interno**




% sobre los encuestados que sufrieron un delito económico por un perpetrador interno

Argentina 2014 Argentina 2011

*82 encuestados argentinos completaron la Encuesta Global de Delitos Económicos 2014.*

# *Apéndice*
# Información regional

**Gráfico 30. Países que reportan menos fraude**

| País | 2014 | 2011 |
|---|---|---|
| Malasia | 24% | 44% |
| Italia | 23% | 17% |
| Turquía | 21% | 20% |
| Perú | 20% | 35% |
| Hong Kong / Macao * | 16% | N/A |
| Japón | 15% | 5% |
| Portugal | 12% | N/A |
| Dinamarca | 12% | 29% |
| Arabia Saudita** | 11% | N/A |
| **Global** | **37%** | **34%** |

*Parte de China 2011. ** Parte del Medio Oriente 2011

África sigue a la cabeza en cuanto a los delitos económicos reportados, aunque la brecha se ha reducido desde 2011. Medio Oriente presenta una situación única: bajos niveles generales de delitos económicos reportados pero los que informaron haber sufrido un hecho de fraude mostraron un alto número de tipos y casos de fraude.

**Gráfico 31. Fraude reportado por regiones**

| Región | 2014 | 2011 |
|---|---|---|
| África | 50% | 59% |
| Norteamérica | 41% | 42% |
| Europa del Este | 39% | 30% |
| Latinoamérica | 35% | 37% |
| Europa del Oeste | 35% | 30% |
| Asia Pacífico | 32% | 31% |
| Medio Oriente | 21% | 28% |
| **Global** | **37%** | **34%** |

# Acerca del perpetrador externo

Los resultados de la encuesta argentina no nos permitieron analizar la situación local de las organizaciones con respecto a los perpetradores externos. En virtud de ello, a continuación se exhiben los resultados más destacables de América Latina y globales.

**Gráfico 32. Perfil del defraudador externo**

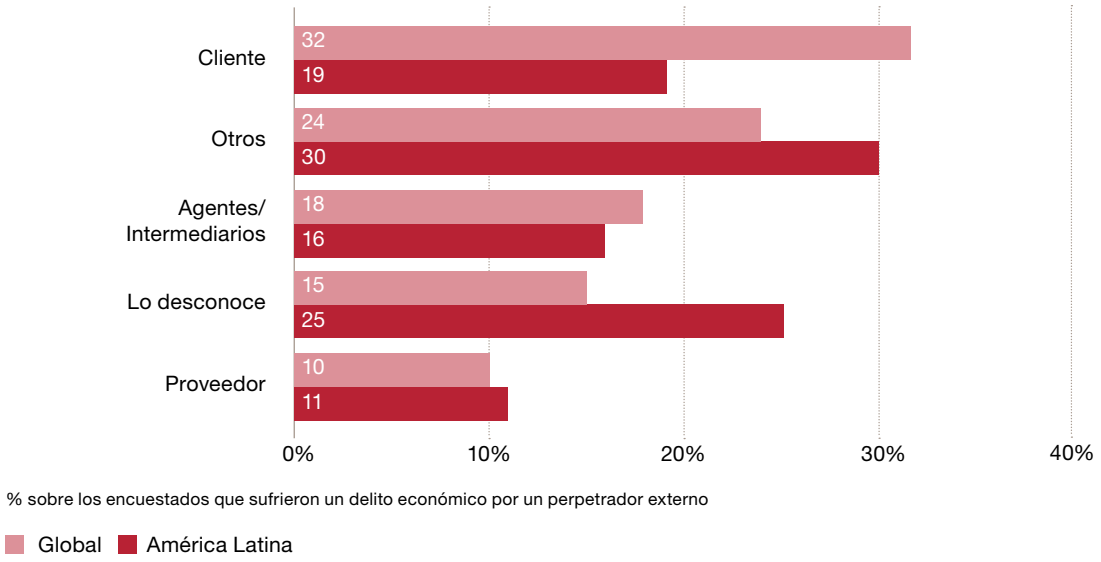
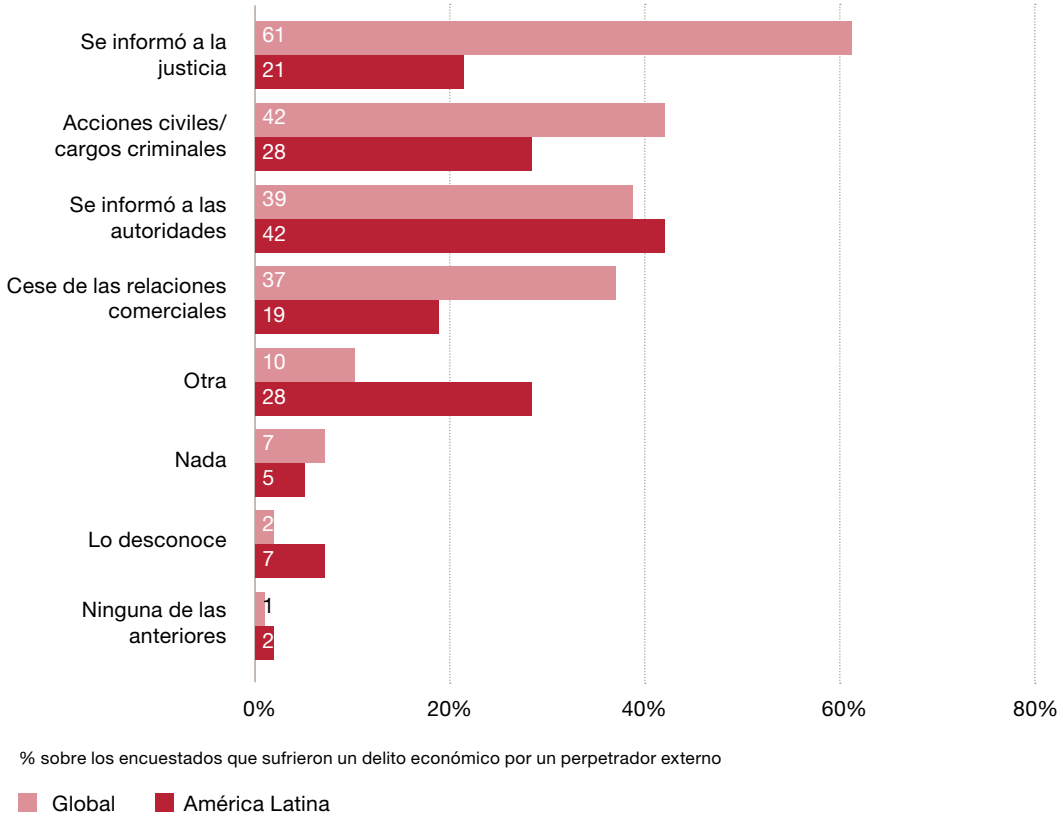



**Gráfico 33. Acciones llevadas a cabo contra los defraudadores externos**



# Metodología

Hemos llevado a cabo nuestra séptima Encuesta Global de Delitos Económicos entre agosto de 2013 y febrero de 2014.

La encuesta constó de cuatro secciones:

- el perfil general de los encuestados;
- las preguntas comparativas teniendo en cuenta qué delito económico habían experimentado las organizaciones;
- las amenazas del delito informático; y
- la corrupción/ soborno y el lavado de activos.

## *Acerca de la encuesta*

La Encuesta Global de Delitos Económicos 2014 se completó con 5.128 encuestados (frente a los 3.877 encuestados en 2011) de 99 países (en comparación con 78 países en 2011). En el caso de Argentina, 82 fueron las empresas encuestadas. Sobre el total de encuestados, 39% eran ejecutivos de la alta gerencia.

***Utilizamos las siguientes técnicas de investigación:***

***1. Encuesta de los ejecutivos en la organización.*** Los hallazgos de este estudio provienen de las respuestas brindadas por directivos empresarios acerca de los delitos económicos en sus organizaciones. Obtuvimos respuestas sobre los distintos tipos de delincuencia económica sufrida, el impacto en la organización (tanto la pérdida financiera como cualquier otro daño colateral), los perpetradores de estos delitos, qué medidas la organización adoptó y cómo respondieron frente a la delincuencia.

***2. Cuestiones relativas al delito informático, la corrupción / soborno y el lavado de dinero.*** Esta encuesta toma una mirada detallada a estas amenazas que suelen ser de carácter sistémico y por lo tanto son más propensas a ser de largo plazo, dañando con gran impacto a la organización.

***3. Análisis de las tendencias en el tiempo.*** Desde que empezamos a hacer estas encuestas en el año 2001, hemos hecho una serie de preguntas fundamentales, y algunas otras que son relevantes según el momento, lidiando con aspectos que probablemente tengan un impacto en las organizaciones de todo el mundo. Con estos datos históricos disponibles, podemos ver temas actuales, desarrollar gráficos, e identificar tendencias.

***Otras fuentes***:

- PwC—17ma. Encuesta Anual de CEOs [http://www.pwc.com/gx/en/ceo-survey/]
- PwC—Building Trust in a Time of Change: Global Annual Review 2013 [http://www.pwc.com/gx/en/annual-review/megatrends/index.jhtml]
- PwC—Global State of Information Security Survey [http://www.pwc.com/gx/en/consultingservices/information-security-survey/index.jhtml]
- PwC – 7ma. Encuesta Global sobre Delitos Económicos [http://www.pwc.com/crimesurvey]

## Gráfico 34. Posición de los encuestados argentinos

| | |
|---|---|
| Miembro del consejo de administración | 7% |
| Consejero delegado/ Presidente/ Director General | 7% |
| Director financiero/ Tesorero/ Controller | 9% |
| Director de sistemas de información/ Director Tecnológico | 4% |
| Director de seguridad | 2% |
| Director | 9% |
| Jefe de división | 5% |
| Jefe de departamento | 16% |
| Gerente | 38% |
| Otros | 3% |

## Gráfico 35. Tipo de organizaciones argentinas participantes

| | |
|---|---|
| Empresa cotizada (en Bolsa de Valores) | 34% |
| Privada | 56% |
| Sector público/ Empresa pública | 7% |
| Otras industrias/ sectores | 3% |

## Gráfico 36. Industrias participantes

| Industria | América Latina | Global |
|---|---|---|
| Servicios financieros | 22% | 26% |
| Telecomunicaciones | 4% | 3% |
| Venta mayorista y minorista | 11% | 10% |
| Servicios profesionales | 4% | 4% |
| Farmacéuticas | 6% | 4% |
| Energía, servicios públicos y minería | 11% | 6% |
| Logística | 6% | 5% |
| Manufactura | 8% | 9% |
| Seguros | 6% | 6% |
| Ingeniería y construcción | 6% | 5% |
| Química | 3% | 1% |
| Otros | 4% | 5% |
| Tecnología | 2% | 3% |
| Empresas públicas | 2% | 6% |
| Salud | 1% | 2% |
| Medios y entretenimiento | 1% | 2% |
| Automotriz | 6% | 3% |
| Defensa | 0% | 1% |

# Terminología

## Fraude en los estados contables

Alteración de los estados contables y/u otros reportes económicos-financieros de modo que no representen la realidad económica de las operaciones que realiza la organización. Ya sea a través de la manipulación de los principios contables, ocultando la verdadera situación patrimonial a la hora de tomar un préstamo, o por ejemplo para poder acceder a financiación en los mercados de capitales.

## Malversación de activos incluyendo engaño por parte de los empleados

El robo de activos (incluidos activos monetarios / dinero o suministros y equipamiento) por parte de los directores, aquellos que se encuentren en posiciones fiduciarias o cualquier empleado para su propio beneficio.

## Soborno y corrupción

El uso ilegal de una posición privilegiada obteniendo una ventaja en contraposición con el deber. Ésto puede implicar la promesa de un beneficio económico u otro favor, el uso de la intimidación o el chantaje. También puede referirse a la aceptación de incentivos. Por ejemplo: sobornos, extorsiones, regalos (con segundas intenciones), propinas, etc.

## Delito informático

Delitos económicos en los que se utilizan herramientas informáticas, tales como computadoras y/o Internet, que juegan un papel central, y no accidental o casual, en la comisión del delito.

## Delito económico

El uso deliberado del engaño para privar a otro tanto de dinero, propiedad o como de un derecho legal.

## Espionaje

Es el acto o la práctica de espiar o contratar espías para obtener información confidencial.

## Pérdida financiera

Cuando se estiman las pérdidas financieras debido al fraude, los participantes deberían incluir tanto la pérdida directa como indirecta. La primera refiere al costo del fraude y la segunda puede incluir los gastos relacionados con la investigación y remediación del problema, las sanciones impuestas por las autoridades oficiales y los costos judiciales.

Esto excluiría cualquier monto estimado a “pérdida de oportunidad de negocio”.

## Evaluación del riesgo de fraude

Las evaluaciones de riesgo de fraude se utilizan para determinar si una organización ha realizado acciones para establecer:

i. Los riesgos de fraude asociados a cada operación;

ii. Los riesgos críticos (es decir, evaluar los riesgos por impacto y probabilidad de ocurrencia);

iii. La identificación y evaluación de los controles clave (si los hay) vigentes para mitigar los riesgos;

iv. La evaluación del programa anti-fraude en general y los controles establecidos;

v. Las acciones para remediar las debilidades en los controles.

## Fraude en recursos humanos (Contratación y payroll)

Es realizado por los miembros del departamento de Recursos Humanos, incluyendo el fraude de payroll, empleados fantasmas, pagar para trabajar, contrataciones (ejemplo, contratar amigos y/o familiares, gente no capacitada, falsificación de documentos, etc.), entre otros.

## Incentivos / presión para trabajar

El individuo tiene un problema financiero que es incapaz de resolverlo legítimamente. Entonces considera que cometer un acto ilegal es su única manera de resolver el asunto. El problema financiero puede ser profesional (por ejemplo, el trabajo está en peligro) o personal (por ejemplo, una deuda de juego).

## Abuso de información privilegiada

El abuso de información privilegiada se refiere generalmente a la compra o venta de un título de valor, violando la obligación fiduciaria o en detrimento de otro tipo de relación de confianza. Es decir, la obtención de información relevante y no perteneciente al dominio público. Los incumplimientos relacionados con el abuso de información privilegiada también podrán incluir la divulgación de información privilegiada sobre esos títulos, la comercialización de títulos por parte de la persona que recibió esa información privilegiada, y la comercialización de títulos por parte de quienes se apropian indebidamente de esa información.

## Delito contra la propiedad intelectual y/o industrial (incluyendo marcas, patentes, falsificación de productos y servicios)

Esto incluye el robo de información de la compañía, la copia y/o distribución ilegal de productos falsificados que se encuentran en infracción ya sea de patente o derecho de autor, o la creación de monedas y billetes con la intención de que sean genuinos.

## Mercados con alto nivel de riesgo de corrupción

Basándonos en el Índice de Percepción de Corrupción del organismo "Transparency International", determinamos que para considerar un mercado de alto riesgo debe obtener una puntuación de 50 o menos.

## Lavado de activos

Acciones cuya intención es legitimar la procedencia de activos provenientes del crimen organizado, disfrazando su verdadero origen.

## Oportunidad o capacidad

El individuo encuentra alguna manera en que pueda abusar de su posición de confianza para resolver su problema financiero con un bajo riesgo de ser atrapado.

## Fraude en compras y contrataciones

Conducta ilegal por la cual el delincuente obtiene una ventaja, evita la obligación o daño a su organización. El delincuente puede llegar a ser un empleado, propietario, miembro del directorio, un funcionario, una figura pública o un proveedor que estuvo involucrado en la compra de servicios, bienes o activos de la organización afectada.

## Racionalización

El individuo encuentra la manera de justificar el delito cometido de una manera que hace que para él sea un acto aceptable o justificable.

## Fraude fiscal

Una práctica ilegal donde una organización o una corporación evitan intencionalmente el pago de su verdadera obligación fiscal

*PwC Forensic Services comprende especialistas en investigación de fraudes y en tecnología forense, contadores, economistas, actuarios y ex-funcionarios de la justicia. Ayudamos a las organizaciones a hacer frente a los principales riesgos financieros y reputacionales asociados a los delitos económicos. Identificamos irregularidades, analizamos complejos problemas de negocio, y mitigamos el riesgo de fraude.*

# Contactos


**Jorge C. Bacher**
Socio, Buenos Aires, Argentina
(+5411) 4850 6814
jorge.c.bacher@ar.pwc.com

**Andrés Sarcuno**
Gerente, Buenos Aires, Argentina
(+5411) 4850 6887
andres.sarcuno@ar.pwc.com

**Leandro Castro**
Financial and Accounting Investigations
Buenos Aires, Argentina
leandro.castro@ar.pwc.com

**Ignacio Aquino**
Socio, Buenos Aires, Argentina
(+5411) 4850 6816
ignacio.aquino@ar.pwc.com

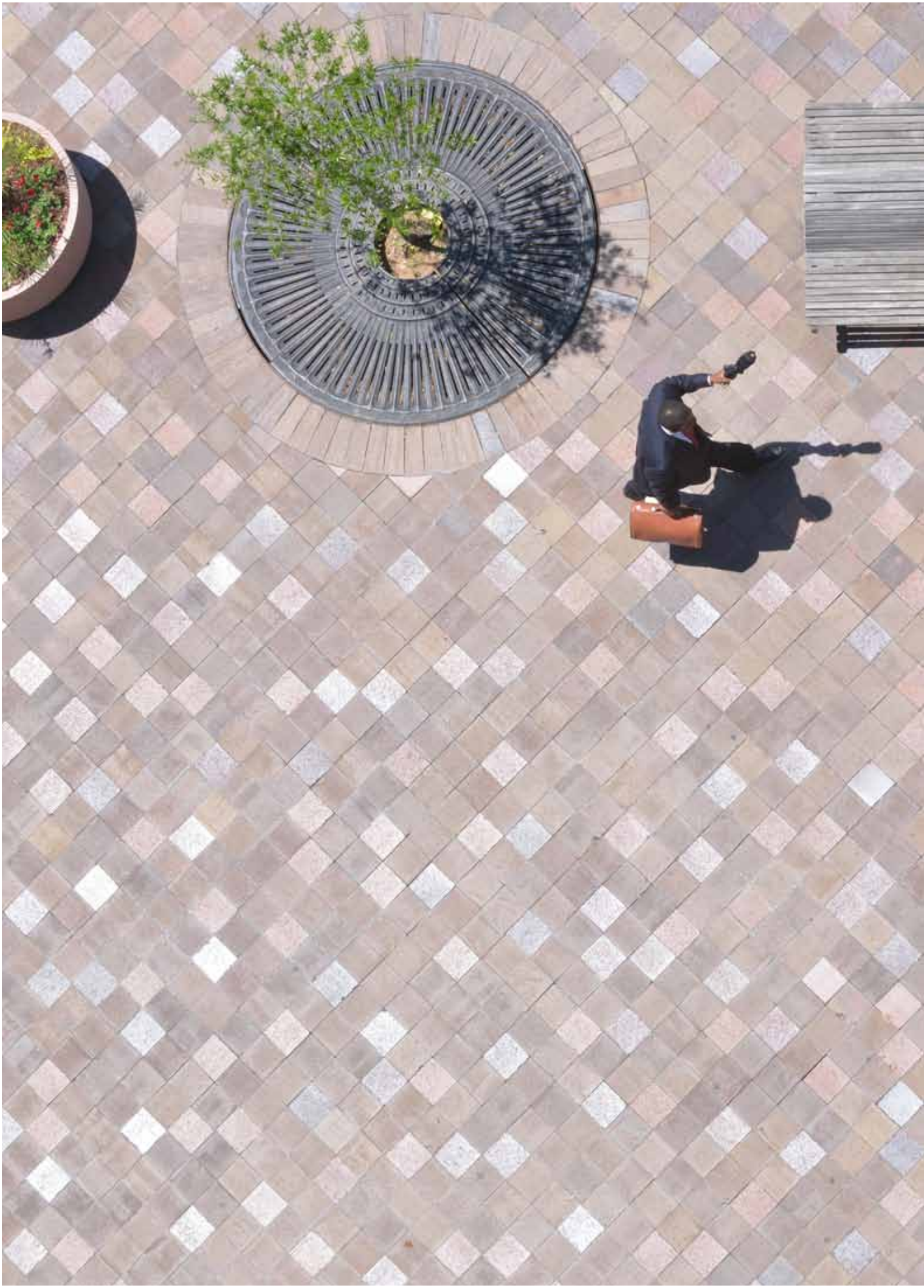
**Kurt Kolakauskas**
Gerente, Buenos Aires, Argentina
(+5411) 4850 6887
kurt.kolakauskas@ar.pwc.com

**Martin Strizic**
Corporate Intelligence
Buenos Aires, Argentina
martin.strizic@ar.pwc.com


### *Forensic Technology Solutions*


**Diego Taich**
Director, Buenos Aires, Argentina
(+5411) 4850 6834
diego.taich@ar.pwc.com

**Andrea Navarro**
Gerente, Buenos Aires, Argentina
(+5411) 4850 6243
andrea.navarro@ar.pwc.com



*www.pwc.com/ar*

Esta publicación ha sido preparada para una orientación general acerca de asuntos de interés solamente, y no constituye asesoramiento profesional.

Los receptores de la misma no deben actuar en base a la información contenida en esta publicación sin obtener asesoramiento independiente. No se efectúa manifestación ni se otorga garantía alguna (expresa o implícita) con respecto a la exactitud o integridad de la información contenida en esta publicación y, en la medida en que lo permite la ley, PwC Argentina, sus miembros, empleados y agentes no aceptan ni asumen ninguna responsabilidad, ni deber de cuidado por cualquier consecuencia de su accionar, o del accionar de terceros, o de negarse a actuar, confiando en la información contenida en esta publicación, o por ninguna decisión basada en la misma.

©2014 En Argentina, las firmas miembro de la red global de PricewaterhouseCoopers International Limited son las sociedades Price Waterhouse & Co. S.R.L, Price Waterhouse & Co. Asesores de Empresas S.R.L. y PwC Legal S.R.L, que en forma separada o conjunta son identificadas como PwC Argentina.

www.pwc.be/crimesurvey

# *Economic crime: a threat to business processes*

## Belgium report

*PwC's 2014 Global Economic Crime Survey*
***Belgium report***

*February 2014*

pwc

# Contents

# Opening statement

*It will surprise few to learn that economic crime – such as fraud, IP infringement, corruption, cybercrime, or accounting fraud – continues to be a major concern for organisations of all sizes, across all regions and in virtually every sector.*

That's one headline from our 2014 Global Economic Crime Survey, one of the broadest and most comprehensive economic crime surveys we have ever conducted, with over 5,000 respondents contributing from every corner of the world.

But the real story is not so much that economic crime stubbornly persists. The real story is that economic crime is threatening your business processes, eroding the integrity of your employees, and tarnishing your reputation. Which is why this year's report is focused on how and where it may be affecting you – so you can address the issue from both a preventive and a strategic perspective.

Probably most striking is the fact that in the past 24 months, 50% of the Belgian companies surveyed have been faced with one or more significant cases of economic crime.

Furthermore, as fraud continues to grow in sophistication and magnitude, it should come as no surprise to learn that economic crime continues to move up the CEO's agenda. More than half of chief executives, polled in our just-released 2014 Global CEO Survey, told us they are concerned or extremely concerned about bribery and corruption.

Economic crime, fundamentally, threatens the basic processes common to all businesses – paying and collecting, buying and selling, hiring and firing. Since close interaction with third parties is the foundation upon which virtually every business function is built, all organisations in the course of their daily business face exposure to various types of economic crime from multiple angles.

And the risks continue to evolve. Like a virus, economic crime adapts to the trends that affect all organisations. Especially impactful mega-trends include the increasing reliance on technology and technology-enabled processes across business, and the growing movement of economic energy toward emerging markets.

Our hope is that this report will serve all your stakeholders, from the board down, as both a useful reference point in an unending campaign – and a strategic tool in your business arsenal in the months to come.

**1 in 2** organisations
report being victims of economic crime

# *Highlights*

Economic crime is
**a persistent threat**
to business and business processes – 50% of Belgian respondents and 37% of global respondents reported economic crime.

The schemes used may vary, but
**the global threat remains**
Respondents from 65 territories reported experiencing economic crime.

**Economic crimes of a "systemic" nature,**
such as bribery and corruption, money laundering, and anti-competitive practices, are more regularly examined by regulators and represent a greater risk than "episodic" frauds.

The most damaging forms of economic crime
**exploit the tension between two equally fundamental business goals – profit and compliance.**
Organisations with operations in high risk markets were twice as likely to report being asked to pay a bribe.

**Cybercrime reports continue to rise.**
In Belgium it is the second-most reported type of crime in this year's survey while globally cybercrime is ranked fourth. However, cybercrime is not just a technology problem. It is also a business strategy problem.

**Economic crime follows mega-trends**
– such as the movement of wealth from the West to the South and East and the increasing use of technology platforms for all types of business processes.

Our CEO Survey reveals that more than half of CEOs are concerned about bribery and corruption:
**reported incidences are up to 27%,**
a relative increase of 13% from our last survey.

# Economic crime in 2014



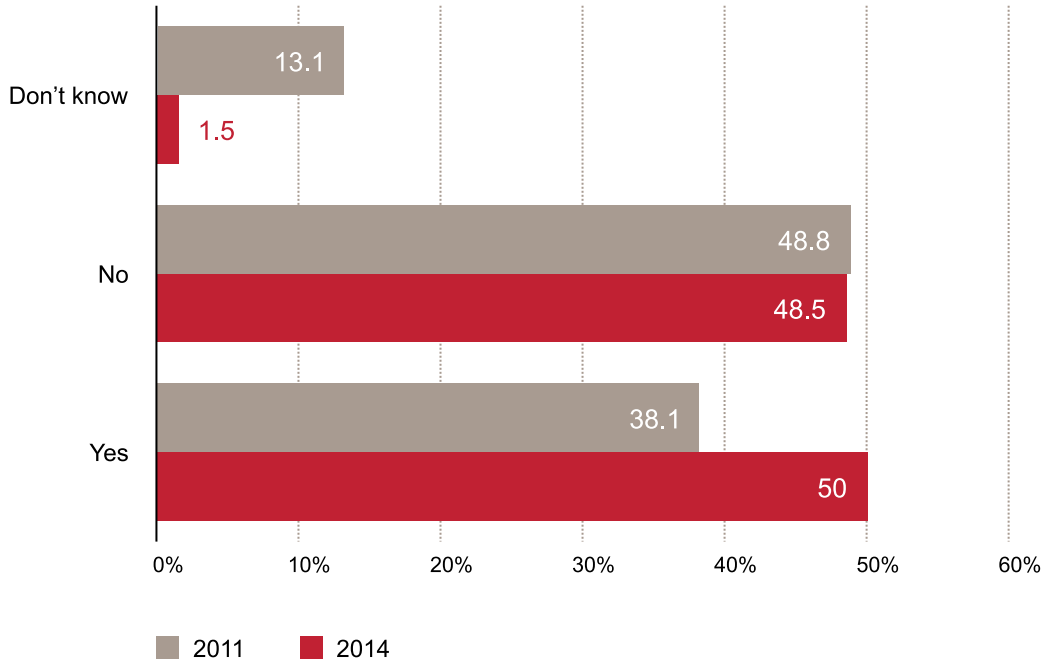
## The Big Picture

Our 2014 survey respondents included 5,128 representatives from over 95 countries around the world and 68 respondents from Belgium. Our survey responses indicate that, despite the best efforts of organisations, regulators and antifraud practitioners, economic crime continues to persist – touching companies across virtually the entire spectrum of industries and services.

### *Economic crime suffered*

In Belgium, half of the respondents reported that their organisation had experienced economic crime during the survey period, which is an increase of 12% compared to the 2011 survey. This increment might originate from the fact that only 1.5% didn't know how much economic crime they suffered; a decrease of 12% can be noticed in the 'don't know' category.

**Figure 1** – Economic crime suffered in Belgium (in %)



The same more or less stable trend can be detected in the global survey results. Around the world, 37% of our 5,128 respondents reported that their organisation had experienced economic crime during the survey period, which is an increase of 3% compared to the 2011 global survey. Here the percentage of global respondents ticking the 'don't know' category has remained more or less the same in 2014 compared to 2011.

Consequently, we can conclude that Belgian companies suffered more economic crime than the global average (in Belgium 50% versus 37% globally) and that the increasing trend compared to 2011 is more significant in Belgium than globally (in Belgium 12% versus a global 3%). However, note that the Belgian increase may be due to the fact that the respondents have become more aware in comparison with the 2011 survey. In addition, as we will discuss and explain in the cybercrime section in particular, all these percentages are likely to be underreported, with potentially troubling consequences.

## *Top territories reporting economic crimes*

5,128 respondents from 95 countries completed the 2014 Global Economic Crime Survey. We asked these respondents to indicate whether they had experienced economic crime in the last 24 months. Table 1 lists the top territories reporting economic crimes.

**Table 1** – Fraud by territory, high fraud

### *Top territories reporting fraud*

| Territory | Reported fraud 2011 | Reported fraud 2014 |
|---|---|---|
| South Africa | 60% | 69% |
| Ukraine | 36% | 63% |
| Russia | 37% | 60% |
| Australia | 47% | 57% |
| Papua New Guinea | n/a | 57% |
| France | 46% | 55% |
| Kenya | 66% | 52% |
| Argentina | 45% | 51% |
| Spain | 47% | 51% |
| **Global** | **34%** | **37%** |

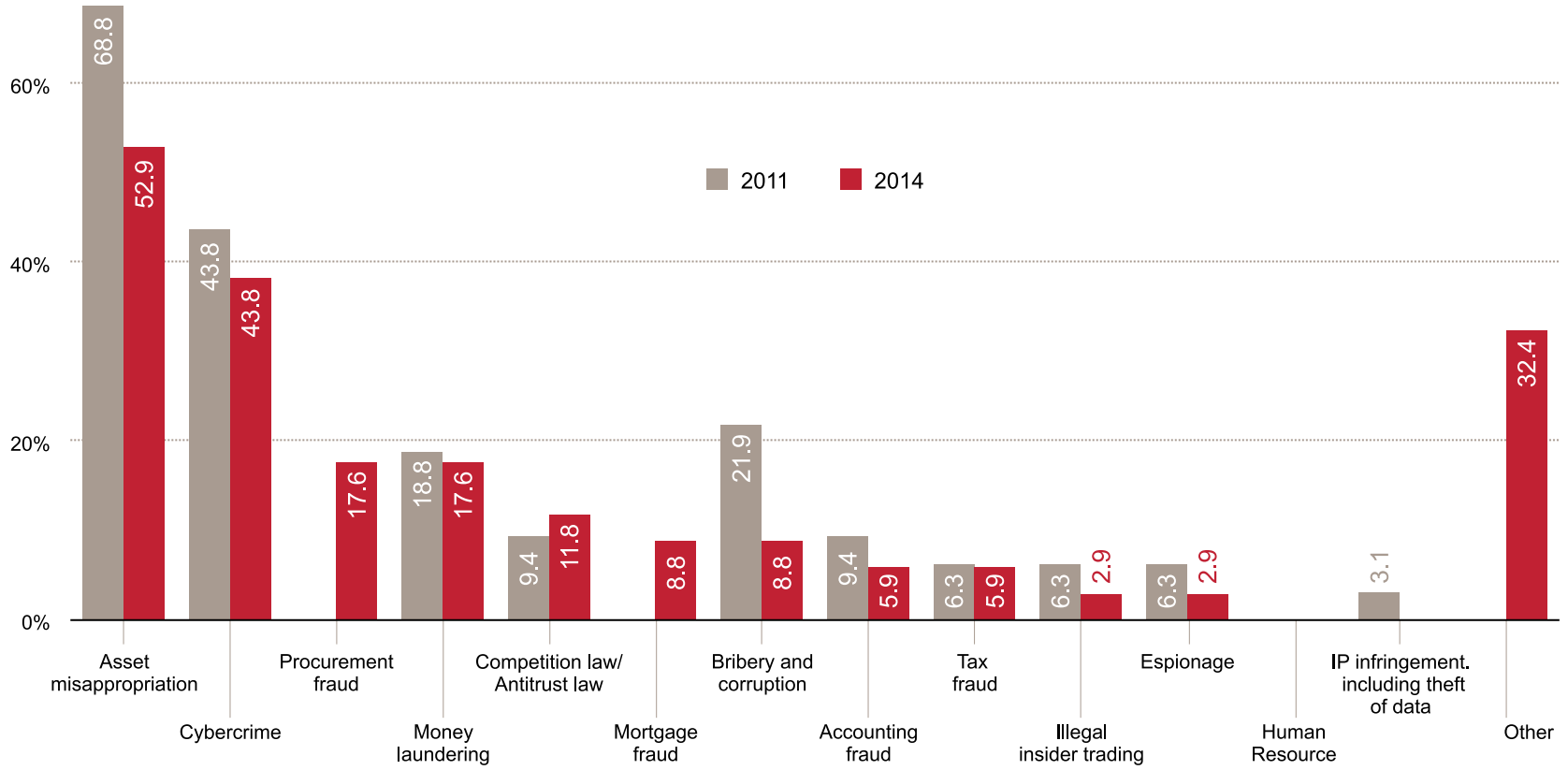
Belgium, reporting fraud levels of 50%, is clearly seen globally at the high end of fraud reported in 2014; and largely exceeds the global average of 37% as well as the Western European average of 35%. In Western Europe, only France (55%) and Spain (51%) have a higher score than Belgium.

## *Types of fraud*

Economic crime comes in many flavours, each with its own characteristics, threats and strategic consequences.

Figure 2 shows the types of economic crime reported by respondents. In this report, we will address the major crimes in more detail – analysing today's numbers and our respondents' predictions for tomorrow, discussing the business processes they attack, and offering insights into how to address these risks.

**Figure 2** – Types of fraud reported in Belgium (in %)



As in our previous surveys, asset misappropriation tends to be the most common type of economic crime suffered, both globally and in Belgium.

During our previous Economic Crime Surveys, the prevalence of this type of fraud had grown. This is the first year that asset misappropriation has experienced a decline in Belgium (-16%). Similarly, this is also the case for the 'bribery and corruption' category (-13%) and for the 'cybercrime' category (-6%). Moreover, in general, the percentages of all categories have dropped, except for the 'competition law/ antitrust law' category and the 'other' category. Two potential reasons can be identified for these declines:

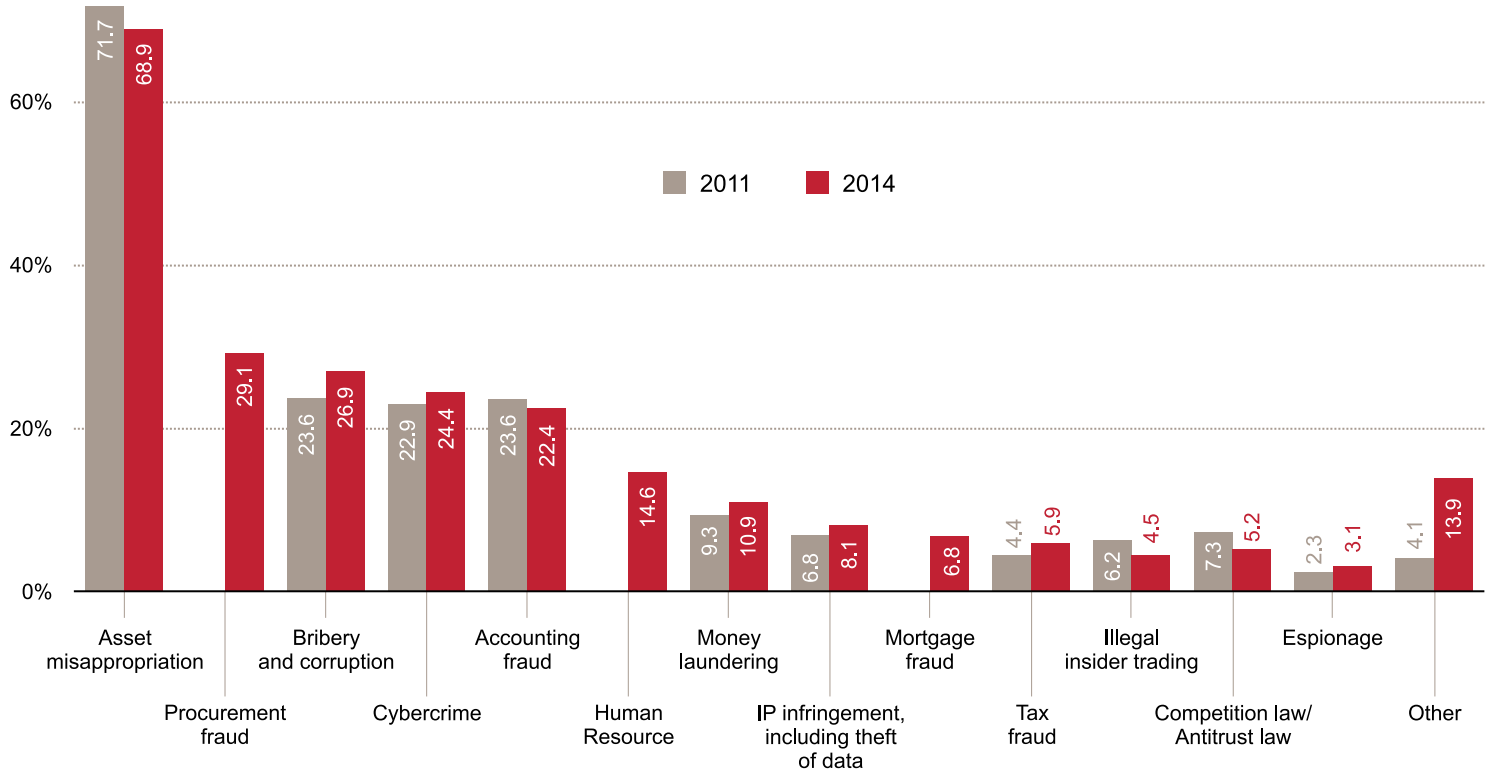
**1.** Firstly, three new categories were added this year – procurement fraud, mortgage fraud and human resources fraud. Potentially driven by the on-going megatrend of outsourcing and organisational interconnectivity, procurement fraud received a significant response (18%), becoming the third-most reported type of fraud. Similarly, a rather high percentage of respondents ticked the 'mortgage fraud' category (9%), which came in sixth place. Consequently, respondents' selection of these two new categories may have contributed to the slight decline in almost all other categories, since these incidents were likely incorporated into these broader categories in the past. In contrast with the two new categories, zero percent of the responding companies reported having faced human resources fraud, which is the third newly added category.

**2.** Secondly, the 'other' category received a significant response of 32% in 2014, whereas zero percent of Belgian respondents selected this category in 2011. Therefore, the increase in this category is another potential cause of the decline in the more specific categories. The fact that such a high number of respondents chose this category might also indicate that they do not know how to classify the fraud that has occurred.

Despite these small declines, the top five types of most common fraud in Belgium have not considerably changed compared to 2011. Asset misappropriation and cybercrime are still placed respectively first and second, followed by one of the new categories, namely procurement fraud. Next to these categories, money laundering and competition /antitrust law fraud continue to occupy respectively the fourth and fifth places.

Although these five most commonly reported types of economic crime were the same for Belgium and globally in the 2011 survey, some differences have occurred between the two in the 2014 survey. Globally, the new category of procurement fraud is ranked even higher than in Belgium, in second place, thereby pushing cybercrime to fourth place. The third and fifth places in the global survey of 2014 are occupied respectively by bribery and corruption and by accounting fraud, which score respectively only seventh and eighth place in Belgium due to the newly-added categories. As mentioned above, both worldwide and in Belgium, asset misappropriation is the number one most commonly reported type of fraud in companies.

**Figure 3** – Types of fraud reported globally (in %)



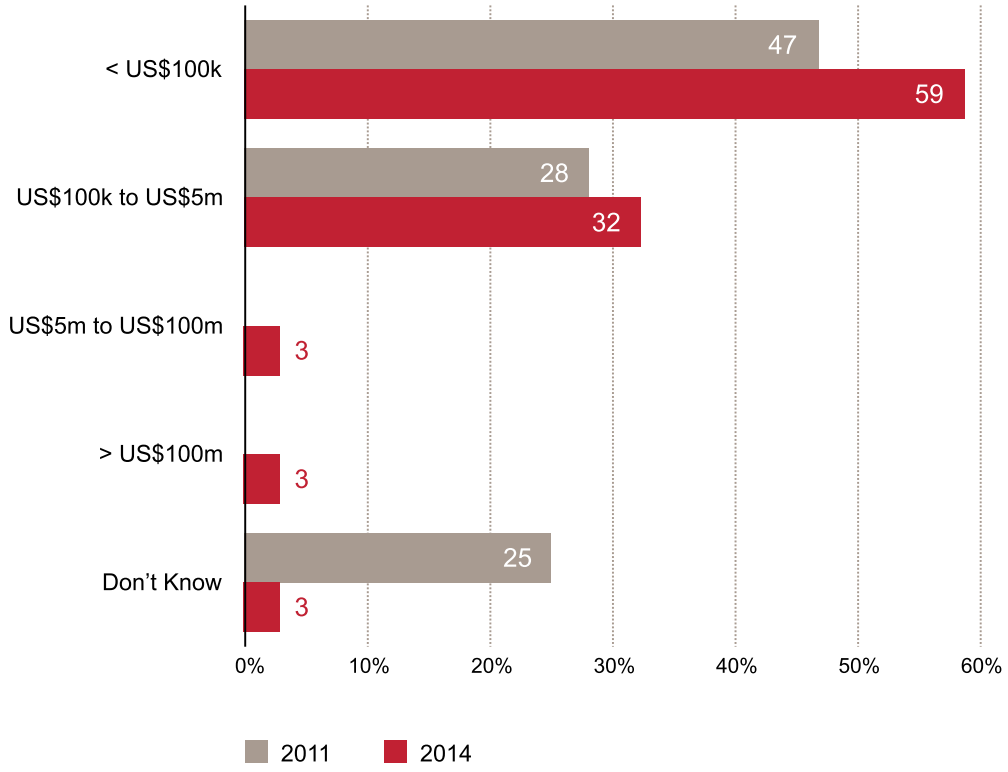
## The damage

Usually, organisations do not grasp the true financial impact of an economic crime until after it has happened – sometimes long after. As in previous years, our survey underlines that the cost of fraud for organisations is significant.

As illustrated, 38% of Belgian organisations that suffered fraud experienced a financial impact equal to or higher than US$100k. This is a lower percentage compared to the global 2014 survey which amounts to 46%. Consequently, companies in Belgium are faced more with financial effects of less than US$100k than the average globally (Belgium 59% versus 47% globally). Note that the increase in all categories in the Belgian survey are probably partly due to the fact that the respondents were better informed and selected the 'don't know' category less (down by 22%).

In addition to economic losses, we want to stress that these are not the only concerns companies face when fighting fraud. Our Belgian respondents pointed to damage to employee morale (15%), damage to relations with regulators (6%) and damage to all business relations (6%) as other severe impacts of fraud.

**Figure 4 -** Financial impact in Belgium (in %)



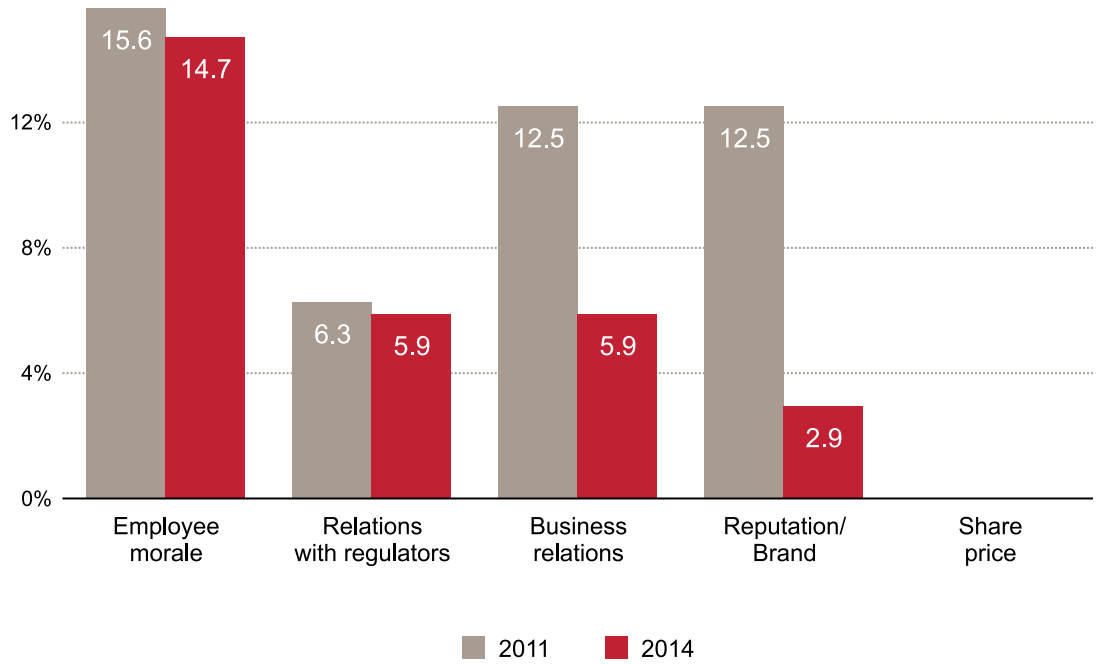
## Collateral damage: hard to quantify, hard to ignore

Economic loss is not the only concern that companies face when combating fraud. Our respondents pointed to damage to employee morale, corporate and brand reputation, and business relations as some of the most severe non-financial impacts of economic crime.

When taking into account the secondary damage, the true cost of an incidence of economic crime can be long lasting. Consider the long chain of adverse events that can follow a single, high-profile incident of economic crime: lost revenues as customers look for other business partners; delayed entry to new markets due to regulatory issues; a battered stock price; and declining productivity and morale.

Fortunately, top management appear to understand the importance of collateral impacts: our 2014 Global CEO Survey reports that half of chief executives (a sharp increase from 37% just a year ago) see a "lack of trust in business" as a key marketplace issue, with significant majorities recognising that business has a wider role to play in society than just building shareholder value.

**Figure 5 -** Collateral effects of economic crime in Belgium (in %)




### Collateral damage: a worst-case scenario

**We have witnessed cases were a single incident led to a situation where an entire business disintegrated.**

Starting with a report of a single event such as insider trading or financial statement fraud, incidents may appear compartmentalised, involving only one account, division, or customer. Still, in a competitive marketplace, there are often few reasons for customers, counterparties or partners to maintain a relationship with a tainted entity. In addition, potential government enforcement actions give rise to uncertainty concerning the company's future operational condition. Customers, capital, employees, and partners disassociate themselves from the organisation. Caught in a storm of uncertainty about its future, the organisation implodes.

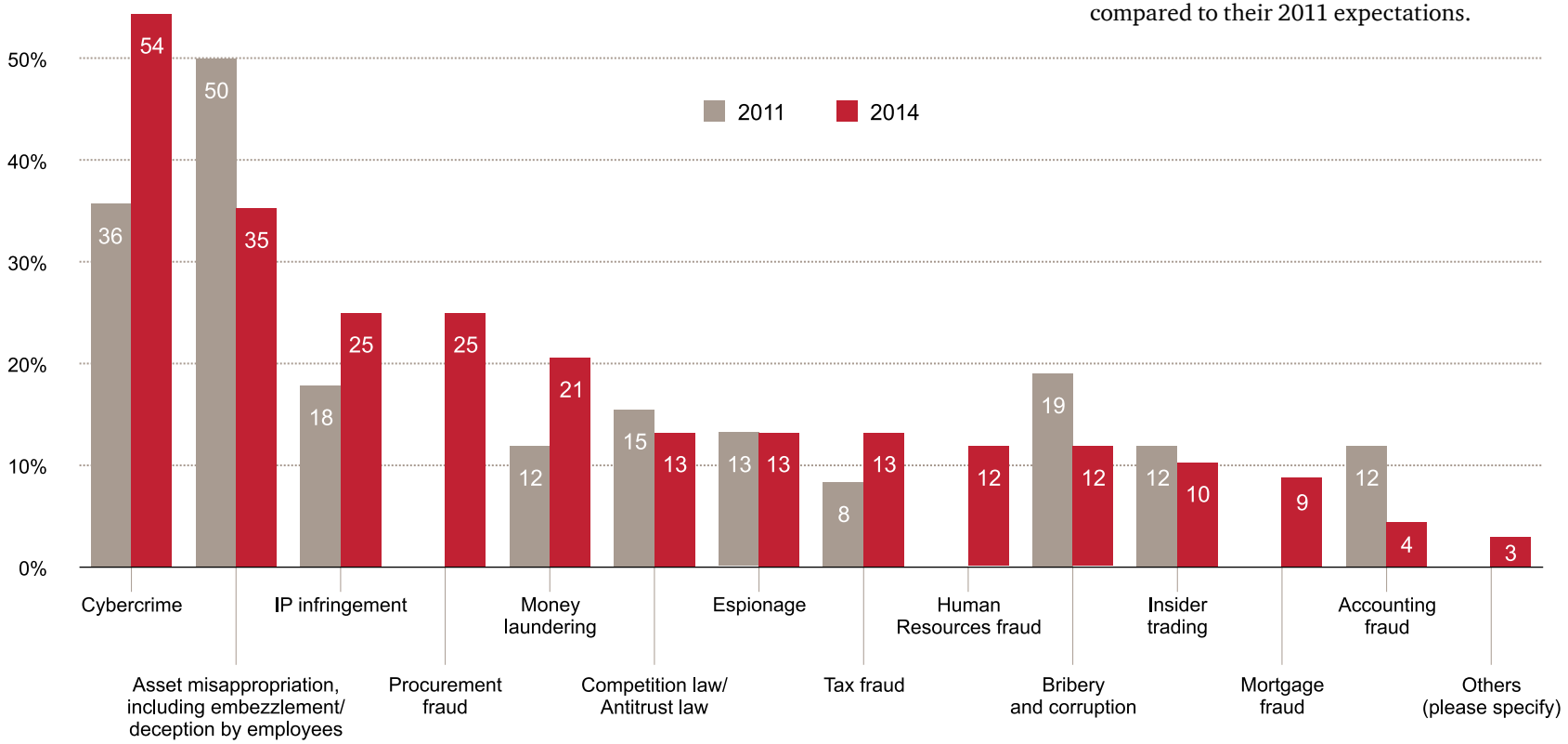
## Looking ahead

In addition to looking at economic crimes suffered in the past and their impacts, we asked respondents to look to the future and tell us which types of fraud they thought would pose the highest risks to their companies going forward.

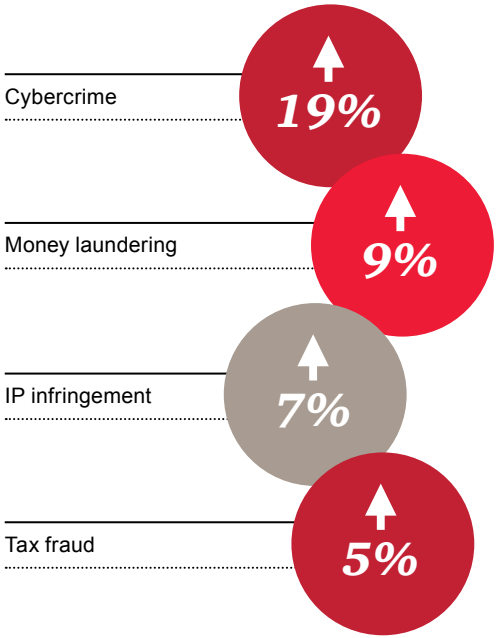
In figure 6 their predictions for key crimes in 2014 are presented, along with comparable responses from 2011.

As the chart makes clear, Belgian respondents do not anticipate experiencing greater levels of fraud equally across all categories compared to 2011. This is in contrast with the global results. In the latter, expectations for all categories have gone up for the future, except for competition and antitrust law fraud for which global respondents expect a small decrease of 5%. On the other hand, the changes in estimations for the Belgian respondents are more diverse compared to their 2011 expectations.

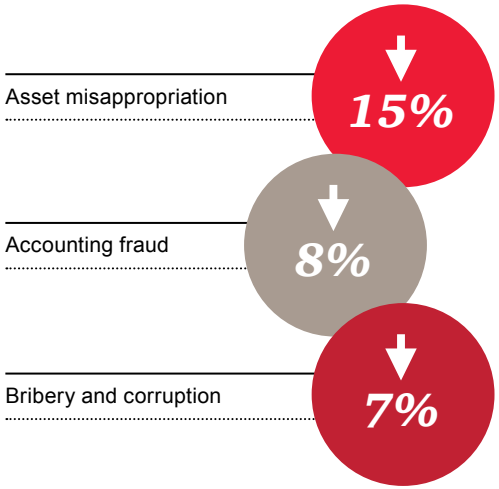
**Figure 6** - Types of fraud indicated as most likely to be experienced in the future in Belgium (in %)



## *Rising expectations:*

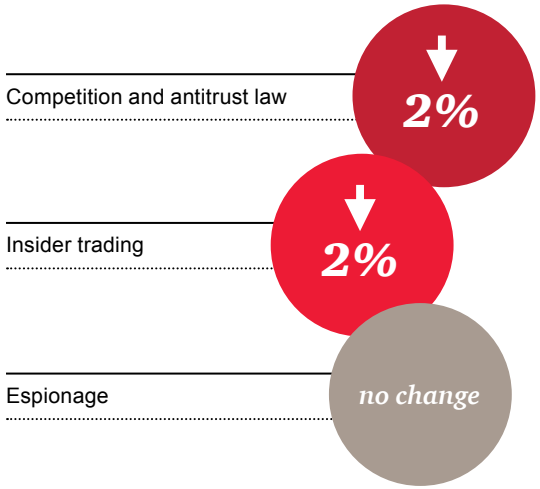



## *Declining expectations:*




Together with the newly added categories (procurement fraud, mortgage fraud and human resources fraud) these fluctuations have resulted in a slightly different top five of main types of economic crimes that respondents believe their organisation is most likely to experience in the near term.

## *More or less stable expectations:*



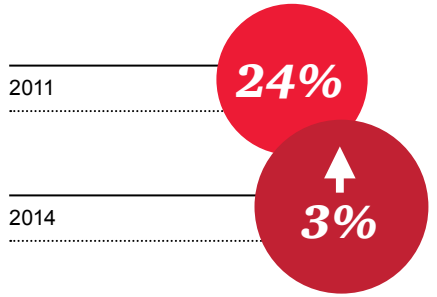

With inter alia the drop in bribery and corruption, the top five for 2014 in Belgium consists of the following types of economic fraud: cybercrime, asset misappropriation, IP infringement, procurement fraud and money laundering.

# *Under the eye of enforcement*

*Some types of economic crime attract significantly more attention from government enforcement agencies than others. For this reason we have decided to dedicate a section of our analysis to an important subset of economic crime – bribery and corruption, money laundering, and anticompetitive behaviour.*

All three of these crimes arise from the failure of businesses to adhere to the expected code of business conduct established by countries around the world. And several countries, among them the US and the UK, are committed to enforcement programmes with increasingly stringent standards and stiff penalties.

In an interconnected world, these categories of economic crime pose unique threats to global organisations. In addition to triggering fines and even criminal indictments, such violations can be seen as part of a larger organisational problem (be it a failure of internal controls, processes, or lack of appropriate culture or tone at the top). They can also create a great deal of damaging fallout – from reputational harm (including viral negative attention in social media, unwanted publicity in traditional media, litigation or adverse stock market reactions) to financial losses, costly disruptions to business plans, and loss of critical talent.




## Bribery and corruption

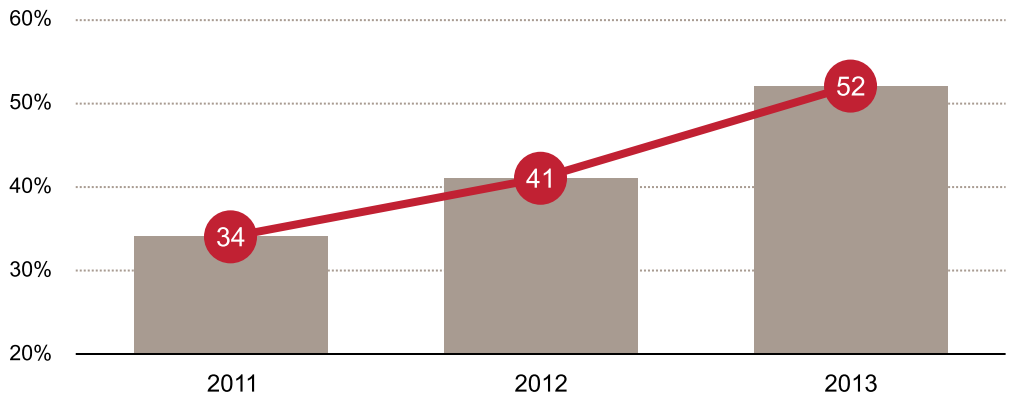
### *The C-Suite gets the message*

While it is not the most common form of crime reported, of all the types of fraud covered in our survey, bribery and corruption may pose the greatest threat to global businesses because of the number of business processes it threatens. Sales, marketing, distribution, payments, international expansion, expense reimbursement, tax compliance, facilities operations are all vulnerable processes.

Every region reported a significant number of incidences of bribery and corruption. Twenty-seven per cent of all respondents who reported economic crime experienced corruption during the survey period, making it the third-highest crime specified – a 3% increase overall from the 24% reported in 2011.

When an economic crime threatens a company in so many ways, it deserves CEO attention – which could explain the sharp increase in CEO focus on the risks of corruption and bribery in this year's CEO Survey.

**Figure 7** – Rising CEO concern about bribery and corruption in Belgium (in %)

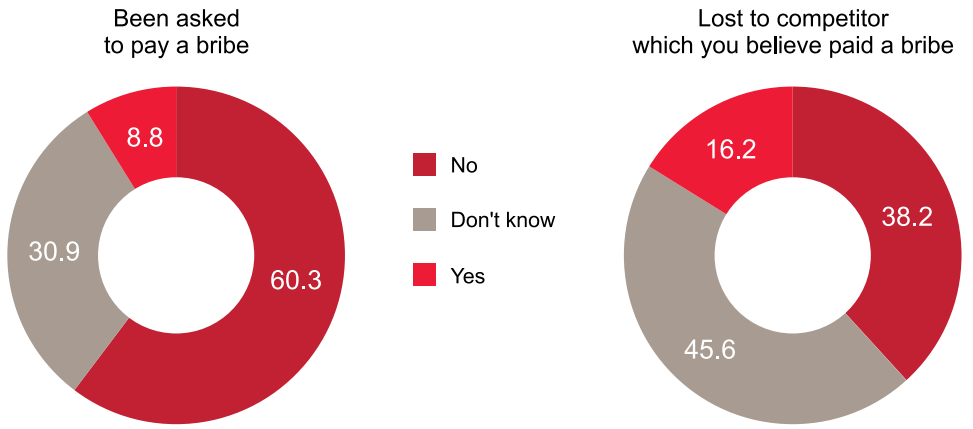


## *From the developed to the developing*

The global economy is generally on the rebound, potentially reinvigorating organisations' appetite for expansion, and risk. Our survey results confirm that a large number of organisations operate in territories identified as posing a high corruption risk (50%) and/or plan to pursue opportunities in such areas in the next two years (8%). The data underscores that countries within these regions are experiencing a relatively higher share of incidences of bribery and corruption (36%) vs. the global average (27%).

We believe that one driver of the high reported figures of bribery and corruption may be the mega-trend of the shift in wealth from the developed economies of the West to the emerging high-growth economies of the South and East – many of which may have different cultural attitudes toward fraud and corruption, fewer regulations, and less-consistent enforcement of those regulations. These conditions naturally create a higher risk profile for this type of economic crime.

**Figure 8** – Bribery request and lost opportunities in Belgium (in %)




Africa and Eastern Europe reported the highest overall percentage of bribery and corruption (39%), with the Middle East (35%) also registering above the global average. Notably, the Middle East and Africa have significant resource extraction and infrastructure/ construction-based economies, which are traditionally industries with significant fraud and corruption risks.

Since bribery and corruption is often prosecuted by regulators across borders, organisations should be mindful of the significant risks involved with operating in these high-growth areas, even if local practices and customs are less rigorous.

So while North America and Western Europe are actually low on the scale of regions reporting bribery and corruption, their government enforcement practices have a deep influence in this area.

Of the Belgian respondents, only 8.8% confirm having been asked to pay a bribe, this figure is likely to be underestimated as 60.3% don't know if someone in their organisation has or hasn't been asked to pay a bribe. More Belgian respondents (16.2%) indicate that they believe they may have lost out to a competitor which paid a bribe.

## Money laundering

In this Global Economic Crime Survey, money laundering is defined as "actions intended to legitimise the proceeds of crime by disguising their true origin". Based on this definition, 18% of the Belgian respondents who reported some kind of economic crime identified money laundering as an issue, ranking it in fourth place. As can be expected, financial services companies in particular report significant risk from this type of fraud.

Globally, the financial services industry respondents report that their number-one economic crime concern is entirely different compared to that of most other industry sectors and is money laundering.

Money laundering represents a risk if a financial institution fails to report it. If the organisation is diligent in its compliance efforts to review customer transactions in accordance with the law, they are not likely to be punished by regulators, even if some incidents do occur.

Over one quarter (27%) of global respondents in the financial sector reported experiencing money laundering during the survey period, a response rate more than double that of the next closest industry sector, insurance (11%). In addition, financial services respondents perceive far more risk from money laundering than either corruption and bribery or competition law, with 58% reporting this as their biggest concern among the three.

While money laundering schemes vary in their sophistication and complexity, in every scheme they require access to the facilities and services of a financial institution. In this, the threats they pose share a common, very real aspect: money laundering is facilitated by human weakness – whether benignly by inattention or incompetence, or maliciously by corruption and intent. The challenge of such systemic threats is they can't be completed avoided – at least not without irrational steps like withdrawing from the market in question  meaning business processes must operate even in face of such threats.

The crime of money laundering threatens the business processes of financial institutions in several ways:

- **Know your customer (KYC)**. The process of marketing to potential customers, as well as integrating new customers, is directly affected by the threat of money laundering.
- **Compliance**. Equally significant, money laundering threatens the institution's processes for maintaining compliant operations – at the teller's window, in the money transfer room, and in its check processing and settlement process.
- **Risk management**. Money laundering also threatens an institution's due diligence, suspicious transaction reporting and risk management – especially when risk is concentrated in a commonly controlled group of accounts or loans used by money launderers, or when systems monitoring capabilities fall behind the service platforms in use.

Money laundering presents collateral threats as well. In addition to enforcement settlements, this crime can bring reputational damage, negative publicity and adverse relationships with regulators. Additional burdens include the cost of compliance, surveillance, and other business process upgrades.

Recently, a new form of money laundering threat has developed: alternative payment networks using "virtual" currencies. While the transactions on these sites may be "virtual," they are backed by actual deposits in financial institutions around the world. Identifying such tainted funds is yet another challenge for bank compliance and operating systems.

So operating in environments that pose a systemic threat of money laundering to the business processes of financial institutions is a unique challenge. Not only are money laundering schemes numerous and sophisticated, but they create a potentially significant tension between the equally laudable goals of acquiring and serving profitable customer and operating a wholly compliant institution across multiple jurisdictions.

## Competition law/antitrust

Lastly, the third government enforcement-related fraud – anticompetitive behaviour – scores highly in the ranking of reported types of fraud in our 2014 survey. For Belgium, it can be found at fifth place, with 12% of the responding Belgian companies claiming to have had experience with it.

Globally, Western (25.3%) and Eastern European (24.5%) respondents especially cited competition law as a higher risk– with Asia Pacific, Africa, and both American continents lagging behind. The reason for this can be found in the fact that the EU Commission has been increasingly aggressive in pursuing high-profile actions against cartels, price-fixing and other forms of market abuse – including in the recent, highly publicised Libor affair.

Because of its significance, PwC Germany also launched a study on the subject of economic crime. Among other things, their study focused on the weaknesses of antitrust compliance programmes. Among the most important issues detected were the lack of employee training, absence of a systematic risk analysis of business partners, weak internal audits and the need for improvement of whistle-blower systems. We believe that paying more attention to these aspects will allow companies to facilitate the detection of antitrust violations more easily. And while this risk resonated primarily with European respondents, the actions of the EU Commission affect entities on a *global* scale.

### LIBOR scandal

Competition law violations reached the headlines during our 2014 survey in the form of widespread allegations of collusion among banks in reporting LIBOR, the benchmark London Interbank Offered Rate. European Commission officials became the latest global regulators to take action against multiple global financial institutions after the discovery of widespread rigging of LIBOR.

A 2012 international investigation revealed that employees of multiple banks had participated in a scheme to manipulate LIBOR by submitting false rates in an effort to influence the publicly reported rate.

As of January 2014, regulators in the US, UK and EU had fined a group of banks more than US$8 billion for rate-rigging, and regulators in Switzerland, Canada, and Japan were continuing their investigations. Interestingly, unlike the national regulators, the European Commission's investigation was centred not on fraud but on the antitrust violation of illegal cartels.

Many observers see the LIBOR case as pointing to a more aggressive future stance by European antitrust authorities in investigating alleged anticompetitive behaviours in any industry.

# Cybercrime

*The advancement of technology in business services, combined with the explosive growth in social media and data connectivity, has permanently altered – and in many ways, brought together – the business and consumer landscapes.*

Unfortunately, connectivity and access also have a dark side – one which empowers motivated, sophisticated criminals who are able to operate below the radar. And because cybercrime operates largely unseen, organisations may never even realise they are being targeted until long after the damage is done.

This fact alone makes the many varieties of electronic fraud one of the most threatening types of economic crime.

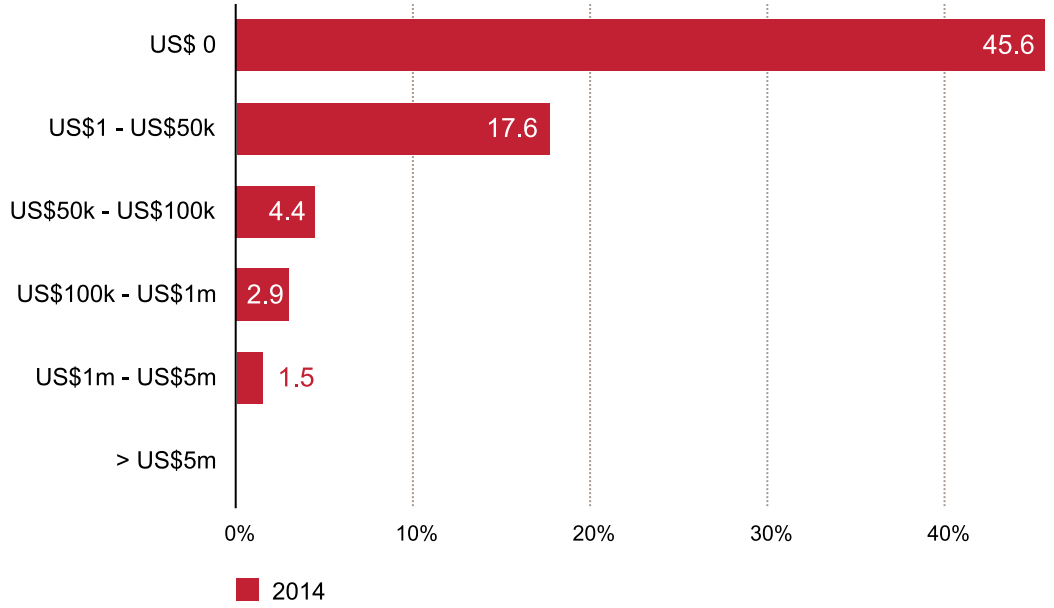
## The cost you can count

Our 2011 report was the first in our series that highlighted cybercrime as a high-level threat to organisations. This year's survey confirms the significant, continued impact of this crime on business, with now almost four out of ten Belgian respondents reporting having experienced cybercrime (refer to figure 2) and 1.5% of these suffering financial losses of more than US$1 million (refer to figure 9). Note that this last figure is considerably less than the 11% of global respondents who suffered financial losses of more than US$1 million. The financial services industry is the clear leader in reported cybercrimes.

As is the case for the previously described economic crimes, the corresponding fallout is not limited to financial losses. Other severe concerns of Belgian companies emerging in our 2014 survey include service disruption (85%), reputational damage (84%), theft or loss of personally identifiable information (81%) and IP theft including theft of data (79%).

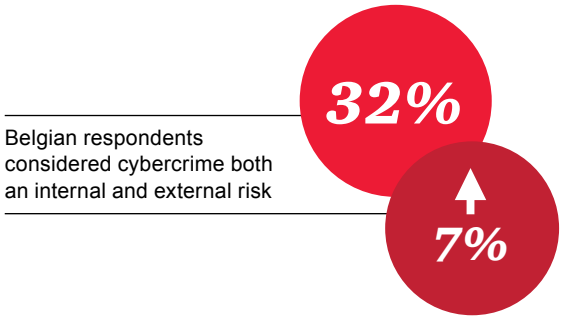
As a sign that organisations are taking this threat more seriously, our survey indicates that the perception of cybercrime is increasing at a faster pace than that of reported actual occurrences. This year, 71% of our respondents stated the perception of cybercrime risk had increased in their organisation in the survey period, up from 45% in 2011 (refer to figure 10). Globally the same trend can be seen, albeit less pronounced than in Belgium.

**Figure 9** – Estimated financial losses due to cybercrime in Belgium (in %)



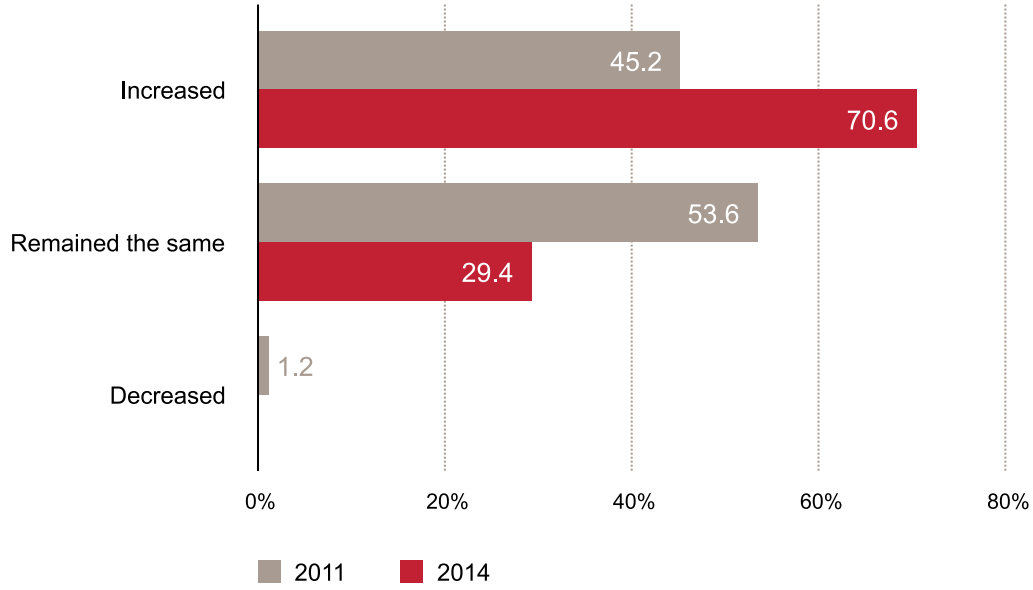
In addition, the 2014 survey reconfirms the findings of 2011 that the perception of cybercrime is changing from being exclusively an external threat to being both an internal and external threat. More precisely, 32% of Belgian respondents considered cybercrime both an internal and external risk, accounting for an increase of 7% compared to the previous survey. It is thus clear that organisations do recognise the internal risk of cybercrime.

Note that while a figure of 40% reporting cybercrime is concerning enough, we must also consider that a significant percentage did not report cybercrime, either because it was not known, difficult to quantify, or because it was not shared due to competitive reasons.




Belgian respondents considered cybercrime both an internal and external risk

**Figure 10** – Perception of the risks of cybercrime (in %)



## Cybercrime is a human problem, not a technology problem

Even when organisations are generally aware of the types of cyber threats they face, many do not truly understand the capabilities of cybercriminals, what cybercriminals might target, and what the value of those targets might be. While our 2014 Global CEO Survey reports that nearly half of CEOs (47%) are concerned about cyber security threats (including lack of data security), cyber security is now trending lower on the scale of CEO concerns than in previous years.

Organisations continue to make their critical data available to management, employees, vendors and clients on a multitude of platforms – including high-risk ones such as mobile and cloud – and this because the economic and competitive benefits appear so compelling.

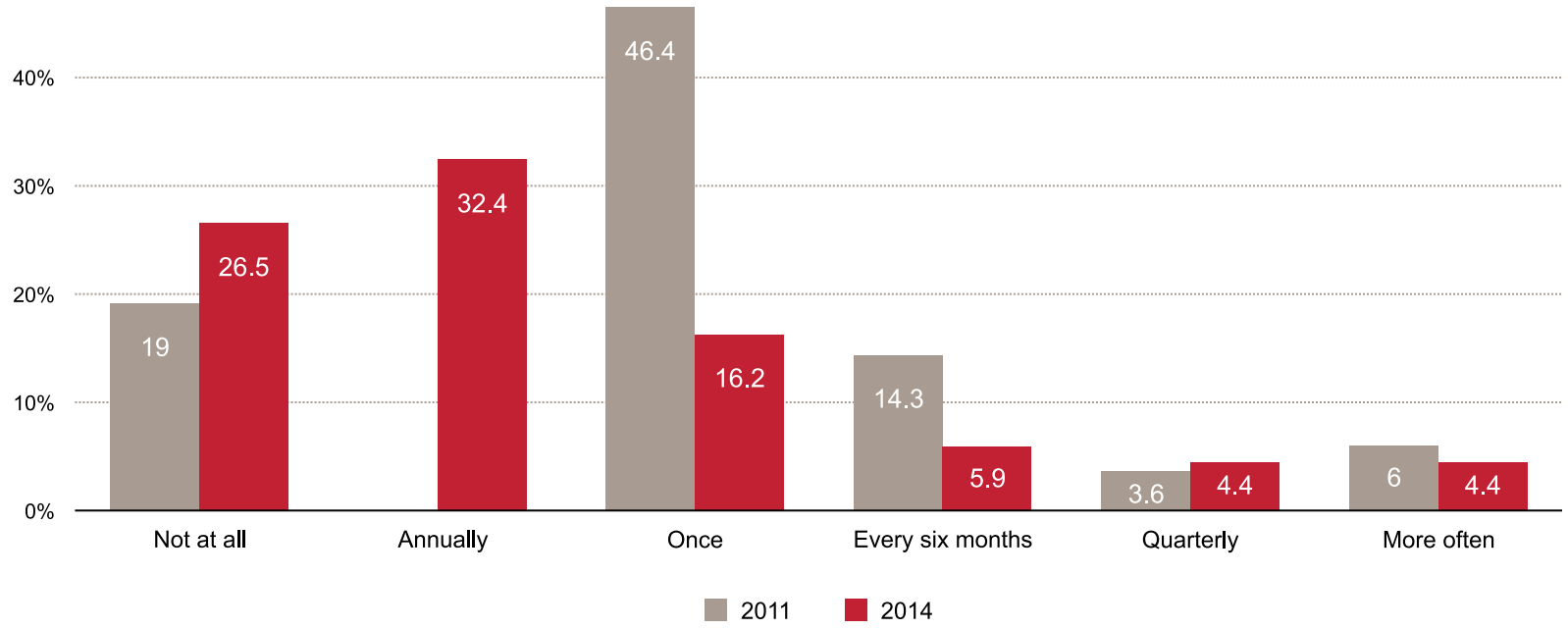
The truth is, in today's nerve-net global ecosystem, the landscape is constantly changing, and the sophisticated adversary takes advantage by attacking new weaknesses. This is why it is essential for organisations to at least try to keep pace with the actors who threaten them. Ultimately cybercrime is not purely a technology problem. It is a human problem – a strategy and process problem.

# Fraud risk assessment

*In order to prevent fraud, it is important for organisations to assess the risks and identify the gaps. Regular fraud risk assessments help organisations analyse their exposure to fraud. Globally, 24% of all respondents do not perform fraud risk assessments. In Belgium more than one in four respondents stated that they do not perform fraud risk assessments, and an additional 10.3% said they do not know if they perform a fraud risk assessment.*

38% of those companies not performing a fraud risk assessment indicated that they are not sure what a fraud risk assessment involves which is almost the same percentage as in our 2011 survey. Knowledge about fraud risk assessment has thus not increased at all since our last survey.

**Figure 11** – Frequency of fraud risk assessment (in %)



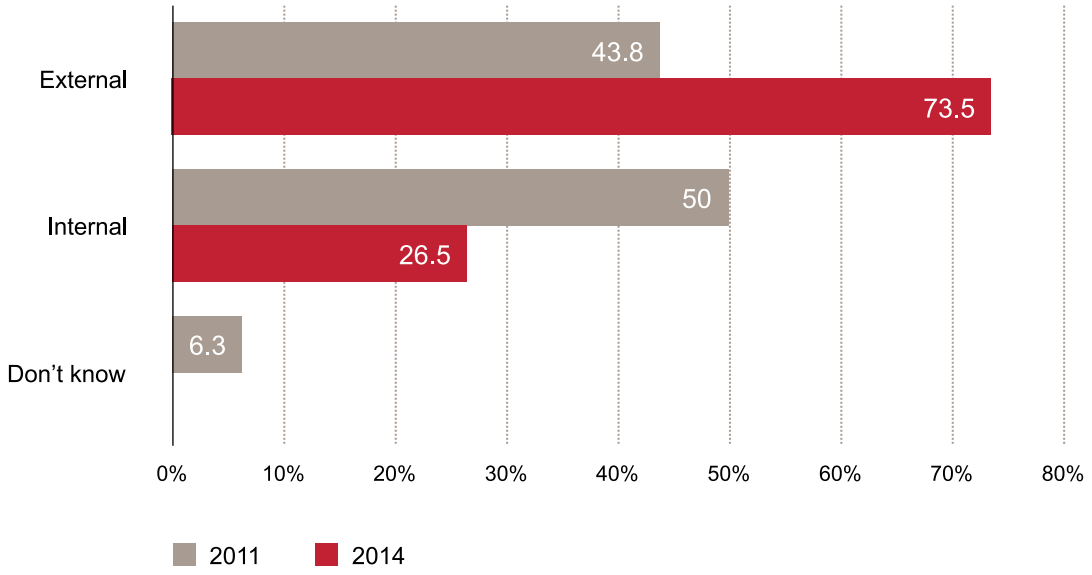
# The fraudster

*Now that you have a better understanding of the types of economic crime that could occur in your organisation, it is time to have a look at the typical profile of a fraudster. After all, the rule of thumb in fighting economic crime is the same as in any battle: Know your enemy.*

## The internal v. external fraudster

We asked respondents whose organisation had experienced economic crime to profile the main perpetrator of the most serious fraud they had faced. The ensuing Belgian picture is rather different compared to the 2011 survey, with now only 27% reporting that the main perpetrator was internal and 74% reporting the main perpetrator was external, which resemble the results from the 2009 survey.

**Figure 12** – Main perpetrator of fraud in Belgium (in %)



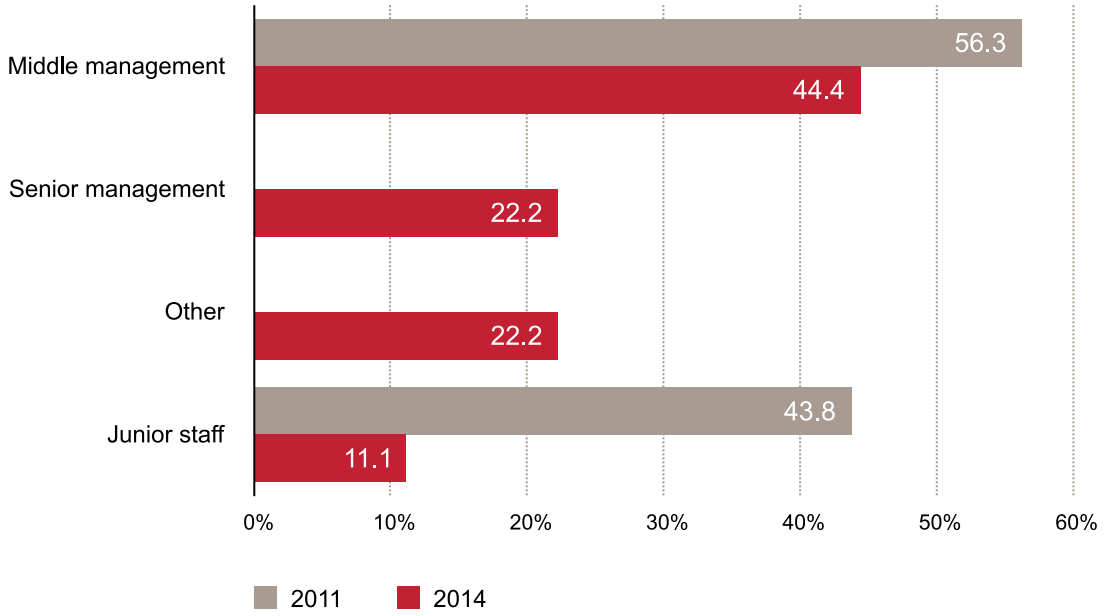
## *Profile of the internal fraudster*

Practitioners commonly refer to a 'Fraud Triangle' – the three elements that are often present when a perpetrator commits fraud: pressure, opportunity and rationalisation. Three quarters (78%) of our respondents indicated that the opportunity or ability to commit the crime was the factor that most contributed to economic crime by an internal actor. While this news may at first seem anticlimactic, it is important to keep in mind that, of the three factors, opportunity is the one most in an organisation's control. The implication is that while life's pressures and the ability to rationalise may swirl around employees, if an organisation can limit the opportunity, they may be able to stop the fraud before it starts.

While we cannot plot the specific pressure or rationalisation behind each internal act of fraud, we can at least profile the actor. We asked respondents who had pointed to an internal player as the main perpetrator of economic crime to profile the age, gender, length of service, and education level of that perpetrator.

Our results indicate that the average profile of the internal fraudster generally remained the same as in 2011 – middle-aged males (89% males and 44% between 41 and 50 years old) who have been with the organisation for more than ten years (44%) and reached a middle management level (44%).

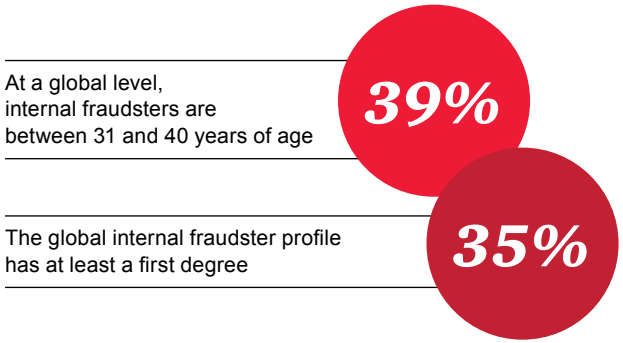
**Figure 13** – The seniority level of the internal fraudster in Belgium (in %)




Note that this year the resulting perpetrator's education level seemed to be equally divided between postgraduate, first degree graduate and high school or less levels of education, while in the 2011 survey the main Belgian perpetrator had a high school level of education or less.

In addition, it is noteworthy that while in the 2011 survey there were no reports of Belgian internal fraudsters at a senior management level, this percentage now accounts for 22%, thereby lowering the percentage of internal fraudsters among junior staff (from 44% in 2011 to 11% in 2014).

Globally, we noted that the typical internal fraudster does not have exactly the same profile as in Belgium. At a global level, internal fraudsters are younger given the majority are between 31 and 40 years of age (39%). In addition, the global internal fraudster profile has at least a first degree (35%) and is thus more highly qualified than in Belgium. Furthermore, at the global level, the typical internal fraudster has been with the organisation three to five years (29%) which also differs from the Belgian results. Gender and organisational level are the only categories for which Belgian results are in line with global results (77% male and 42% middle management globally).




## Senior management and the impact of fraud

In our experience, the greater the age and seniority of the perpetrator of an internal act of fraud the greater its proportional impact. That's because executives of greater seniority are likely to get a greater degree of deference in navigating exceptions to internal control policies.

Consider the senior private banker who assures the wire transfer operators that he'll handle the client call-back procedure to confirm instructions for payments. Or the boss who says she'll take care of getting the documentation needed to support the payment. Or even the division manager who budgets for the amount he intends to "withdraw" from the corporate coffers based on bogus invoices for services.

These real-life examples from North America, Asia and Europe illustrate the unique position of senior people. Not only are they authority figures with respect to internal control policies – and thus have access not enjoyed by employees of a lesser rank – they can also be custodians of the corporate culture. As such, the financial damage of the fraud can be compounded by its corrosive effect on that same culture.

## *Profile of the external fraudster*

As with the profile of the internal fraudster, there has been little change in the overall profile of the external fraudster since our previous survey.

Of the external fraudsters, 44% were customers and 8% vendors. These figures were in line with global results. However, almost 20% of external fraudsters at a global level were agents or intermediaries. In Belgium, no reports were received of economic crime committed by this type of external fraudster.

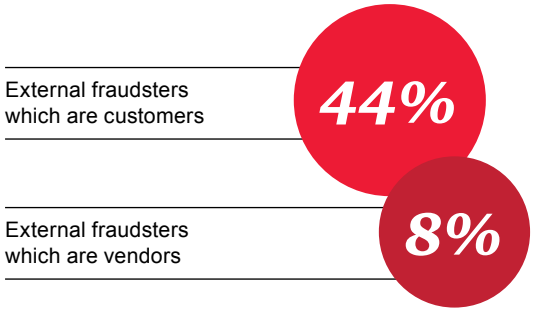
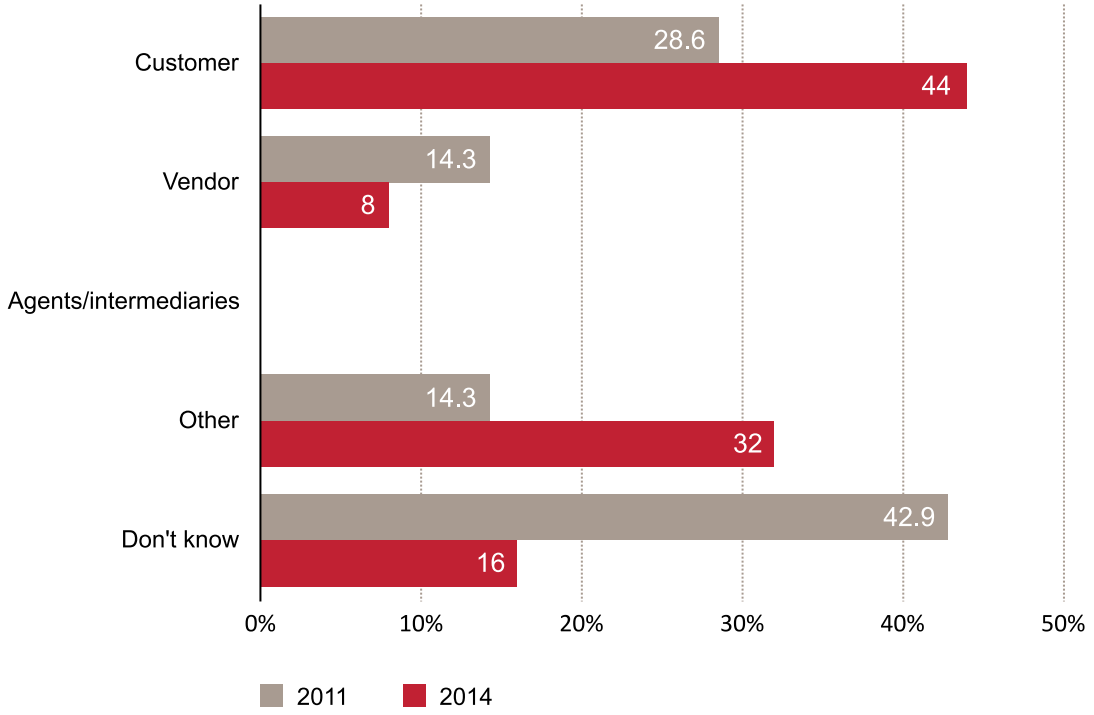



**Figure 14** – The profile of the external fraudster in Belgium (in %)



## The detection of fraud

So how do you stop an economic crime before it happens – or at least, while it is happening?

Fraud detection methods usually fall into one of three categories:

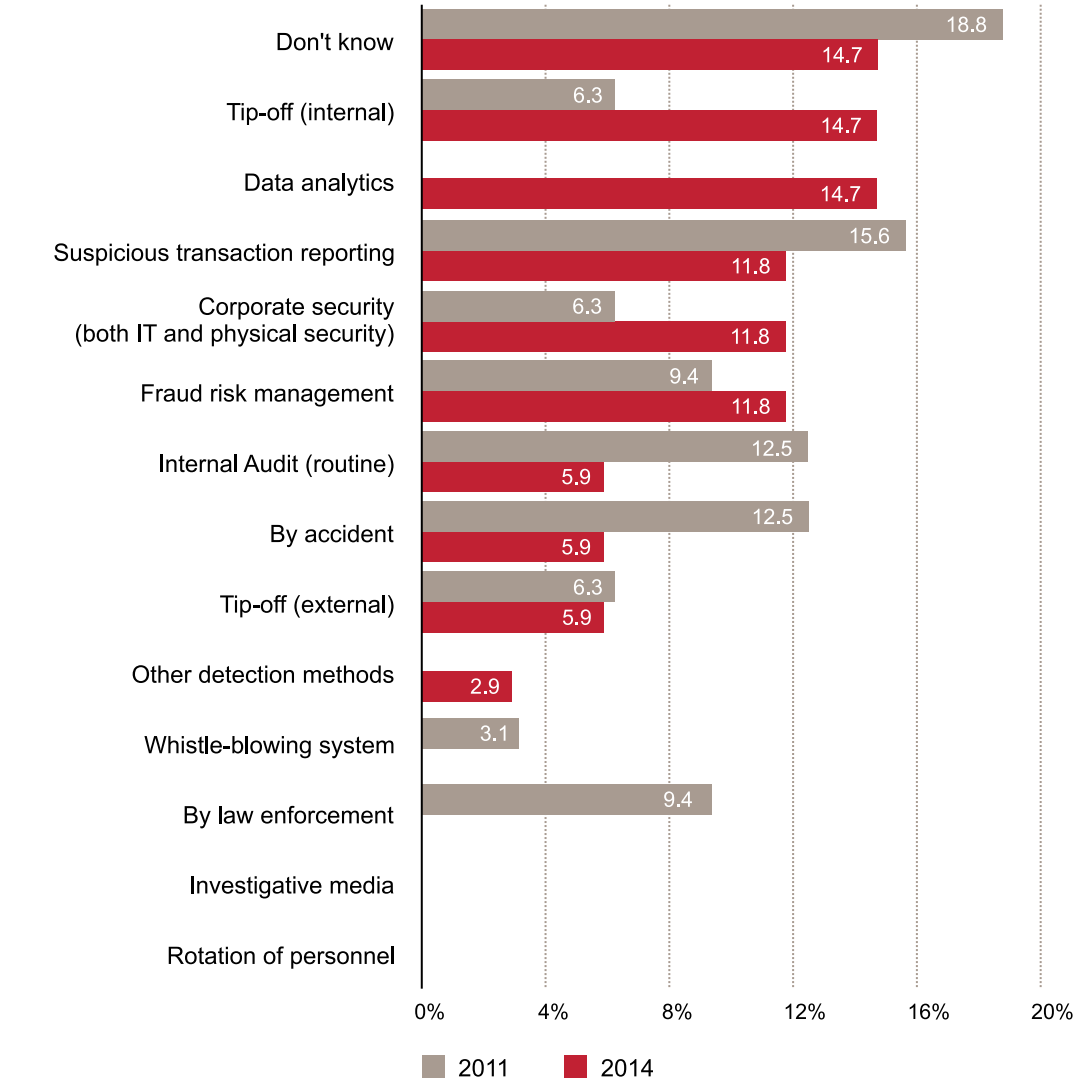
**1. Corporate controls** such as internal audit, fraud risk management, electronic and automated suspicious transaction reporting, corporate security or change of personnel/ duties;

**2. Corporate culture** aspects such as internal tip-offs, external tip-offs or whistleblowing systems;

**3. Detection beyond the control of management** such as by accident, law enforcement, investigative media or others.

Figure 15 displays the distribution of methods by which the major fraudster at Belgian organisations was detected.

**Figure 15** – Fraud discovery methods in Belgium (in %)



When comparing the results for Belgium with the global ones, it is noteworthy that Belgian companies generally discovered fraud more through corporate controls, and less via manners that are outside of management's control. This is true for every corporate control listed above, except for the investigations made by the internal audit department of an organisation. Here, the global results have shown them to be more effective (10% globally versus 6% in Belgium). In addition, if we take a look at the corporate culture controls, we can see that in Belgium, less use is made of whistleblowing systems, but this is compensated by a higher deployment of the internal tip-off mechanism.

Lastly, an encouraging sign can be noticed in the number of respondents who indicated that they 'don't know' how fraud was detected, decreasing from 19% to 15% in the 2014 survey. While this is still a rather large percentage, this greater awareness of how fraud is detected can help organisations tailor their procedures to increase effectiveness.

## Rise of data analysis

Over the past several years, we have seen a marked rise in the number of major frauds discovered through data analytics and suspicious transaction reporting. What does this process entail?

Data analytics begins with a systematic approach to data gathering, cleansing and standardisation. Current technology enables analytics to leverage a growing abundance of available and disparate information, allowing for better comprehension of an organisation's data – and therefore a better understanding of potential risks. A well-designed programme will efficiently risk-rank transactions and entities for investigation, and may use an approach which facilitates the detection of hidden relationships and connections with known high-risk entities. It identifies atypical transactional patterns through statistical, keyword, and exception-based data mining.

Through continuous feedback, anti-corruption and anti-fraud analytics continue to evolve and improve. Companies are implementing frameworks which are designed to optimise findings by leveraging their collective knowledge and experiences from past reviews and investigations.

Moving forward, we expect more organisations to build on this success story, and use these leading data analysis tools to help detect and mitigate fraud.

## Confronting perpetrators

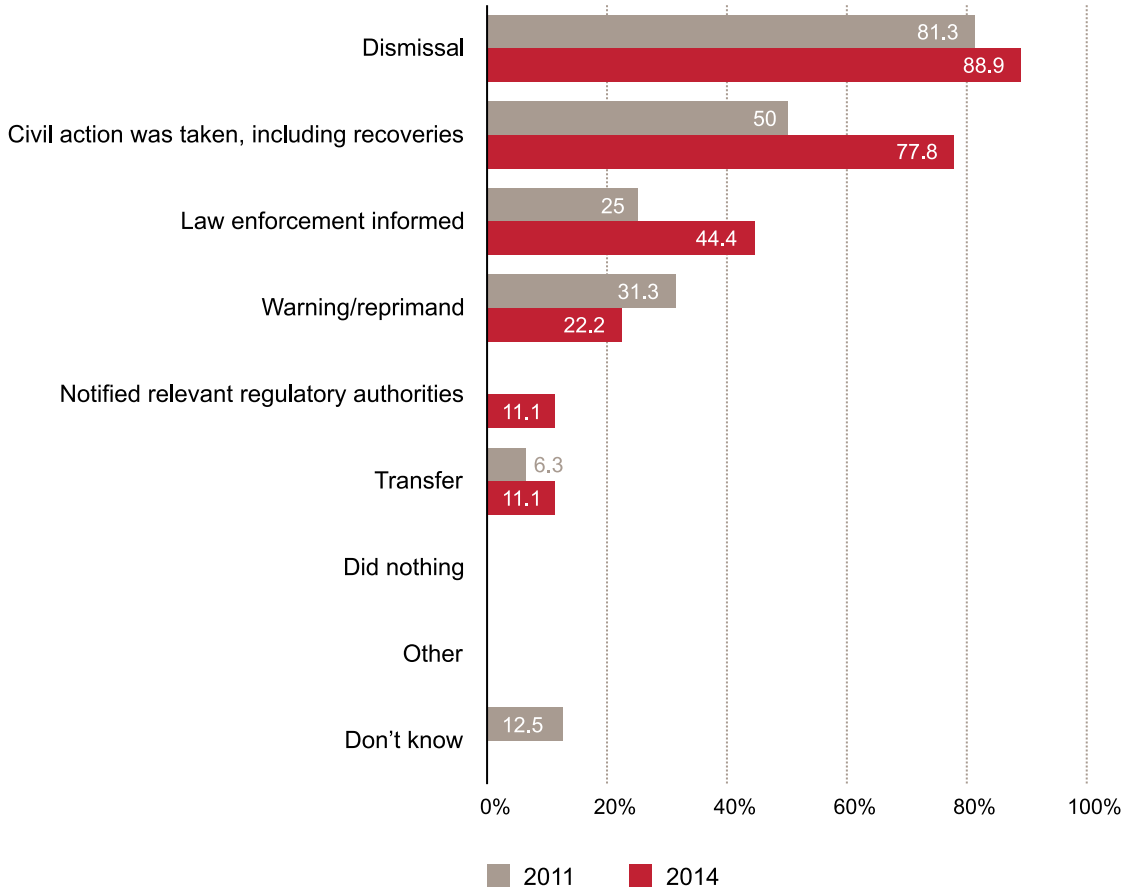
Once fraud has been detected, the question that still remains is how to confront the perpetrators. What are the most common sanctions organisations impose?

### *Confronting the internal perpetrator*

This year's survey confirms that organisations continue to respond to internal fraud aggressively, with nearly 89% saying they dismiss perpetrators once detected. Overall, the chart documents the uptick in the use of firm actions – including dismissal, civil action, informing law enforcement and notifying regulatory authorities – against internal perpetrators. This is consistent with the global trend.

Dismiss perpetrators once detected **89%**

**Figure 16** – Actions taken against internal fraudsters in Belgium



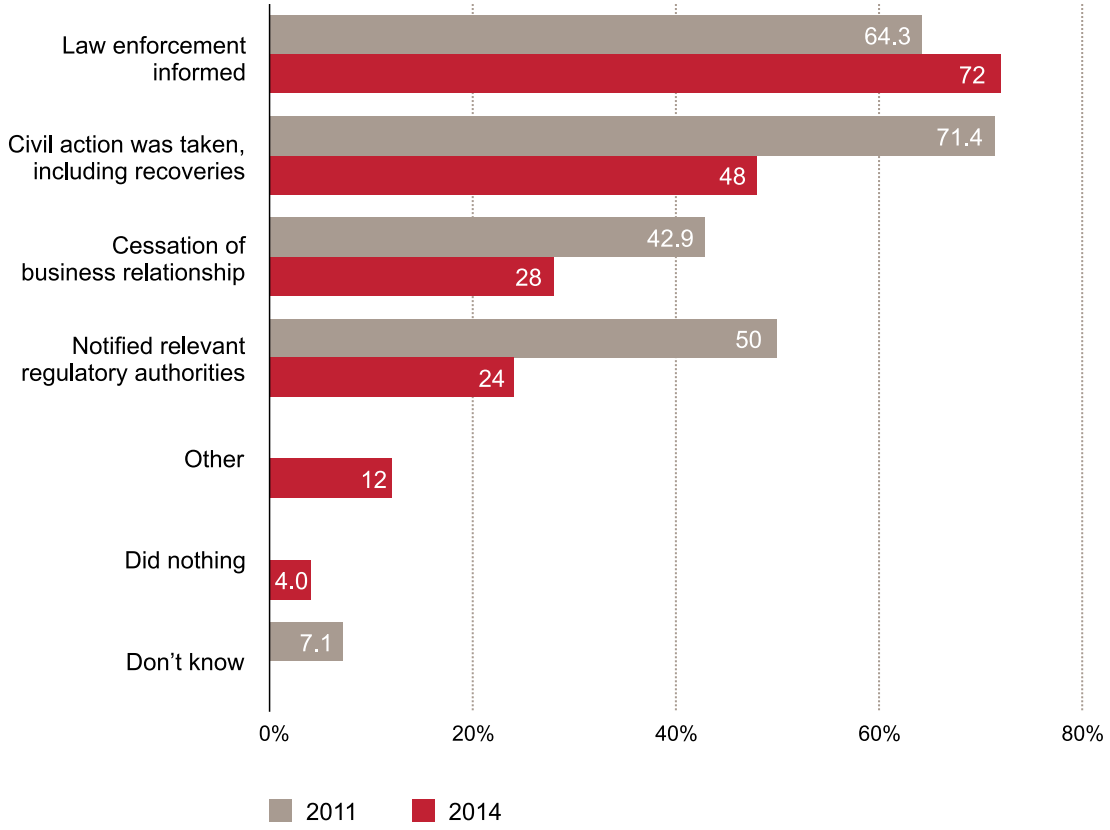
## *Confronting the external perpetrator*

The most common course of action taken against external perpetrators was informing law enforcement (72%). Previous survey results have indicated that organisations take different levels of action against external crime perpetrators than internal, and our most recent survey findings are consistent with this. There are numerous reasons for this. First, dismissal is not a ready option. In its place, it appears organisations contact law enforcement and notify regulatory authorities more frequently. Civil action on the other hand turns out to be applied less often compared to cases in which the fraudster turns out to be internal, which is in contrast with the 2011 survey results.

The most common course of action taken against external perpetrators was informing law enforcement

**72%**

**Figure 17** – Actions taken against internal fraudsters in Belgium (in %)



# Data appendix

## Detailed regional and industry data

5,128 respondents from over 95 countries completed the 2014 Global Economic Crime Survey. We asked these respondents to indicate whether they had experienced economic crime in the last 24 months. Table 1 lists the top territories reporting economic crime. Belgium is, globally, with 50%, seen clearly at the high end of fraud reported in 2014.

**Table 1** – Fraud by territory, high fraud

### *Top territories reporting fraud*

| Territory | Reported fraud 2011 | Reported fraud 2014 |
|---|---|---|
| South Africa | 60% | 69% |
| Ukraine | 36% | 63% |
| Russia | 37% | 60% |
| Australia | 47% | 57% |
| Papua New Guinea | n/a | 57% |
| France | 46% | 55% |
| Kenya | 66% | 52% |
| Argentina | 45% | 51% |
| Spain | 47% | 51% |
| **Global** | **34%** | **37%** |

As indicated by the table, a number of growing economies have elevated reports of economic crime. Certain developed countries also registered high figures, potentially reflecting greater detection capabilities.

**Table 2** – Fraud by territory, low fraud

### *Territories reporting least fraud*

| Territory | Reported fraud 2011 | Reported fraud 2014 |
|---|---|---|
| Malaysia | 44% | 24% |
| Italy | 17% | 23% |
| Turkey | 20% | 21% |
| Peru | 35% | 20% |
| Hong Kong/ Macau* | n/a | 16% |
| Japan | 5% | 15% |
| Portugal | n/a | 12% |
| Denmark | 29% | 12% |
| Saudi Arabia** | n/a | 11% |
| **Global** | **34%** | **37%** |

** Part of greater China in 2011*
*** Part of greater Middle East in 2011*

Table 1 lists the territories who reported the lowest rates of economic crime.

Low reports of fraud can reflect a number of things: respondents reluctant to report fraud, low levels of asset misapropriaiton (the most common fraud) or lack of controls which can help detect fraud.

**Table 3** – Fraud by region

### *Reported frauds in regions*

| Territory | Reported fraud 2011 | Reported fraud 2014 |
|---|---|---|
| Africa | 59% | 50% |
| North America | 42% | 41% |
| Eastern Europe | 30% | 39% |
| Latin America | 37% | 35% |
| Western Europe | 30% | 35% |
| Asia Pacific | 31% | 32% |
| Middle East | 28% | 21% |
| **Global** | **34%** | **37%** |

Africa still leads in terms of reported economic crime, though the gap has narrowed since 2011. The Middle East presents a unique situation: low overall levels of economic crime reported, but those who reported fraud showed a high number of types and instances of fraud.

# Participating territory counts

| | 2011 | 2014 |
|---|---|---|
| **Asia Pacific** | **669** | **906** |
| Australia | 79 | 79 |
| China including Hong Kong[1] | 22 | n/a |
| Hong Kong / Macau | n/a | 116 |
| China (excluding Hong Kong) | n/a | 85 |
| India | 106 | 115 |
| Indonesia | 84 | 4 |
| Japan | 73 | 75 |
| Malaysia | 93 | 110 |
| New Zealand | 93 | 82 |
| Papua New Guinea | 1 | 81 |
| Singapore | 18 | 82 |
| Taiwan | 2 | 0 |
| Thailand | 79 | 76 |
| Vietnam | 19 | 1 |

| | 2011 | 2014 |
|---|---|---|
| **Middle East[2]** | **128** | **232** |
| Unspecified Middle East Countries | 127 | n/a |
| Bahrain | n/a | 2 |
| Egypt[3] | n/a | 7 |
| Jordan | n/a | 9 |
| Lebanon | n/a | 8 |
| Oman | n/a | 1 |
| Qatar | n/a | 12 |
| Saudi Arabia | n/a | 74 |
| Sudan[3] | 1 | 1 |
| Syria | n/a | 1 |
| UAE | n/a | 117 |

| | 2011 | 2014 |
|---|---|---|
| **Africa** | **259** | **604** |
| Algeria | 0 | 2 |
| Angola | 1 | 22 |
| Botswana | 1 | 5 |
| Cameroon | 0 | 6 |
| Democratic Republic of Congo | 0 | 1 |
| Ghana | 29 | 3 |
| Guinea | 0 | 2 |
| Ivory Coast | 0 | 3 |
| Kenya | 91 | 124 |
| Lesotho | 0 | 1 |
| Liberia | 5 | 0 |
| Malawi | 0 | 1 |
| Morocco | 0 | 17 |
| Mozambique | 0 | 4 |
| Namibia | 2 | 26 |
| Nigeria | 3 | 82 |
| Sierra Leone | 0 | 1 |
| South Africa | 123 | 134 |
| Swaziland | 1 | 4 |
| Tanzania | 0 | 12 |
| Tunisia | 2 | 17 |
| Uganda | 0 | 12 |
| Zambia | 1 | 83 |
| Zimbabwe | 0 | 42 |

[1] China and Hong Kong were combined from 2005-2011. They were separated in the 2014 survey.
[2] Was formerly part of Asia Pacific Region Totals.
[3] Was formerly part of the African Region.

| | 2011 | 2014 |
|---|---|---|
| **Western Europe** | **1,318** | **1,555** |
| Andorra | 1 | 0 |
| Austria | 8 | 6 |
| Belgium | 84 | 68 |
| Cyprus | 5 | 88 |
| Denmark | 116 | 118 |
| Finland | 61 | 34 |
| France | 112 | 131 |
| Germany[4] | 38 | 10 |
| Greece | 92 | 11 |
| Ireland | 80 | 78 |
| Israel | 1 | 31 |
| Italy | 127 | 101 |
| Luxembourg | 3 | 12 |
| Netherlands | 41 | 75 |
| Norway | 67 | 92 |
| Portugal | 0 | 75 |
| Spain | 85 | 79 |
| Sweden | 79 | 91 |
| Switzerland | 140 | 83 |
| UK5 | 178 | 372 |

| | 2011 | 2014 |
|---|---|---|
| **North America** | **209** | **215** |
| Canada | 53 | 100 |
| USA | 156 | 115 |
| **Central & Eastern Europe** | **804** | **877** |
| Bulgaria | 58 | 79 |
| Croatia | 1 | 0 |
| Czech Republic | 84 | 94 |
| Estonia | 1 | 0 |
| Hungary | 85 | 91 |
| Kazakhstan | 0 | 1 |
| Lithuania | 7 | 1 |
| Moldavia | 1 | 0 |
| Montenegro | 1 | 0 |
| Poland | 79 | 94 |
| Romania | 76 | 77 |
| Russia | 126 | 111 |
| Serbia | 14 | 52 |
| Slovakia | 84 | 76 |
| Slovenia | 48 | 33 |
| Turkey | 55 | 78 |
| Ukraine | 84 | 90 |

| | 2011 | 2014 |
|---|---|---|
| **South & Central America** | **483** | **711** |
| Argentina | 77 | 82 |
| Bahamas | 0 | 2 |
| Barbados | 0 | 1 |
| Bolivia | 3 | 0 |
| Brazil | 115 | 132 |
| Chile | 1 | 75 |
| Colombia | 1 | 1 |
| Cuba | 0 | 2 |
| Dominican Republic | 0 | 1 |
| Ecuador | 11 | 22 |
| Mexico | 174 | 211 |
| Peru | 17 | 82 |
| Venezuela | 84 | 100 |
| **No primary country specified** | **8** | **28** |
| **Total** | **3,878** | **5,128** |

[4] Includes the instance when the survey responder indicated Guernsey as country.

# Terminology

## *Accounting fraud*

Financial statements and/or other documents are altered or presented in such a way that they do not reflect the true value or financial activities of the organisation. This can involve accounting manipulations, fraudulent borrowings/raising of finance, fraudulent application for credit and unauthorised transactions/rogue trading.

## *Asset misappropriation*

Including embezzlement/deception by employees, the theft of assets (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit.

## *Bribery and corruption*

The unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail. It can also refer to the acceptance of such inducements. Specific examples include kickbacks, extortion, gifts (with strings attached), facilitation payments, etc.

## *Competition law/antitrust law*

Competition law promotes or maintains market competition by regulating anti-competitive and unfair business practices by organisations. Contraventions may include price fixing, excessive, predatory or discriminatory pricing, unfair trading terms, and tying (i.e., stipulating that a buyer wishing to purchase one product must also purchase all or some of his requirements for a second product).

## *Cybercrime*

Also known as computer crime is an economic offence committed using a computer and internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a secondary tool in order to create the fraud and only includes such economic crimes where a computer, internet or use of electronic media and devices is the main element and not an incidental one.

## *Economic crime*

The intentional use of deceit to deprive another of money, property or a legal right.

## *Espionage*

Espionage is the act or practice of spying or of using spies to obtain secret information.

## *Financial loss*

When estimating financial losses due to fraud, the participants should include both direct and indirect losses. The direct losses are the actual amount defrauded and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to 'loss of business opportunity'.

## *Financial terms*

When estimating financial losses due to fraud, the participants should include both direct and indirect losses. The direct losses are the actual amount defrauded and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to 'loss of business opportunity'.

### *Fraud risk assessment*

Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to specifically consider:

i. the fraud risks to which operations are exposed;
ii. an assessment of the most threatening risks (i.e. evaluation of risks based on significance and likelihood of occurrence);
iii. identification and evaluation of the controls (if any) that are in place to mitigate the key risks;
iv. assessment of the general anti-fraud programmes and controls in an organisation; and
v. actions to remedy any gaps in the controls.

### *Human Resources fraud (recruitment and/or payroll fraud)*

Fraud committed by members of the Human Resources department, including payroll fraud, ghost employees, pay-to-work, recruitment (i.e., hiring friends and/or relatives, hiring unqualified individuals, falsification of documents, etc.).

### *Incentive/pressure to perform*

The individual has a financial problem that they are unable to solve through legitimate means so they consider committing an illegal act as a way to solve the problem. The financial problem may be professional (e.g. job is in jeopardy) or personal (e.g. personal debt).

### *Insider trading*

Insider trading refers generally to buying or selling a security in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. Insider trading violations may also include 'tipping' such information, securities trading by the person 'tipped', and securities trading by those who misappropriate such information.

### *IP infringement (including trademarks, patents, counterfeit products and services)*

This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing them off as genuine.

### *Markets with a high level of corruption risk*

While corruption risk levels can be subjective, for the purposes of this survey we suggest a territory with a Transparency International Corruption Perception Index ("CPI") score of 50 or less be considered a market with a high level of corruption risk.

### *Money laundering*

Actions intended to legitimise the proceeds of crime by disguising their true origin.

### *Mortgage fraud*

Mortgage fraud schemes employ some type of material misstatement, misrepresentation or omission relating to a real estate transaction which is relied on by one or more parties to the transaction.

### *Opportunity or ability*

The individual finds some way that they can use (abuse) their position of trust to solve the financial problem with a low perceived risk of getting caught.

### *Procurement fraud*

Illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to his organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation.

### *Rationalisation*

The individual finds a way to justify the crime to themselves in a way that makes it an acceptable or justifiable act.

### *Tax fraud*

An illegal practice where an organisation or corporation intentionally avoids paying its true tax liability.

# Contributors

The 2014 Global Economic Crime Survey team consisted of the following individuals:

## *Survey leadership team*

- ***Steven Skalak***
  *Partner and Global Survey Champion*
  United States
- ***Didier Lavion***
  *Partner*
  United States

## *Survey management team*

- ***Matthew Curry***
  *Global Project Manager*
  United States

## *Survey marketing team*

- ***Anjali Fehon***
  *Marketing Director*
  United States
- ***Shannon Schreibman***
  *Global Marketing Manager*
  United States

## *Survey editorial board*

- ***Steven Skalak***
  *Partner*
  United States
- ***Didier Lavion***
  *Partner*
  United States
- ***Ian Elliott***
  *Partner*
  United Kingdom
- ***Vidya Rajarao***
  *Partner*
  India
- ***Muniu Thoithi***
  *Director*
  Kenya
- ***Alex Than***
  *Executive Director*
  Malaysia
- ***Brian McGinley***
  *Partner*
  China
- ***Claudia Nestler***
  *Partner*
  Germany
- ***David Harley***
  *Principal*
  Australia
- ***Malcolm Shackell***
  *Partner*
  Australia

## Forensic services

PwC's Forensic services network is comprised of forensic accountants, economists, statisticians, former regulators and law enforcement officers, fraud examiners, and forensic technologists. We help organisations tackle the major financial and reputational risks associated with economic crime. We identify financial irregularities, analyse complex business issues, and mitigate the future risk of fraud.

# *Belgian contacts*

## Forensic services leaders

***Rudy Hoskens***
Partner

Tel: +32 478 66 21 33
rudy.hoskens@be.pwc.com

***Jacqueline Gram***
Director

Tel: +32 478 25 83 80
jacqueline.gram@be.pwc.com

***Sally Trivino***
Director

Tel: +32 478 39 29 80
sally.trivino@be.pwc.com

© 2014 PwC Belgium. All rights reserved.

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with close to 184,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

# *Economic crime is on the rise —but you can fight back*

**36%**
More than one in three Canadian organizations reported being victims of economic crime.

**38%**
Over one third of Canadian organizations surveyed pursued an opportunity in a market with a high level of corruption.

**47%**
Almost half of respondents said their perception of cybercrime risk increased at their organization.

pwc

*Despite the efforts of organizations, regulators, law enforcement and anti-fraud practitioners, economic crime stubbornly persists. On the upside, this threat presents opportunities for sound management of fraud and corruption risk and strategic business positioning.*

# Contents

*With fraud's growth in sophistication and magnitude, it should come as no surprise to learn that economic crime continues to escalate as a priority for CEOs.*

# *Introduction*

Our 2014 PwC Global Economic Crime Survey ("survey") has reinforced the fact that, despite the efforts of organizations, regulators, law enforcement and antifraud practitioners, economic crime stubbornly persists. The real story is that economic crime may be attacking your business processes, eroding the integrity of your employees, and tarnishing your reputation. That is why this year's report focuses on how and where economic crime may be affecting you, and what your business can do about it.

Much like a virus, the many-faceted threat of economic crime is in a continuous state of mutation, opportunistically hiding within the macro trends affecting every organization and attacking organizations where they are most vulnerable.

Meanwhile, cybercrime continues to increase in volume and sophistication, and sometimes overlooked categories of economic crime—such as procurement fraud and human resource fraud—are moving up the list of threats, alongside asset misappropriation, bribery and corruption, money-laundering and accounting fraud.

With fraud's growth in sophistication and magnitude, it should come as no surprise to learn that economic crime continues to escalate as a priority for CEOs. More than half of chief executives polled in our *PwC 2014 Global CEO Survey* told us they are concerned or extremely concerned about bribery and corruption.

So this year, rather than simply waving the "red flag" of caution, we focus on the stories and strategies suggested by our survey data, because within the trends and global threats are strategic opportunities—not only for the sound management of risk, but also for business success and competitive advantage.

This report compares the 2014 Canadian survey results to the 2011 Canada and 2014 Global survey results, and sets the stage of our position relative to the world around us.

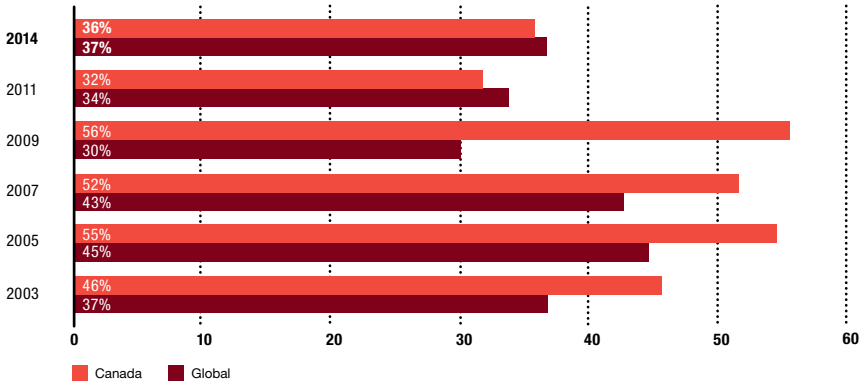
*Since our 2011 survey, there has been an increase both globally and in Canada in the number of organizations that reported being a victim of economic crime.*

# The big picture

The results of our 2014 survey show that 36% of Canadian organizations (37% globally) reported being victims of economic crime during the survey period. Figure 1 illustrates that, since our 2011 survey, there has been an increase both globally (3%) and in Canada (4%) in the number of organizations that reported being a victim of economic crime. This year's survey confirms that economic crime remains a fundamental fact of life for every segment of the global business community.

Since PwC's 2011 survey, Canada has reported lower instances of economic crime than our global counterparts. This trend may be due to Canadian organizations being more diligent in implementing robust anti-fraud regimes, including fraud risk assessments and whistle-blowing systems, reducing opportunities to commit fraud, and an increase in the organization's ability to prevent fraud in comparison to our global counterparts. Notwithstanding the above, the overall increase in reported instances of economic crime serves as a troubling statistic, as the number may likely be underreported.

**Figure 1: Organizations reporting fraud**

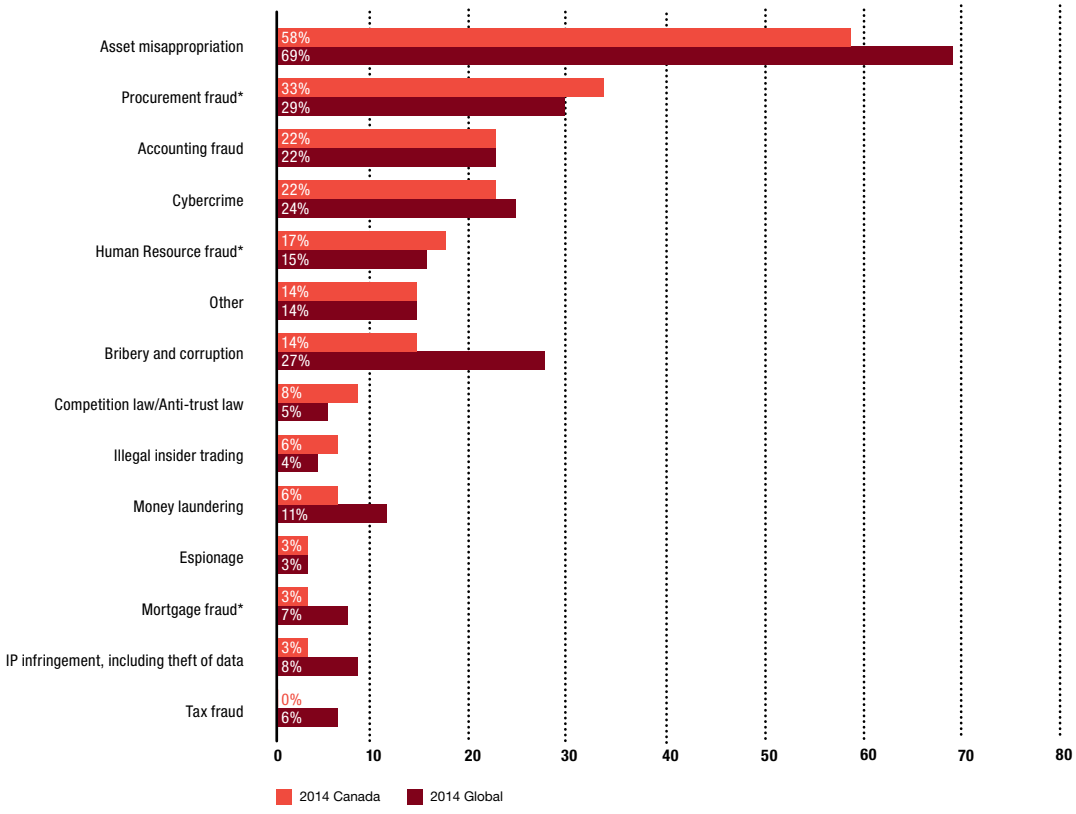


## Types of fraud

Economic crime comes in many flavours, each with its own characteristics, threats, and strategic consequences. Figure 2 shows the different types of economic crime experienced by Canadian respondents over the survey period. The most common type of fraud encountered by Canadian organizations surveyed was asset misappropriation, which is defined as the theft of assets (including monetary assets/cash or supplies and equipment) by individuals (eg. employees or directors) within an organization. Asset misappropriation was identified by 58% of Canadian organizations that were victims of economic crime in the survey period. Procurement fraud (33%), a new survey addition, was the next most common followed by cybercrime and accounting fraud (22%).

In addition to procurement fraud, we added two other distinct classifications in the 2014 survey: human resource fraud and mortgage fraud.

**Figure 2: Types of economic crime**




* Procurement fraud, mortgage fraud and human resource fraud were available to respondents to select as types of fraud experienced in the 2014 survey for the first time.

## The financial damage

While it is difficult to quantify the financial impact of economic crime, more than 1 in 10 Canadian respondents who had experienced economic crime in the survey period reported losses of more than US$5 million (see Figure 3).

It is noteworthy that the global results indicate that the percentage of respondents that experienced losses greater than US$100 million doubled from one to two percent from our previous survey. These large losses may be connected to the reported increase in incidents of bribery and corruption—frauds which can be especially costly to organizations due to regulatory fines, legal fees and remediation expenses.

**Figure 3: Financial losses**

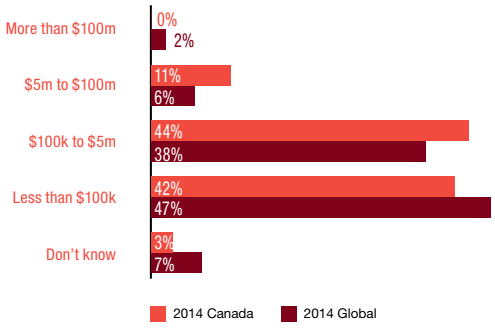
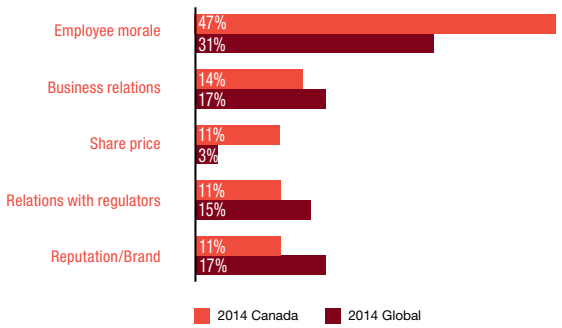



**Figure 4: Collateral damage —Significant impact on business operations**




## Collateral damage: Hard to quantify, hard to ignore

Economic loss is not the only concern that organizations face when combating fraud. Canadian respondents identified the most significant non-financial impact of fraud as the collateral damage to employee morale (47%), followed by a negative impact to business relations (14%) and brand reputation (11%). Figure 4 provides detail on organizations reporting significant collateral damage in Canada.

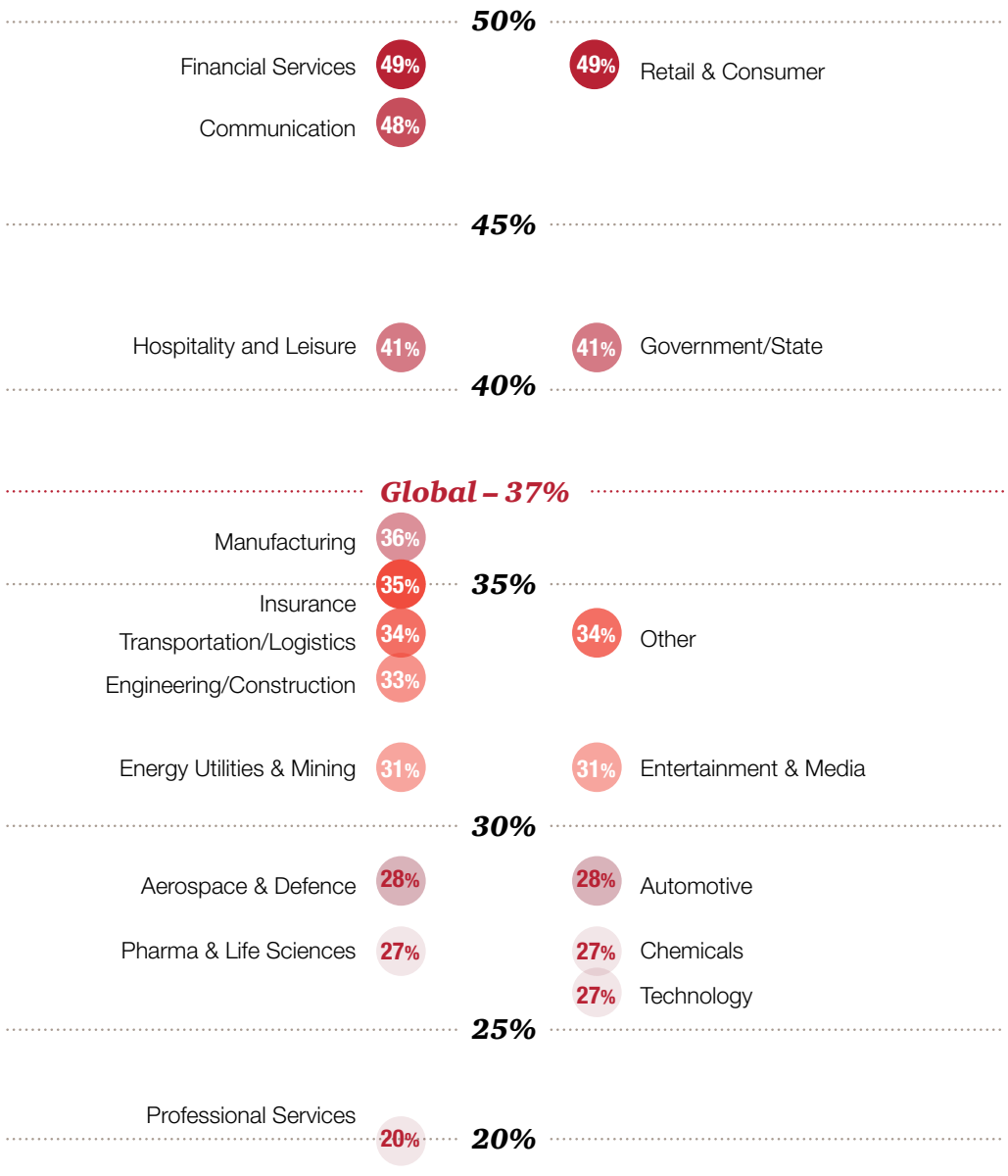
When taking into account collateral damage, the true cost of a fraud incident can be long lasting. While it is difficult to quantify in strictly financial terms, one fact is crystal clear: if fraud affects hiring, retention, business relationships and reputation, an organization's income statement will be impacted—even if it isn't labelled as "fraud". Today's employee is highly motivated by non-financial factors, including an atmosphere of teamwork and the knowledge that the employer is a "good place to work". Negative media attention or the perception that criminal activity is tolerated will impact employee morale and can tarnish an employee's perception of its employer.

Eleven percent of Canadian respondents felt their organization's reputation was significantly affected as a result of the economic crime experienced. However, since an organization's reputation is often closely tied to its competitive advantage, and can take years to repair if damaged, the impact of collateral damage should not be underestimated.

## Economic crime across industries

At the Global industry level, three sectors stand out for reports of economic crime—financial services, retail and consumer, and communication. Financial services fraud levels appear driven by comparatively high levels of cybercrime and money laundering. The retail and consumer sector, as expected, experienced a comparatively high level of asset misappropriation. The communication sector followed suit.  Figure 5 presents the results per industry.

**Figure 5: Economic crime reported by industry**




*% of all respondents who experienced economic crime over the survey period*

We observe a large clustering of industries reporting fraud in the 27% to 36% range. While the overall reported percentages are lower than the global mean (37%), many of these industries—in particular the Energy, Utilities & Mining, Engineering / Construction and Transportation/Logistics industries—are relatively more prone to experiencing economic crimes such as bribery and corruption or procurement fraud.

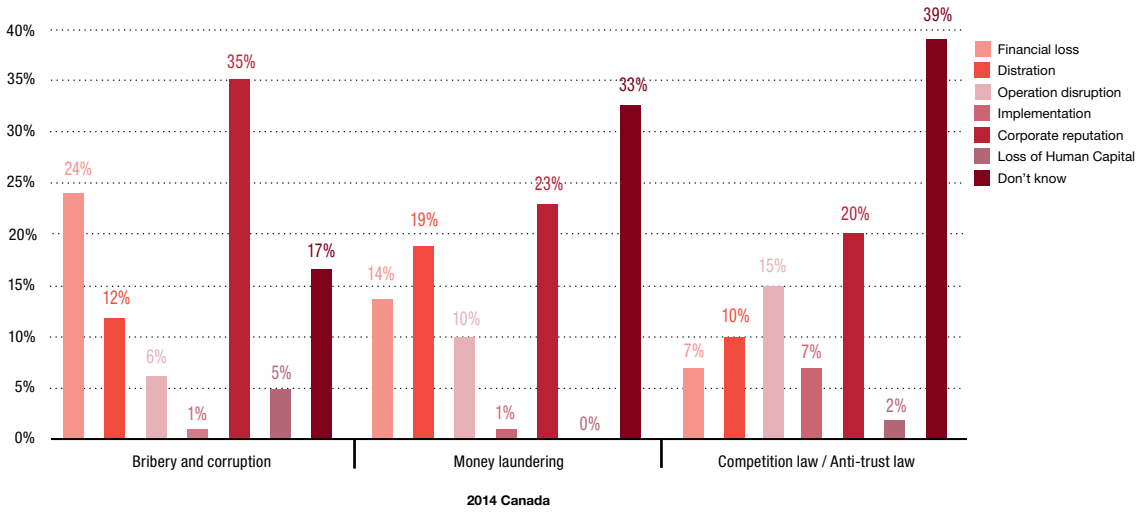
# *Bribery and corruption, money laundering and competition law/ anti-trust law:* in the spotlight

Some types of business crimes, such as bribery and corruption, money laundering, and anticompetitive behaviour, carry significantly more risks than others. All three of these crimes are enforced by government authorities and are subject to increasingly stringent standards, enforcement and harsh penalties. In an interconnected world, these three types of economic crime pose special dangers to global organizations.

If asset misappropriation is akin to a pickpocketing or burglary, a serious violation of an anti-bribery statute such as the Corruption of Foreign Public Officials Act, "CFPOA" or Foreign Corrupt Practices Act, "FCPA"—which can lead to substantial fines and a black mark on the organization—can resemble a systemic assault on your company.

In addition to triggering large fines and even criminal indictments, such violations can be seen as a larger organizational problem and can invite significant negative fallout—from reputational harm to financial losses, costly disruptions to your business, and leakage of your critical talent pool.

**Figure 6: Bribery and corruption , money-laundering and competition law/anti-trust law impact to organizations**



Our survey findings demonstrate these facts. With regard to bribery and corruption, money laundering, and/or competition law/anti-trust law, when asked what they perceived as being the most severe impact to their organization, Canadian respondents ranked negative impact to corporate reputation as being the most severe known impact across all three economic crime categories (35%, 23% and 20% of respondents respectively) followed by the following:

- **Bribery and corruption:** financial loss was ranked second at 24% of Canadian respondents, followed by distraction caused by legal/regulatory enforcement action (12%), operational disruptions (6%), loss of human capital (5%) and implementation of policy, procedures and tools to comply (1%).
- **Money laundering:** distraction caused by legal/regulatory enforcement action was ranked second at 19% of Canadian respondents, followed by financial loss (14%), operational disruptions (10%) and implementation of policy, procedures and tools to comply (1%).
- **Competition law/anti-trust law:** operational disruption was ranked second at 15% of Canadian respondents, followed by distraction caused by legal/regulatory enforcement action (10%), financial loss and implementation of policy, procedures and tools to comply (each at 7%) and loss of human capital (2%).

## Quantified losses

It is also important to take stock of the financial cost associated with bribery and corruption, money laundering and anticompetitive behaviour. As previously noted in this report, these types of frauds may not be the most prevalent (Figure 2). Nevertheless, our survey results illustrate that the cost associated with them can be enormous. More precisely:

- **Bribery and corruption:** 13% of Canadian respondents reported losses over US$100,000 and 4% reported losses as high as US$5 million to US$100 million;
- **Money laundering:** 4% of Canadian respondents reported losses as high as US$100,000 to US$1 million;
- **Competition law/anti-trust law:** 4% of Canadian respondents reported losses over US$100,000, and 1% reported losses as high as US$5 million to US$100 million.

When asked to rank the perceived risk of bribery and corruption, money laundering and competition laws/anti-trust law when conducting business globally, the majority of Canadian respondents (60%) ranked bribery and corruption as the highest.

# Bribery and corruption focus

Every global region reported a significant number of incidents of bribery and corruption. While Canada specifically did not rank among the highest countries reporting corruption, several interesting statistics were noted. These statistics are illustrated in Figure 7 below.

**Figure 7: Bribery and corruption: Specific impact to organizations**

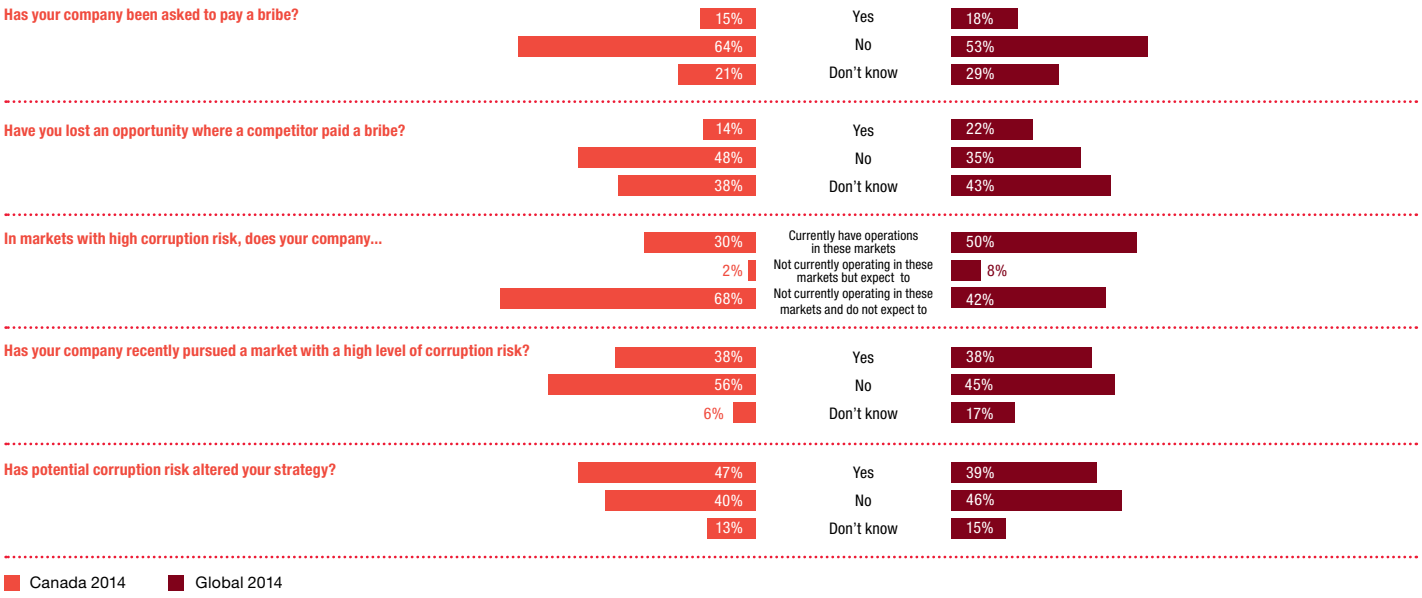


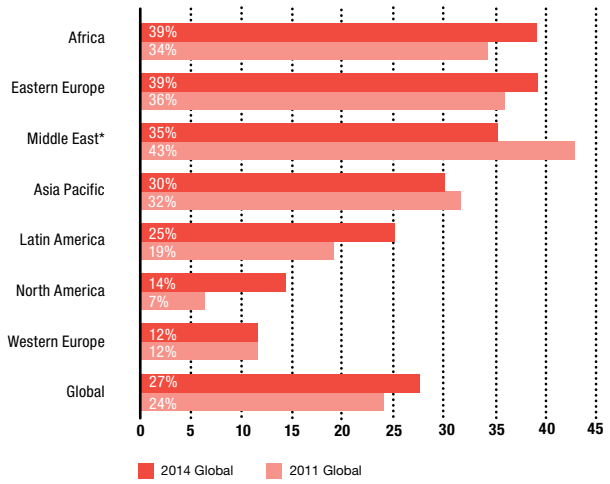

Figure 7 above shows us that overall, Canadian respondents reported fewer incidents (15%) than their global counterparts (18%) where they have dealt with requests for bribes. It was also noted that 14% of Canadian respondents believed they have lost an opportunity to a competitor who paid a bribe.

The results of our survey show that 50% of organizations globally have operations in markets with a high level of corruption risk, compared to only 30% of Canadian organizations. This large variance shows that Canadian organizations may not be prepared or feel comfortable with their current bribery and corruption risk management procedures and controls to enter into high risk markets. While Canadian organizations may have avoided high risk markets more than global organizations, they may also be potentially foregoing revenue opportunities in markets where fraud risk can be mitigated using an appropriate fraud risk management plan.

During the survey period, 38% of Canadian respondents noted that their organization recently pursued an opportunity in a market with a high level of corruption risk. Of these same respondents 47% altered their business plan due to the corruption risk while 40% did not. The remaining 13% did not know if they had or not, which is concerning given the consequences of corruption that have been previously demonstrated in this report. These statistics should alert management and boards to consider a fraud risk management plan, particularly when entering a high-risk market. With that said, of the 47% of respondents that altered their business plan, the survey indicated that 78% performed additional due diligence procedures. The next-highest strategy of these respondents (at 33%) was to walk away entirely, which again may point to a possible foregone opportunity and "money left on the table".

We believe that one driver of the high reported figures of bribery and corruption may be the larger trend of the shift in wealth from the developed economies of the West to the emerging high-growth economies of the South and East. Figure 8 below presents reported bribery and corruption by region reported by the global respondents.

**Figure 8: Reported bribery and corruption, by region**




* Middle East was included in the "Asia Pacific" raegion in 2011

As demonstrated in Figure 8 above, we observe a higher reported rate of bribery and corruption in regions such as Africa, Eastern Europe and the Middle East. Many of these countries or regions may have different cultural attitudes toward fraud and corruption, fewer regulations, and less strict enforcement of those regulations, thus creating a higher risk profile for this type of economic crime. So while North America (14%) and Western Europe (12%) are actually low on the scale of regions reporting bribery and corruption, their government enforcement practices have a considerable influence in this area.

Since bribery and corruption is often pursued by regulators across borders, organizations should be mindful of the significant risks involved with operations in these high-growth areas, even if local practices and customs are less rigorous.

## Bribery and corruption – confronting the risk

Regardless of your industry and regions of operations, what can you do to diminish the risk of bribery and corruption? We suggest focusing on four key areas:

1) **Management and tone at the top.** While compliance is everyone's responsibility, setting the right tone must start at the top, with an understanding of anticorruption statutes, a clear and consistent message that bribery will not be tolerated, and adequate resources to fight the threat.

2) **Risk assessment.** Your business and the compliance environment are constantly evolving, so it is essential that you conduct periodic risk assessments and ensure that any previously identified risks have been mitigated.

3) **Control environment.** Staying on the right side of anticorruption risk requires both a robust communication plan and vigilant internal enforcement procedures. That means not only a written code of conduct and employee training (including training on compliance-sensitive issues such as gifts and entertainment), but also a system of controls monitoring suspicious transactions. Finally, remember that you are only as compliant as your weakest link. Business partners, vendors and other third parties must be vetted and monitored to ensure risk associated with work in countries with increased exposure to corrupt practices is addressed.

4) **Evaluating effectiveness.** Risk assessment and control plans don't lead to compliance. Due diligence, periodic visits from management to high-risk locations, compliance reporting to the board, hotline follow-ups, following-up on reported incidents of fraud and corruption and business-partner audits all must be maintained and re-evaluated on an on-going basis as part of an effective internal compliance program.

*While Canadian organizations may have avoided high risk markets more than global organizations, they may also be potentially foregoing revenue opportunities in markets where fraud risk can be mitigated using an appropriate fraud risk management plan.*

# *Our networked world:* The benefits and risks are here to stay

*Cybercrime, also known as computer crime, is an economic offence committed using the computer and internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a by-product in order to create the fraud and only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one.*

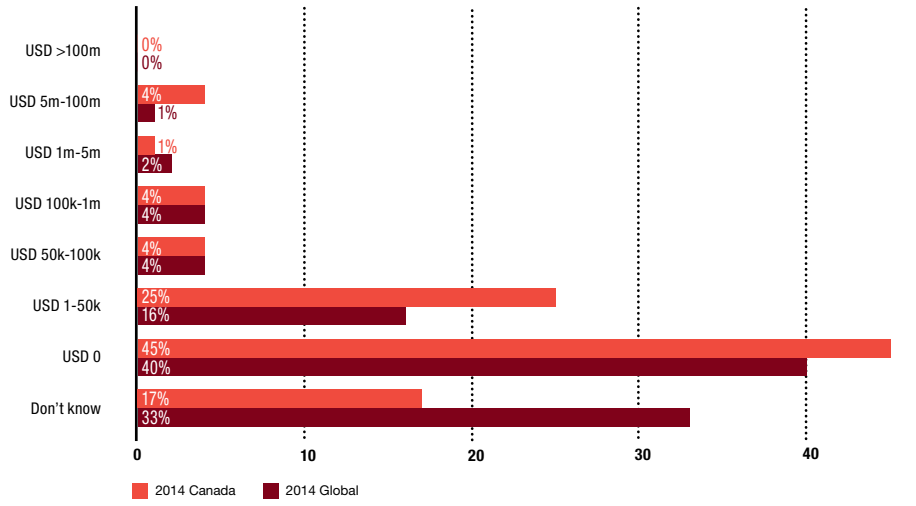
According to our 2014 survey, cybercrime continues to rank as one of the top economic crimes, behind asset misappropriation and procurement fraud (Figure 2). The advancement of technology in business services combined with the explosive growth in social media and dependence on organizational connectivity has increased the proliferation of cybercrime in our society.

As noted, connectivity and access have a dark side—one which empowers motivated, sophisticated criminals who are able to operate below the radar. Because cybercrime operates in the shadows, organizations may never even realize they are being targeted until long after the damage is done. This fact alone makes electronic fraud one of the most dangerous types of economic crime.

## The cost you can count

Our 2011 report was the first in our series that highlighted cybercrime as a high-level threat to organizations. This year's survey confirms the significant, continued impact of this crime on business, with now approximately one in four respondents reporting they have experienced a cybercrime (Figure 2)—and over 5% of these organizations suffering financial losses of more than US$1 million (Figure 9).

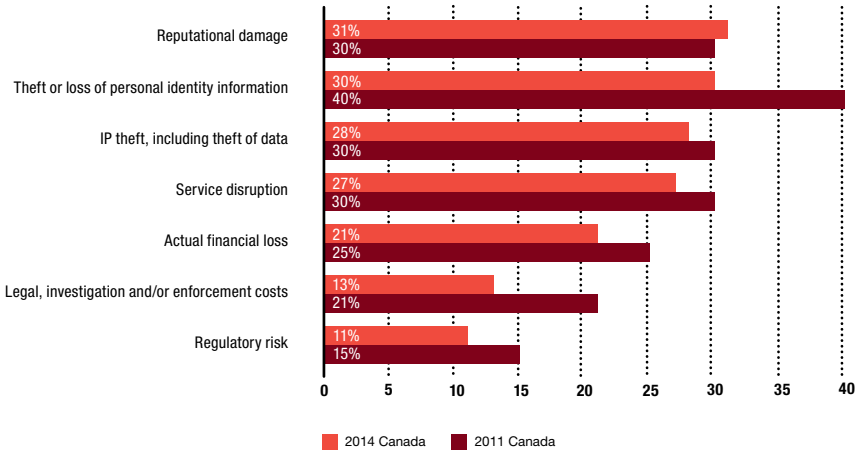
**Figure 9: Cybercrime: Estimated losses**



## The cost organizations care about

Acknowledging the financial repercussions associated with cybercrime, our survey results indicate that Canadian respondents have identified their greatest concerns related to cybercrime are reputational damage and the potential consequences associated with theft or loss of personal identifiable information. The potential cost related to these risks was considered to be a greater threat than the actual financial loss of cybercrime.

**Figure 10: The cost organizations care about**

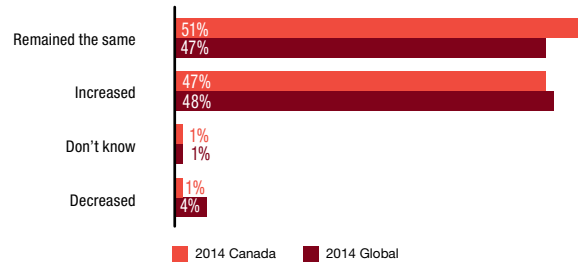



Survey results underscore that, when it comes to cybercrime, organizations understand indirect consequences may pose a much higher risk to the organization than the dollar value of the fraud. For example, a cyber-attack on a video game network resulting in leaked personal information can erode customer confidence, cause service disruptions and trigger a decline in users, all of which can affect the company from a monetary perspective. It is important to note that although you may not be able to immediately quantify the financial impact of cybercrime that does not necessarily diminish its severity. Falling victim to cybercrime rarely has just one consequence, and can have serious future implications.

## The perceived future of cybercrime

As a sign that organizations are taking the threat of cybercrime seriously, our survey indicates that 47% of respondents said their perception of cybercrime risk increased at their organization during the survey period. Only 1% of respondents noted that their perception of risk decreased. This illustrates the growing concern that organizations have towards cybercrime in Canada and around the world, and the need to remain aware of new and emerging cybercrime threats.

**Figure 11: Perception of the risks of cybercrime**



## What you don't know can hurt you

While approximately one quarter of respondents reporting cybercrime is concerning enough, consider that a significant percentage of those who did not report cybercrime may have suffered an event and not even known about it. That gives considerable cause for alarm.

Further complicating the picture is that even when it is detected, cybercrime often goes unreported. Outside of breaches in regulated areas such as identity theft, there are few regulatory requirements for disclosure. And often—such as in the case of theft of key intellectual property—there may be compelling competitive reasons for organizations to keep such losses confidential, to avoid public loss of trust or criticism.

For example, if a confidential bid planning document was accessed by cybercriminals and used by rivals to gain advantage, would an organization disclose the incident? Are organizations adequately defending against such cybercrime breaches, and if they were discovered, how would they value the loss?

The bottom line is that much of the damage wrought by these kinds of attacks is not disclosed, either because it is not known, is difficult to quantify, or because it is not shared. Naturally, this kind of operational murkiness poses risks for a business ecosystem that is increasingly reliant on both technology and intellectual property—and that values transparency.

An environment where it may be easier to steal a vital intangible asset than to value, disclose, or even detect its loss, is a risky one.

## Data integrity is under attack

The data collected and stored with many businesses often contains private information, providing cybercriminals with opportunities to steal data which can be used for multiple purposes, including accessing financial accounts and extracting cash.

Businesses today are highly dependent on technology and connectivity, which amplifies the impact of cyber-attacks affecting: intellectual property, competitive advantage, operational stability, regulatory compliance and reputation, in addition to data integrity. Not all information assets are equal and they continue to grow at an extraordinary rate. Safeguarding all data at the highest level is just not realistic, or possible. Loss of some types of data is troubling; loss of others can destroy parts of a business.

Your critical data is likely distributed and disbursed throughout the ecosystem, greatly expanding the domain you need to be concerned with and protect. The integrity and stability of your business is now, more than ever, dependent on those in your data network.

An unintended consequence of the technology enablement within the business environment is the growing vulnerabilities being exploited by adversaries—significantly increasing the exposure and impact on the business. Examples include the theft of research and development information, rapid replication of product or process, access to strategic or customer information, or the disruption of operational stability. Ultimately these adversaries undermine a company's long-term profitability and competitive advantage.

Company leaders and boards can no longer afford to view cyber-attacks as a technology problem; cyber-attacks are now an enterprise risk issue. It starts at the top, with senior executives viewing cybersecurity as an integral part of their business agenda and risk tolerance.

## Cybercrime is a human problem, not a technology problem

Even when organizations are generally aware of the types of cyber-threats they face, many do not truly understand the capabilities of cybercriminals, what cybercriminals might target, and what the value of those targets might be. Organizations seek ways to make their critical data available to management, employees, vendors, and clients on a multitude of platforms—including high-risk ones such as mobile and cloud—because the economic and competitive benefits appear so compelling.

It is intuitively easy to understand the benefits of data availability. And nobody expects organizations to shrink their digital data footprint. However, with increasing volumes of data more accessible on even more platforms, it's clear that valuable data will remain under attack, and that the cost of security breaches will continue to be steep.

The truth is, in today's nerve-net global business community, the landscape is constantly changing, and the sophisticated adversary takes advantage by attacking new weaknesses. This is why it is essential for organizations to keep pace with the forces that threaten them. Ultimately, cybercrime is not a technology problem, it is a human problem involving both strategy and process.

## Defense against cyber-attacks

- **Get the CEO involved** – the CEO and the board of directors need to be aware of cyber threats and understand the risks and opportunities of the cyber world.
- **Reassess** – reassess the security function and preparedness of the organization should a cybercrime occur. Unlike traditional economic crimes, cybercrime vulnerabilities are constantly evolving with technology, which means an organization needs to adapt its procedures continually.
- **Build awareness** – organizations need to have a clear awareness of the current and emerging cyber environment. By understanding it, well informed and prioritized decisions and actions can be taken.
- **Create a cyber-incident response team** – a team which needs to act with speed and agility. A well-functioning cyber response team means once an incident is spotted anywhere in the business, it will be tracked, risk-assessed and escalated.
- **Educate all employees** – an organization needs to embed a 'cyber awareness' culture and the relevant policies, protocols and procedures must be communicated to all employees.
- **Take a more active and transparent stance towards cybercrime** – take action by pursuing cybercrime perpetrators through legal means and communicate more publicly the actions the organization is taking regarding the threats, incidents and responses.

# *Procurement fraud:* A growing opportunity, a growing threat

As discussed previously, this year we added procurement fraud—illegal conduct by an employee, owner, vendor, or official in connection with the purchase of services, goods or assets for an organization, often for the individual's personal gain—as a new category of economic crime in our survey.

Generally speaking, when an organization goes outside its own walls for services, goods or assets, the potential for procurement fraud exists. We suspect two drivers led to a significant response in this category.

First, as our recently launched *2014 Global CEO Survey* highlights, we have seen an increased interconnectedness of business entities in outsourcing elements of the value chain, purchase of materials, or increased reliance on suppliers.

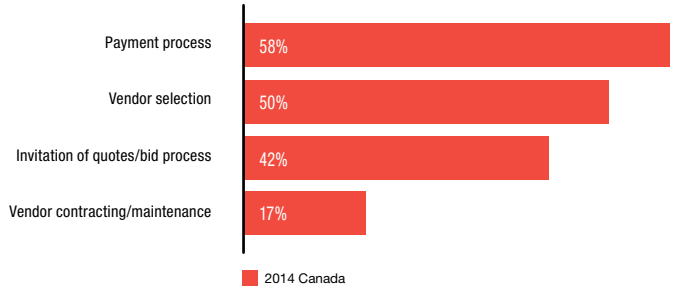
Second, as economies have emerged from the recent economic crisis, a shift in staffing practices seems to have occurred. Short-term, post-crisis measures such as replacing permanent, in-house positions with more dispensable and scalable outside resources have in many instances persisted, with organizations more willing to outsource tasks. This change in hiring has left organizations susceptible to segregation of duties issues in the procurement process.

The high levels of responses of procurement fraud reported—33%, second only to asset misappropriation (Figure 2)—exceeded our expectations. This could be partly attributable to the connection of procurement fraud to bribery & corruption. In past surveys, procurement-related kickbacks, bid-rigging, or similar activities may have been reported with bribery and corruption. Still, its appearance in the number-two spot is worthy of note.

## Occurrence of procurement fraud

Figure 12 illustrates that Canadian respondents noted procurement fraud primarily occurred during the payment process (58 %), vendor selection (50%) and bid process (42%).

**Figure 12: Where does procurement fraud take place?**



*By implementing a few strategies, organizations can potentially reduce procurement fraud and also streamline the bid process and vendor selection*

## The purchasing and supply process under attack

As noted, the bid process/vendor selection workflow areas are ripe for fraud. An individual within the purchasing and supply department may have a pre-existing relationship with a vendor who wants to win business from the organization. The insider provides information on the bidding process, such as the bid amounts of competitors, to ensure an advantage for their preferred bidder. Conversely, the insider could approve a price higher than necessary.

A public sector procurement process provides an example of how easily the purchasing and supply process can be attacked. The public sector can make large, long-term purchases of expensive, sophisticated equipment in markets where only a limited number of suppliers have the scale to compete. On the service side, these organizations regularly solicit bids with numerous smaller responsibilities, such as equipment servicing, food & housing services, or logistical support.

In non-competitive and often non-transparent environments, these bids provide an opportunity for procurement fraud. We have seen a number of high-profile scandals in such environments over the past several years and expect to see more in the years ahead.

## Fighting back

It's a bit of a paradox that while anti-bribery and anti-corruption policies have been implemented at many organizations—often through pressure from the C-suite, mindful of high-profile anticorruption statutes such as the CFPOA—there are far fewer training programs in place for the closely related procurement fraud.

Yet procurement fraud training would likely be far less complex and costly, as the risk factors are more straightforward and more easily identified.

By implementing a few strategies such as the following, organizations can potentially reduce procurement fraud and also streamline the bid process and vendor selection:

- Ensure the company solicits sealed bids that are revealed before a group of people. This will ensure the integrity of the bids and the tendering process;
- Institute segregation of duties within the purchasing/procurement departments to ensure that several individuals are involved in the process; and,
- Consider using different vendors for different projects. For example, requiring vendors to be reviewed or retendering for the work on a regular basis sends the message that vendors will have to remain competitive with market prices. It will also give the organization comfort by seeing what other prices/services the market can provide.

# *Accounting fraud:* The persistent threat

Accounting fraud has always been one of the most commonly reported types of economic crime in our survey, and since 2005 has been cited by over 20% of our global respondents that experienced economic crime.

This year was no exception. From a Canadian standpoint, 22% (Figure 2) of respondents reported having experienced accounting fraud. This is equal to the 22% (Figure 2) noted through the 2014 Global figures.

Financial statements are a fundamental barometer of a business—and a traditional starting point for analyses relating to credit decisions, contract awards, and capital raising in public markets. Accounting fraud—which includes misleading or falsely prepared financial statements—can dupe banks, lessors, vendors, and investors into risky or misguided decisions. Due to the ubiquitous use of financial statements and financial data in business operations, this kind of economic crime impacts a variety of business processes.

# *Asset misappropriation:* Above and beyond

Asset misappropriation is by far the most common economic crime, experienced by 58% of respondent organizations reporting any fraud (Figure 2). This amount is almost double the incidence rate of procurement fraud, the second-highest reported type of economic crime. While the individual impact of this fraud may be lower than that of cybercrime or bribery and corruption, the magnitude of the threat requires organizations to be vigilant.

## (Not) falling off the back of a truck

You have likely heard the phrase "falling off the back of the truck." This euphemism for asset misappropriation points to one of the fundamental business processes it attacks—distribution, logistics and warehousing.

Take a global retail company with warehouses of inventory. Not only are these products exposed to employees, they also pass through several third party organizations, leading to several points of vulnerability in the supply chain and distribution process. Schemes can be as simple as employees walking off with inventory, or more complicated endeavours such as marking good inventory as "scrap" and then reselling it.

Asset misappropriation also includes the theft of cash through embezzlement, often at the hands of an authority responsible for custody of the money. One example of the many schemes in this category include "lapping" customer accounts, where a fraudster steals money from one customer account and replaces it with money received from another customer. There are multiple ways these criminals try to obscure their crimes—such as defrauding in small amounts in order to evade warning triggers.

## Fighting back against asset misappropriation

As these types of fraud mainly occur in a trusted business environment, the best advice for organizations is to implement common sense procedures, such as:

- **Know your employee:** Obtain independent employment checks, and don't ignore the results.
- **Know your vendor:** Just as employers conduct background checks on employees with access to valuable assets, an organization should conduct checks on potential vendors.
- **Segregate job duties:** Ensure multiple individuals are involved in any process that results in cash or inventory distribution, making it more difficult for the fraudster to operate undetected.

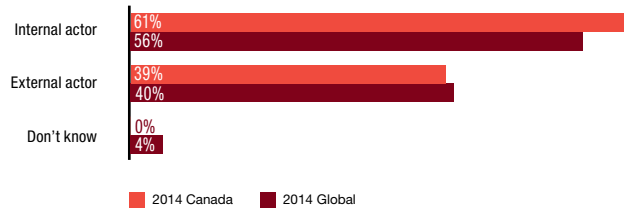
While reading through this list of popular frauds and potential risks to an organization's assets, it is important to remember that by implementing a well-conceived and designed fraud risk management plan, several controls can be used to prevent multiple types of fraud. For example, by implementing segregation of duty controls throughout the company, you can potentially prevent asset misappropriation through reduced opportunity for employees to "walk-off" with goods, in addition to preventing procurement fraud through a segregated bid process.

# The internal vs external fraudster

## Who's committing fraud? The enemy hiding in plain sight

A rule of thumb in fighting economic crime is the same as in any battle: know your enemy. We asked respondents whose organization had experienced economic crime, to profile the main perpetrator of the most serious fraud they had faced. As presented in Figure 13, 61% of organizations reported that the main perpetrator was internal, while 39% reported the main perpetrator was external.

**Figure 13: Who was the main perpetrator of fraud?**




The silver lining of having most of one's fraud losses attributable to internal players—people you theoretically have some visibility over—is that there is upside potential in mitigating these risks through improved internal policies, processes and controls. This is not always the case with external fraudsters.

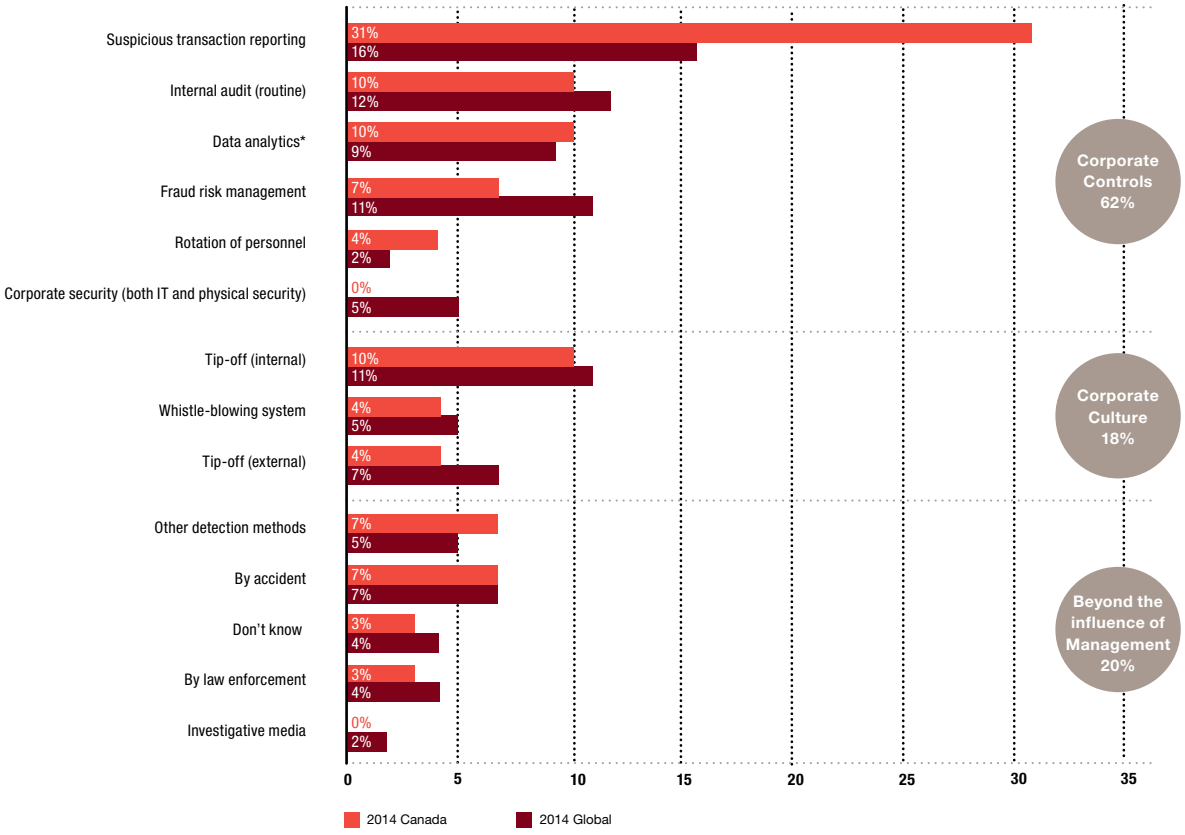
*31% of the frauds reported were detected by suspicious transactions reporting.*

## To catch a thief

So how do you stop an economic crime before it happens—or at least, while it is happening?

Fraud detection methods usually fall into one of three categories: corporate controls, corporate culture, or events beyond the influence of management. Figure 14 displays the methods by which the major fraudster at organizations was detected. Canadian survey statistics show that 31% of the frauds reported were detected by suspicious transactions reporting.

**Figure 14: Fraud detection methods**




* Data Analytics was added as a category in the 2014 survey.

## The internal fraudster

Practitioners commonly refer to a "Fraud Triangle"—the three elements often present when a perpetrator commits fraud: pressure, opportunity and rationalization.

Three quarters (73%) of our respondents indicated the opportunity or ability to commit the crime was the factor that most contributed to economic crime by an internal perpetrator. While this news may at first seem anticlimactic, it's important to keep in mind that, of the three factors, opportunity is the one most in an organization's control. The implication is that while life's pressures and the ability to rationalize may exist, if an organization can limit the opportunity, they may be able to stop the fraud before it starts.

While we cannot plot the specific pressure or rationalization behind each internal act of fraud, we can at least profile the perpetrator. We asked respondents who had pointed to an internal player as the main perpetrator of economic crime to profile the staff level, age, gender, length of service, and education level of that perpetrator. The results are presented in Figures 15 and 16:

**Figure 15: Internal perpetrator (staff level)**

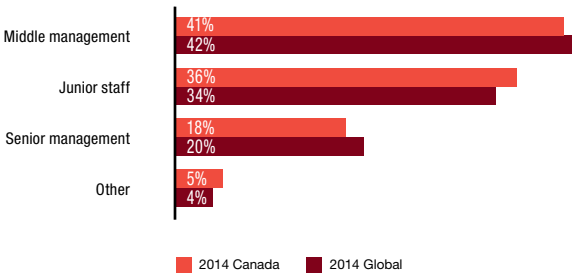
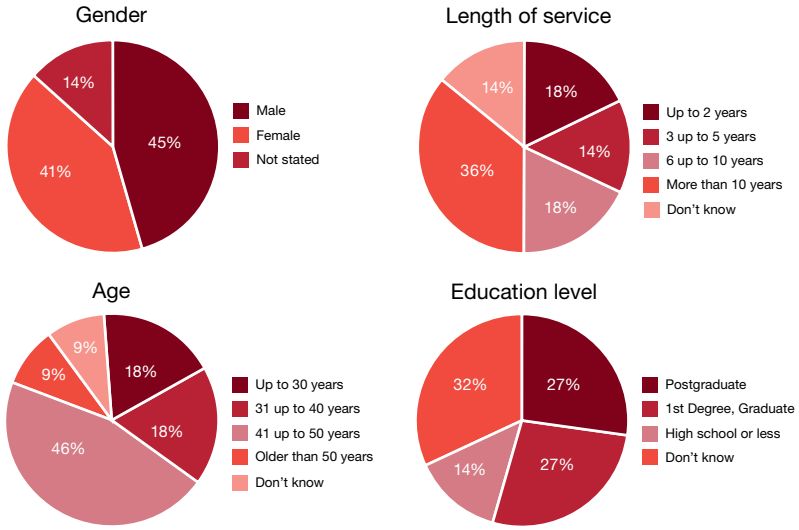



**Figure 16: Profile of the internal fraudster**




2014 Canada

Our 2014 Canadian results indicate that the profile of the internal fraudster were both middle-aged males (45%) and females (41%), with a college education or higher who have been with the organization more than 10 years. These individuals are mainly in a middle management role.

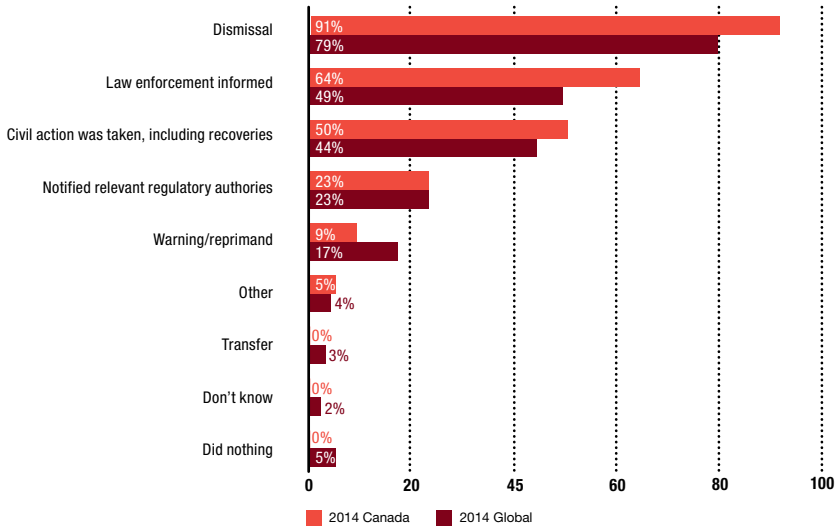
It is important to note that the profile of the fraudster is trending towards long-serving and more sophisticated fraudsters. While survey results show that economic crimes committed by senior management were fewer than by employees at more junior levels, these crimes tend to be more sophisticated and larger in dollar value. As sophisticated frauds are more difficult to detect, this could also be a factor as to why economic crimes committed by senior management were not identified nearly as often as those committed by middle management or junior staff.

## Confronting the internal perpetrator

This year's survey confirms that organizations continue to respond to internal fraud aggressively, with over 90% saying they are dismissing perpetrators once detected. Overall, Figure 17 illustrates the importance in the use of inter-firm actions—including dismissal, informing law enforcement, civil action and notifying regulatory authorities—against internal perpetrators.

The telling statistic is that there were no Canadian organizations that either didn't know or did nothing with regards to what actions were taken against internal perpetrators. This serves as a warning to the would-be internal perpetrators: if you get caught, there will be consequences.

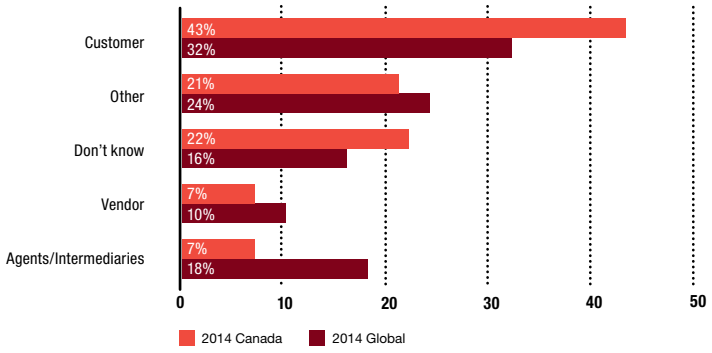
**Figure 17: Actions taken against internal perpetrator**




## The external fraudster

Forty three percent of Canadian organizations reported customers as being the primary external perpetrator of fraud.

**Figure 18: External perpetrator (role)**

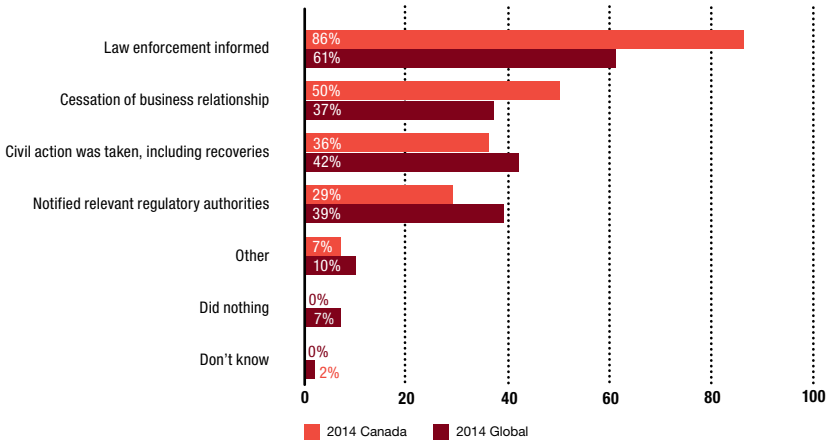



## Actions against the external fraudster

The most common action taken against external perpetrators was informing law enforcement (86%). Survey results indicate that organizations are more likely to inform law enforcement if perpetrators are external (as opposed to internal – see Figure 17 (64%)). There are numerous reasons for organizations to vary their actions against external perpetrators, including the reality that dismissal is not an available option for an external perpetrator.

There are many hurdles to overcome during an investigation into concerns of fraud, whether by an internal or external perpetrator. One of the major hurdles is that law enforcement agencies often do not have the capacity to conduct full investigations into allegations of fraud. As a result, it is important for the victim company to have a proper investigative protocol in place to ensure the alleged fraud is investigated fully by the company prior to turning these findings over to law enforcement.

**Figure 19: Actions taken against external perpetrator**

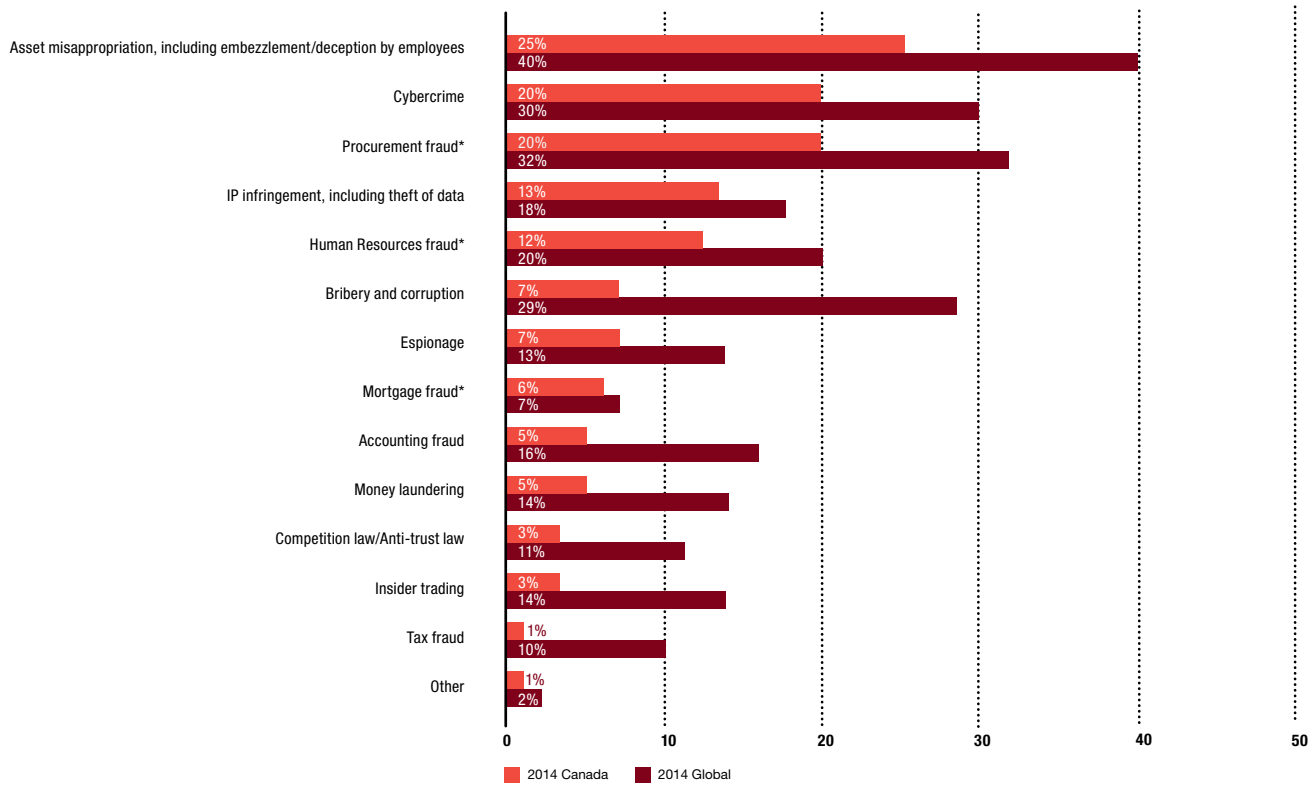


*30% of Canadian respondents stated that their respective organizations had not performed a fraud risk assessment during the survey period*

# Organizations see more fraud ahead

Figure 20 outlines the perceived threats of economic fraud that organizations believe they are facing over the next 24 months. The majority of respondents (25%) believe their organization is susceptible to asset misappropriation, followed by both cybercrime and procurement fraud (20%).

**Figure 20: Perception of fraud over the next 24 months**




* Procurement fraud, mortgage fraud and human resource fraud were available to respondents to select as types of fraud experienced in the 2014 survey for the first time.

Despite economic crime experienced and the perception of increased fraud risk, 30% of Canadian respondents stated that their respective organizations had not performed a fraud risk assessment during the survey period. When respondents were asked the main reason their organizations had not performed a fraud risk assessment in the last 24 months:

- 53% indicated the perceived lack of value;
- 17% responded that they were not sure what a fraud risk assessment involved;
- 7% stated that cost was the main reason one had not been performed; and
- 7% did not know why a fraud risk assessment had not been performed.

When directors take an active interest in fraud within their organization, and take robust disciplinary action towards the perpetrators of fraud, the right "tone at the top" is established. The 2014 survey results demonstrate that an organization's ethical "tone at the top" combined with a strong internal control environment provide the strongest deterrent to fraudulent behaviour and increases the likelihood of detecting fraudulent activities.

A corporate culture that clearly stresses the importance of integrity – where senior management is seen as "walking the talk", and that has a well-communicated, comprehensive anti-fraud regime – is less likely to be victimized by economic crime.

## Implementing an effective anti-fraud regime

When assessing and reviewing an organization's anti-fraud regime, management should consider obtaining professional advice on effective compliance and detection programs, ensuring that anti-fraud guidelines and practices remain current in the face of a changing economic climate, and that measures taken consider the laws and cultures of relevant operating jurisdictions within the global marketplace.

We believe that the key anti-fraud controls should include the following:

1. Governance – oversight by the audit committee and board of directors;
2. Fraud risk assessment;
3. Code of business conduct and ethics;
4. Incident reporting mechanisms;
5. Investigation protocol (including suspicious transaction reporting);
6. Remediation protocol;
7. Hiring and promotion policies and procedures; and
8. Management evaluation and testing.

*A corporate culture that clearly stresses the importance of integrity – where senior management is seen as "walking the talk", and that has a well-communicated, comprehensive anti-fraud regime – is less likely to be victimized by economic crime.*

# Contact us

## Forensics team

**Steven P. Henderson**
National Forensic Services Leader
Toronto
416 941 8328
steven.p.henderson@ca.pwc.com

**Lori-Ann Beausoleil**
Forensic Consulting Leader
Toronto
416 687 8617
lori-ann.beausoleil@ca.pwc.com

**Peter Vakof**
Forensic Technology Services Leader
Toronto
416 814 5841
peter.vakof@ca.pwc.com

## Calgary

**Krista A. Mooney**
Director
403 509 7336
krista.a.mooney@ca.pwc.com

## Halifax

**Paul F. Bradley**
Associate Partner
902 491 7436
paul.f.bradley@ca.pwc.com

**James A. Pomeroy**
Vice President
902 491 7416
james.a.pomeroy@ca.pwc.com

## London

**Chris Gray**
Vice President
519 640 8011
chris.gray@ca.pwc.com

## Montréal

**Marie-Chantal Dréau**
Partner
514 205 5407
marie-chantal.dreau@ca.pwc.com

**Benoit Legault**
Vice President
514 205 5682
benoit.legault@ca.pwc.com

## Ottawa

**Kas Rehman**
Partner
613 755 4328
kas.rehman@ca.pwc.com

**Chantal Amyot**
Director
613 755 4355
chantal.amyot@ca.pwc.com

**Jason Armstrong**
Director
613 755 8743
jason.r.armstrong@ca.pwc.com

**Steve Malette**
Vice President
613 755 5979
steven.m.malette@ca.pwc.com

## Toronto

**Sarah E. MacGregor**
Partner
416 814 5763
sarah.e.macgregor@ca.pwc.com

**Harm Atwal**
Director
416 869 2330
harm.k.atwal@ca.pwc.com

**Jeff Bowen**
Director
416 869 2472
jeff.r.bowen@ca.pwc.com

**H. Ray Haywood**
Director
416 814 5801
h.ray.haywood@ca.pwc.com

**Roberto Israel**
Director
416 814 5740
roberto.r.israel@ca.pwc.com

**Kelly Ohayon**
Director
416 814 5843
kelly.ohayon@ca.pwc.com

**Lloyd Wilks**
Director
416 687 8115
lloyd.wilks@ca.pwc.com

## Winnipeg

**Jeffrey Johnson**
Partner
204 926 2441
jeffrey.b.johnson@ca.pwc.com

**Dave Johnson**
Vice President
204 926 2423
dave.a.johnson@ca.pwc.com

**Kyla Kramps**
Vice President
204 926 2434
kyla.kramps@ca.pwc.com

*www.pwc.com/ca/crimesurvey*

To view a copy of our reports scan the QR code with a QR reader app on your smart phone or tablet

***Value, on your terms***

We focus on four areas: assurance, tax, consulting and deals services. But we don't think off-the-shelf products and services are always the way to go. How we use our knowledge and experience depends on what you want to achieve. PwC Canada has more than 5,700 partners and staff in offices across the country. Whether you're one of our clients or one of our team members, we're focused on building deeper relationships and creating value in everything we do. So we'll start by getting to know you. You do the talking, we'll do the listening. What you tell us will shape how we use our network of more than 184,000 people in 157 countries around the world—and their connections, contacts and expertise—**to help you create the value you're looking for.** See www.pwc.com/ca for more information.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisers.

Parts of this report were originally published as "Economic crime: a threat to business globally" in the US, used with permission from PwC US.

© 2014 PricewaterhouseCoopers LLP, an Ontario limited liability partnership. All rights reserved. PwC refers to the Canadian member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. 3350-03-0214

# *Le crime économique gagne du terrain, mais vous pouvez le combattre*

**36 %**
Un peu plus du tiers des organisations canadiennes ont déclaré avoir été victimes de crimes économiques.

**38 %**
Plus du tiers des organisations canadiennes sondées se sont récemment intéressées à une possibilité d'affaires sur un marché caractérisé par un risque élevé de corruption.

**47 %**
Près de la moitié des répondants canadiens ont affirmé que la perception du risque de cybercriminalité s'est accrue au sein de leur organisation.

pwc

*www.pwc.com/ca/fr/crimesurvey*

*En dépit des efforts des organisations, des autorités réglementaires et de tous les professionnels qui luttent contre la fraude, le crime économique persiste. Cette tendance présente des occasions non seulement de mieux gérer les risques de fraude et de corruption, mais aussi d'améliorer le positionnement stratégique des organisations.*

# Table des matières

*La sophistication et l'ampleur croissantes du crime économique font que ce type de crime constitue une préoccupation grandissante pour les chefs de direction.*

# *Introduction*

Le sondage Global Economic Crime Survey 2014 (« le sondage ») mené par PwC a confirmé qu'en dépit des efforts des organisations, des autorités réglementaires et de tous les professionnels qui luttent contre la fraude, le crime économique persiste. Le crime économique peut attaquer vos processus opérationnels, entacher l'intégrité de vos employés et ternir votre réputation. C'est pour toutes ces raisons que le rapport de cette année se concentre sur la manière dont ce crime peut vous affecter et sur ce que vous pouvez faire pour le combattre.

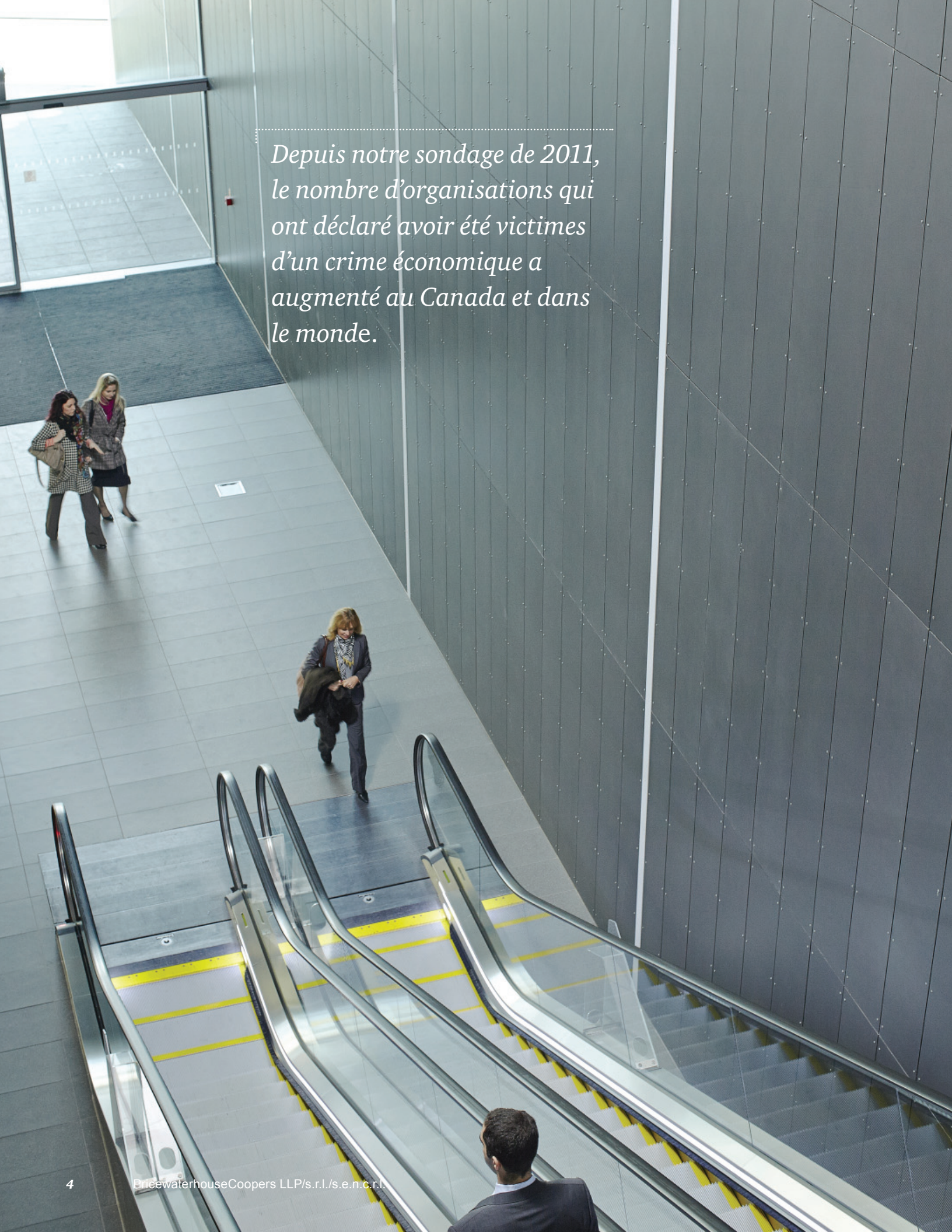
Comme les virus, le crime économique est une menace à facettes multiples en mutation constante; il se dissimule de manière opportuniste au sein des tendances de fond qui touchent chaque organisation et attaque les organisations là où elles sont le plus vulnérables.

La cybercriminalité ne cesse de prendre de l'ampleur et devient de plus en plus sophistiquée, et des catégories de crimes économiques parfois occultées – comme la fraude liée à l'approvisionnement ou la fraude relative aux ressources humaines – remontent vers les premières places sur la liste des menaces, en compagnie d'autres catégories comme le détournement d'actifs, le trafic d'influence et la corruption, le blanchiment d'argent et la fraude comptable.

La sophistication et l'ampleur croissantes du crime économique font que ce type de crimes constitue une préoccupation grandissante pour les chefs de direction. Plus de la moitié des dirigeants de organisations qui ont participé à notre « Enquête mondiale 2014 menée auprès des chefs de direction » ont déclaré que le trafic d'influence et la corruption les inquiétaient ou les inquiétaient fortement.

Cette année, au lieu d'agiter le « drapeau rouge » de la mise en garde, nous nous concentrons sur les thèmes – et les stratégies – suggérés par les résultats de notre sondage, parce qu'il se cache au sein des tendances et des menaces mondiales des opportunités stratégiques – non seulement de bien gérer les risques, mais aussi d'assurer la réussite des organisations et de leur donner un avantage concurrentiel.

Ce rapport présente une comparaison entre les résultats du sondage canadien de 2014, ceux du sondage canadien de 2011 et ceux du sondage mondial de 2014. Il établit la position du Canada par rapport au reste du monde en matière de crimes économiques.



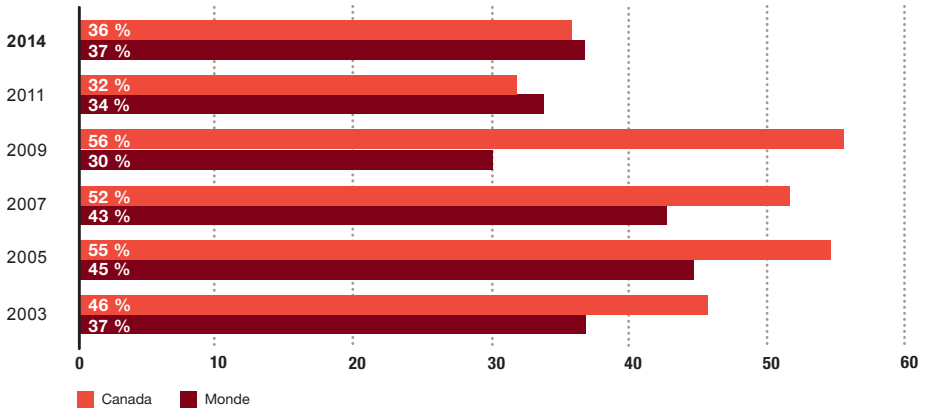
*Depuis notre sondage de 2011, le nombre d'organisations qui ont déclaré avoir été victimes d'un crime économique a augmenté au Canada et dans le monde.*

# *Le portrait général de la situation*

Les résultats de notre sondage de 2014 indiquent que 36 % des organisations canadiennes (37 % à l'échelle mondiale) ont déclaré avoir été victimes d'un crime économique au cours de la période visée par le sondage. La figure 1 montre que, depuis notre sondage de 2011, le nombre d'organisations qui ont déclaré avoir été victimes d'un crime économique a augmenté au Canada (4 %) et dans le monde (3 %). Le sondage de cette année confirme que le crime économique reste une réalité incontournable pour les organisations, et ce, peu importe où elles sont situées dans le monde.

Depuis le sondage mené en 2011 par PwC, moins de crimes économiques ont été signalés au Canada qu'ailleurs dans le monde. Cette tendance pourrait s'expliquer par le fait que les organisations canadiennes sont plus diligentes que les autres à mettre en œuvre des programmes antifraudes robustes, comprenant des mesures d'évaluation des risques de fraude et la mise en place de systèmes de dénonciation, ce qui réduit les occasions de commettre des fraudes et renforce la capacité de l'organisation de les détecter. Cependant, cette augmentation globale du nombre de crimes économiques est troublante, car le nombre de crimes signalés risque d'être inférieur à la réalité.

**Figure 1 : Organisations ayant déclaré une fraude**

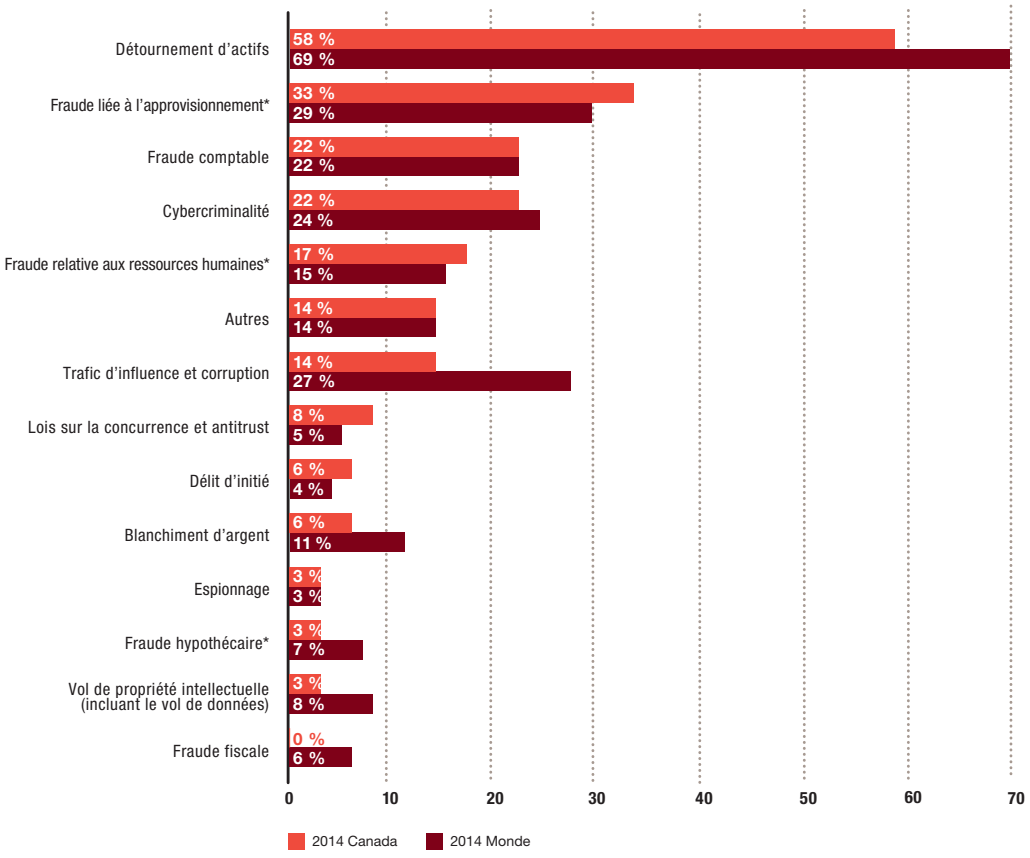


## Les types de crimes économiques

Le crime économique prend diverses formes, chacune ayant ses propres caractéristiques, menaces et conséquences stratégiques. La figure 2 montre les différents types de crimes économiques déclarés par les répondants canadiens. Le crime le plus courant est le détournement d'actifs, soit le vol de biens de l'organisation (y compris les actifs monétaires ou en espèces ou les fournitures et le matériel) par des personnes (p. ex., des employés ou des dirigeants) de l'organisation. Le détournement d'actifs est cité par 58 % des organisations canadiennes qui disent avoir été victimes d'un crime économique au cours de la période visée par le sondage. La fraude liée à l'approvisionnement (33 %), une nouvelle catégorie ajoutée à notre sondage, est la seconde catégorie la plus courante. Viennent ensuite la cybercriminalité et la fraude comptable (toutes deux à 22 %).

En plus de la fraude liée à l'approvisionnement, nous avons ajouté deux nouvelles catégories de crimes économiques à notre sondage de 2014 : la fraude relative aux ressources humaines et la fraude hypothécaire.

**Figure 2 : Types de crimes économiques**




* Les répondants pouvaient sélectionner ces catégories de crimes économiques pour la première fois lors de notre sondage de 2014.

## Le préjudice financier

Bien qu'il soit difficile de mesurer le coût financier d'un crime économique, plus de un répondant canadien sur dix ayant indiqué qu'un crime économique a affecté leur organisation pendant la période visée par le sondage ont déclaré des pertes de plus de 5 millions $ US (figure 3).

Par ailleurs, à l'échelle mondiale, le pourcentage de répondants qui ont déclaré que leur organisation avait subi des pertes de plus de 100 M$ US a doublé depuis notre dernier sondage, passant de 1 % à 2 %. Ces pertes élevées sont peut-être attribuables à l'augmentation des cas de trafic d'influence et de corruption déclarés – des fraudes qui peuvent s'avérer particulièrement coûteuses pour les organisations qui en sont victimes, en raison des amendes découlant des infractions à la réglementation, des frais juridiques et des coûts liés aux mesures correctives.

**Figure 3 : Pertes financières**

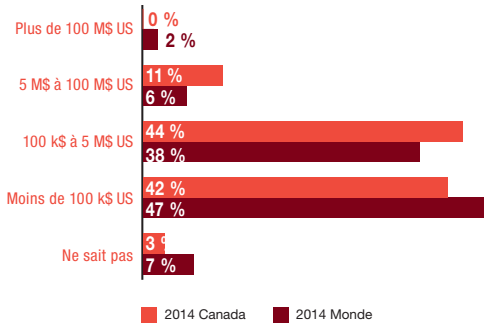
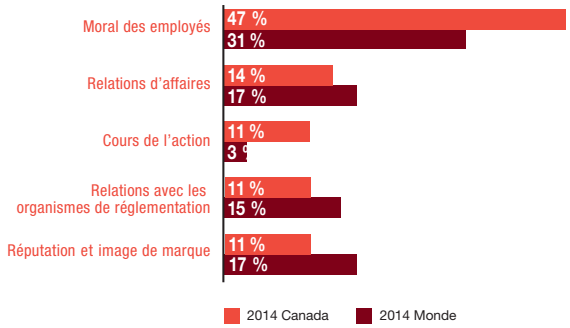



**Figure 4 : Dommages indirects – une incidence notable sur les activités commerciales**




## Les dommages indirects : difficiles à évaluer, difficles à ignorer

Les pertes économiques ne sont pas les seuls problèmes auxquels les organisations sont confrontées dans leur combat contre la fraude. Les répondants canadiens ont indiqué que les préjudices non financiers les plus graves entraînés par la fraude sont, entre autres, les dommages indirects causés au moral des employés (47 %), les incidences négatives sur les relations d'affaires (14 %) ainsi que sur la réputation et l'image de marque (11 %). La figure 4 donne des détails additionnels sur les dommages indirects importants déclarés pas les organisations.

Lorsqu'on prend en considération les dommages indirects, le coût réel d'une fraude peut avoir des conséquences à long terme. Il est certes difficile d'attribuer une valeur purement financière aux dommages, mais une chose est claire : si une fraude affecte l'embauche, la rétention des employés, les relations d'affaires et la réputation, elle aura des effets sur l'état des résultats – même si elle n'y est pas présentée comme une « fraude ». Les employés d'aujourd'hui sont très motivés par des facteurs non financiers, comme l'atmosphère de travail d'équipe et la certitude que l'organisation qui les emploie est une organisation où il fait bon travailler. L'attention négative des médias ou la perception que l'activité criminelle est tolérée peuvent altérer le moral des employés ou leur perception de leur employeur.

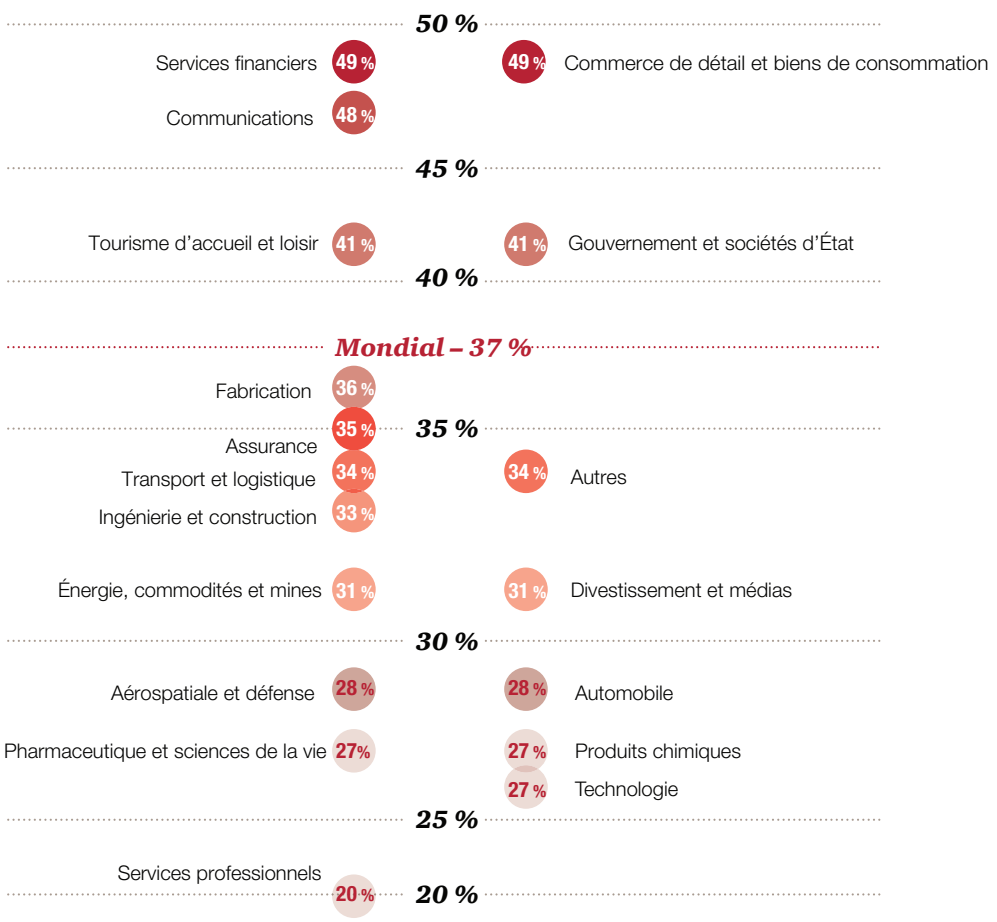
Dans une proportion de 11 %, les répondants canadiens ont estimé que la réputation et l'image de marque de leur organisation avaient été ternies considérablement par suite d'un crime économique. Toutefois, comme ces éléments sont souvent étroitement associés à l'avantage concurrentiel d'une organisation et que plusieurs années sont souvent nécessaires pour les rétablir, il est important de ne pas sous-estimer les répercussions des dommages indirects.

## L'analyse des crimes économiques selon les industries

À l'échelle mondiale, trois industries sont davantage frappées par les crimes économiques : les services financiers, le commerce de détail et les biens de consommation, ainsi que les communications. Dans les services financiers, les cas relativement nombreux de cybercriminalité et de blanchiment d'argent font monter les niveaux de fraude. Sans surprise, les cas de détournement d'actifs sont relativement importants dans l'industrie du commerce de détail et des biens de consommation. Il en est de même dans l'insdustrie des communications.

La figure 5 présente les résultats obtenus par industrie, à l'échelle mondiale.

**Figure 5 : Types de crimes économiques déclarés par industrie**




*% des répondants qui ont été victimes d'un crime économique au cours de la période visée par le sondage*

Comme le démontre la figure 5, nous avons constaté une forte concentration d'industries où les organisations ont signalé des fraudes dans une proportion de 27 % à 36 %. Bien que ces pourcentages soient inférieurs à la moyenne mondiale de 37 %, nombre de ces industries – en particulier celles de l'énergie, des commodités et des mines, de l'ingénierie et de la construction ainsi que du transport et de la logistique – sont plus exposées aux crimes économiques tels que le trafic d'influence et la corruption ou la fraude liée à l'approvisionnement.

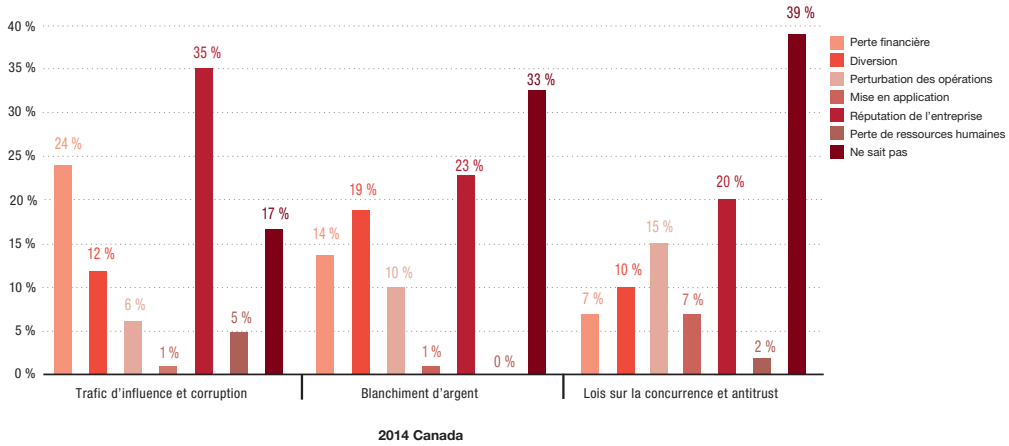
# *Pleins feux sur le trafic d'influence et la corruption, le blanchiment d'argent et les lois sur la concurrence et antitrust*

Certaines formes de crimes économiques peuvent entraîner beaucoup plus de risques que d'autres; c'est le cas du trafic d'influence et de la corruption, du blanchiment d'argent et des comportements anticoncurrentiels. Ces trois crimes sont sanctionnés par les pouvoirs publics et visés par des normes de plus en plus rigoureuses, de mieux en mieux appliquées et des peines de plus en plus sévères. Dans un monde interdépendant, ces crimes représentent des dangers particuliers pour les organisations multinationales.

Si le détournement d'actifs peut s'apparenter à un vol à la tire ou à un cambriolage, une violation grave d'une loi anticorruption comme la Loi sur la corruption d'agents publics étrangers (« LCAPE ») au Canada ou la Foreign Corrupt Practices Act (« FCPA ») aux États-Unis – qui peut donner lieu à de fortes amendes et grandement affecter une organisation – s'apparente à une agression systémique contre l'organisation.

Outre qu'elles donnent lieu à des amendes élevées et même à des poursuites criminelles, ces violations peuvent être considérées comme un problème organisationnel plus vaste et avoir des répercussions très négatives – allant de l'atteinte à la réputation aux pertes financières, en passant par une perturbation coûteuse des opérations et la perte de compétences inestimables au sein du personnel.

**Figure 6 : Incidences sur les organisations du trafic d'influence et de la corruption, du blanchiment d'argent et des lois sur la concurrence et antitrust**



En ce qui concerne la corruption et le trafic d'influence, le blanchiment d'argent et les lois sur la concurrence et antitrust, les répondants canadiens considèrent que l'atteinte à la réputation de l'organisation est la répercussion la plus grave (respectivement 35 %, 23 % et 20 % de ces répondants – figure 6). Les autres répercussions déclarées par les répondants canadiens sont discutées ci-dessous, et ce, de manière disctincte pour chacun de ces trois types de crimes économiques :

- **Le trafic d'influence et la corruption :** les pertes financières se classent en deuxième position avec 24 % des voix des répondants canadiens, suivies de la diversion causée par les mesures d'application de la loi et de la réglementation (12 %), de la perturbation des opérations (6 %), de la perte de ressources humaines (5 %) et de la mise en application de politiques, de procédures et d'outils de conformité (1 %).
- **Le blanchiment d'argent :** la diversion causée par les mesures d'application de la loi et de la réglementation se classe en deuxième position avec 19 % des voix des répondants canadiens, suivie des pertes financières (14 %), de la perturbation des opérations (10 %) et de la mise en application de politiques, de procédures et d'outils de conformité (1 %).
- **Les lois sur la concurrence et antitrust :** la perturbation des opérations se classe en deuxième position avec 15 % des voix des répondants canadiens, suivie de la diversion causée par les mesures d'application de la loi et de la réglementation (10 %), des pertes financières et de la mise en application de politiques, de procédures et d'outils de conformité (chacune avec 7 % des réponses) et de la perte de ressources humaines (2 %).

## La quantification des pertes

Il est important de prendre la mesure du coût financier associé au trafic d'influence et à la corruption, au blanchiment d'argent et aux comportements anticoncurrentiels. Comme nous l'avons mentionné précédemment dans ce rapport, ces types de crimes économiques ne sont pas les plus fréquents (figure 2). Néanmoins, les résultats de notre sondage démontrent que leur coût peut être considérable. Plus précisément :

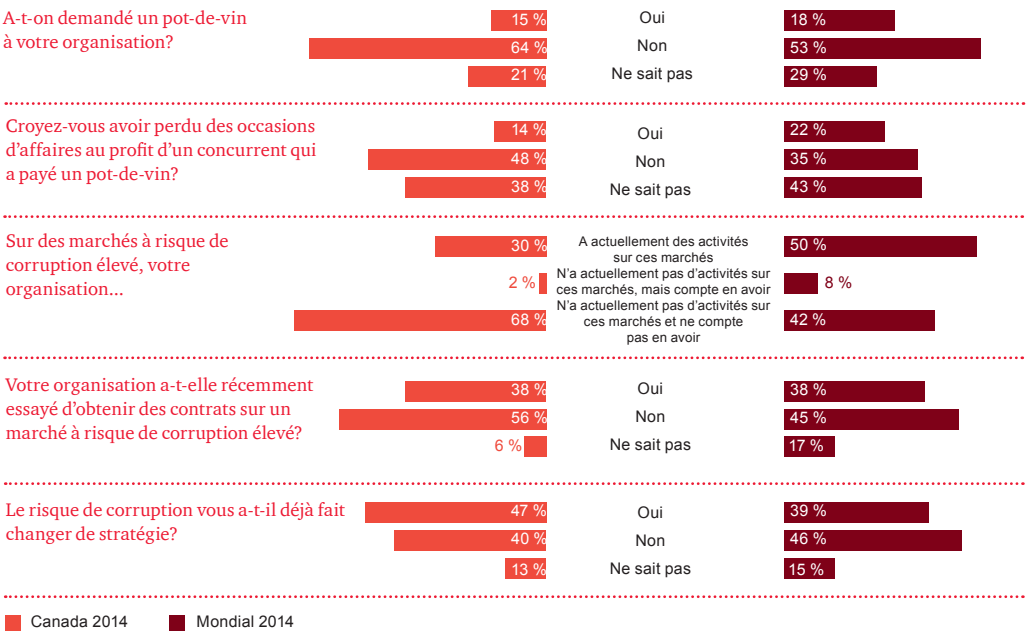
- **Le trafic d'influence et la corruption :** 13 % des répondants canadiens ont déclaré des pertes supérieures à 100 000 $ US et 4 % d'entre eux, des pertes oscillant entre 5 millions $ US et 100 millions $ US;
- **Le blanchiment d'argent :** 4 % des répondants Canadiens ont fait état de pertes comprises entre 100 000 $ US et 1 million $ US;
- **Les lois sur la concurrence et antitrust :** 4 % des répondants ont fait état de pertes de plus de 100 000 $ US et 1 %, de pertes comprises entre 5 millions $ US et 100 millions $ US.

Lorsque nous leur avons demandé de classer les risques de trafic d'influence et de corruption, de blanchiment d'argent et d'infractions aux lois sur la concurrence et antitrust associés aux affaires conduites à l'échelle mondiale, la majorité des répondants canadiens (60 %) a jugé que le trafic d'influence et la corruption sont les éléments qui présentent le niveau de risque le plus élevé.

# *Un gros plan sur le trafic d'influence et la corruption*

Chaque région du monde a déclaré un nombre élevé de cas de trafic d'influence et de corruption. Même si le Canada ne figure pas parmi les pays ayant déclaré les plus hauts taux de corruption, plusieurs données intéressantes méritent d'être signalées. La figure 7 présente ces données.

**Figure 7 : Trafic d'influence et corruption – leurs incidences sur l'organisation**



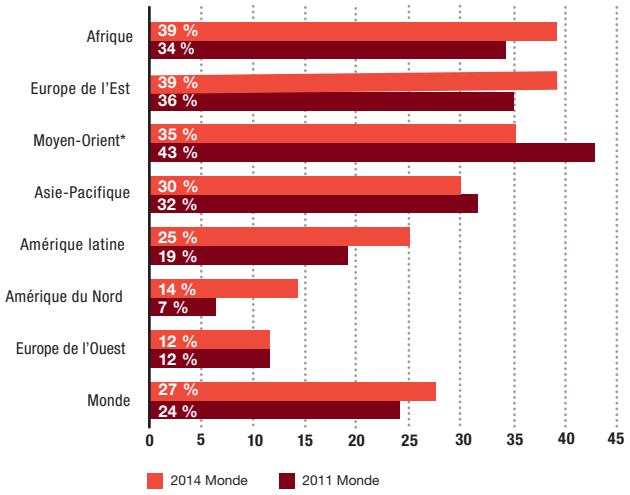

La figure 7 démontre que globalement, les répondants canadiens ont signalé moins de demandes de pots-de-vin (15 %) que les répondants à l'échelle mondiale (18 %). Elle démontre également que 14 % des répondants canadiens estiment avoir perdu une occasion d'affaires au profit d'un concurrent qui a payé un pot-de-vin.

Les résultats de notre sondage révèlent également que 50 % des organisations multinationales estiment évoluer sur des marchés affichant un risque élevé de corruption, alors que ce pourcentage tombe à 30 % pour les organisations canadiennes. Cet écart important suggère que les organisations canadiennes pourraient ne pas être préparées ou avoir suffisamment confiance dans leurs procédures et contrôles anticorruption pour faire affaires sur des marchés à risque élevé. En ayant évité les marchés à risque élevé plus souvent que les organisations multinationales, les organisations canadiennes pourraient avoir perdu des occasions de générer des revenus sur des marchés où il est possible d'atténuer le risque de fraude en appliquant un programme de gestion des risques de fraude approprié.

Pendant le sondage, 38 % des répondants canadiens ont mentionné qu'une occasion d'affaires s'était récemment présentée pour leur organisation sur un marché caractérisé par un risque élevé de corruption. Parmi ces répondants, 47 % ont modifié leur plan d'affaires du fait d'un risque de corruption et 40 % ne l'ont pas fait. Les 13 % restants ignoraient s'ils l'avaient fait ou non, ce qui est préoccupant étant donné les conséquences de la corruption précédemment discutées dans ce rapport. Ces statistiques devraient inciter les membres de la direction et des conseils d'administration à dresser un programme de gestion des risques de fraude, surtout quand l'organisation s'aventure sur un marché très risqué. Cela dit, parmi les 47 % des répondants qui ont modifié leur plan d'affaires, 78 %, ont indiqué avoir mis en œuvre des contrôles diligents supplémentaires. La stratégie ayant recueilli le plus d'appui en deuxième lieu (33 %) consistait à se retirer purement et simplement du marché, ce qui, ici aussi, pourrait s'être traduit par la perte d'une occasion d'affaires et des revenus correspondants.

Nous croyons que l'une des raisons du nombre élevé de cas de trafic d'influence ou de corruption qui ont été rapportés pourrait être la tendance générale au transfert de richesse des pays développés d'Occident vers les pays émergents en expansion rapide du Sud et de l'Est. La figure 8 présente les cas de trafic d'influence et de corruption déclarés par les répondants à l'échelle mondiale, et ce, par région.

**Figure 8 : Trafic d'influence et corruption déclarés par région**




* Le Moyent-Orient était inclus dans la région Asie-Pacifique en 2011.

Comme le révèle la figure 8, davantage de cas de trafic d'influence et de corruption ont été déclarés dans les régions comme l'Afrique, l'Europe de l'Est et le Moyen-Orient. Bon nombre de ces pays ou régions pourraient avoir une attitude culturelle différente face à la fraude et à la corruption, être moins réglementés et soumis à une application de la réglementation plus aléatoire, ce qui hausse le profil de risque de ce type de crimes économiques. Si d'autres régions comme l'Amérique du Nord (14 %) et l'Europe de l'Ouest (12 %) se situent dans le bas de l'échelle pour les cas déclarés de trafic d'influence et de corruption, cela est grandement attribuable à l'influence des mesures d'application de la loi déployées par leur gouvernement respectif.

Comme les cas de trafic d'influence et de corruption font souvent l'objet de poursuites par les autorités au-delà des frontières, les organisations doivent être conscientes des risques importants que comportent les activités exercées dans les régions en expansion rapide, même si les pratiques et les coutumes de ces régions sont plus laxistes.

## Le trafic d'influence et la corruption – l'atténuation des risques

Peu importe votre industrie ou les régions où votre organisation exerce ses activités, il existe des moyens de diminuer le risque de trafic d'influence et de corruption. Voici les quatre sphères que nous proposons de cibler en priorité :

1) **La direction doit donner l'exemple.** Bien que le respect des lois soit l'affaire de tous, l'exemple doit venir d'en haut, ce qui suppose une bonne compréhension des lois anticorruption, un message clair et cohérent affirmant que le trafic d'influence et la corruption ne sont pas tolérés et l'affectation de ressources suffisantes pour lutter contre ces menaces.

2) **L'évaluation des risques.** L'organisation et son environnement de conformité étant en évolution constante, il est essentiel de faire des évaluations périodiques des risques et de s'assurer que les risques identifiés antérieurement ont été mitigés.

3) **L'environnement de contrôle.** Pour lutter efficacement contre les risques de corruption, il faut un plan de communication solide et des procédures internes vigilantes de mise en application. Il faut donc non seulement prévoir un code de conduite écrit et former le personnel en conséquence (notamment sur des questions de conformité délicates comme les cadeaux et les divertissements), mais aussi un système de contrôles pour surveiller les transactions douteuses. Finalement, il faut se rappeler que le degré de conformité d'une organisation se mesure par rapport à son maillon le plus faible. Les partenaires commerciaux, les fournisseurs et les autres tiers doivent aussi être contrôlés et surveillés afin de bien gérer le risque de faire des affaires dans des pays plus exposés à la corruption.

4) **L'évaluation de l'efficacité.** Les programmes d'évaluation des risques et des contrôles ne suffisent pas à assurer le respect de la loi. Il faut également des contrôles diligents, des visites périodiques par la direction des lieux à risque élevé, des rapports de conformité adressés au conseil d'administration, un suivi sur la ligne de dénonciation, un suivi sur les cas potentiels de fraude et de corruption signalés et des audits des partenaires commerciaux. De plus, tous ces éléments doivent être réévalués régulièrement dans le cadre d'un programme interne de conformité.

*En ayant évité les marchés à risque élevé plus souvent que les organisations multinationales, les organisations canadiennes pourraient avoir perdu des occasions de générer des revenus sur des marchés où il est possible d'atténuer le risque de fraude en appliquant un programme de gestion des risques de fraude approprié.*

# *Notre monde est un vaste réseau*
## Les avantages et les risques ne sont pas prêts de disparaître

*La cybercriminalité, aussi appelée crime informatique, est un crime économique commis à l'aide d'un ordinateur et d'Internet.*
*Ce genre de crime comprend la transmission de virus, le téléchargement illégal de contenus, l'hameçonnage et le détournement de domaine ainsi que le vol de renseignements personnels tels que des renseignements sur les comptes bancaires. Cette définition ne comprend pas les types courants de fraudes dans lesquelles un ordinateur est utilisé comme accessoire pour frauder. Elle n'inclut que les crimes économiques dans lesquels un ordinateur, Internet et d'autres appareils électroniques jouent un rôle de premier plan et non accessoire dans la perpétration du crime.*

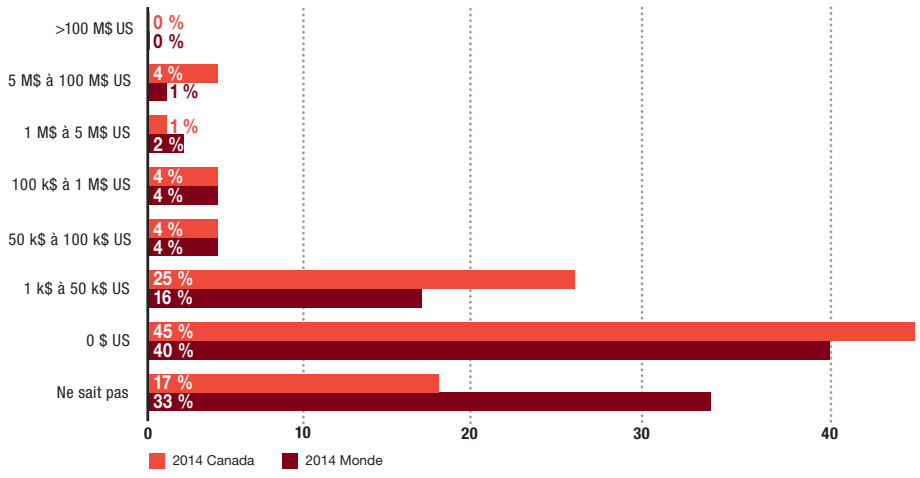
Selon notre sondage de 2014, la cybercriminalité continue de se classer parmi les principaux crimes économiques, derrière le détournement d'actifs et la fraude liée à l'approvisionnement (figure 2). L'avancée de la technologie dans les organisations, l'essor spectaculaire des médias sociaux et la dépendance des organisations à la connectivité ont contribué à la prolifération de la cybercriminalité dans notre société.

La connectivité et la facilité d'accès ont leur côté sombre – cela permet à des criminels décidés, qui maîtrisent parfaitement les technologies, de perpétrer leurs méfaits à l'insu de leurs victimes. Comme ces criminels agissent dans l'ombre, il peut arriver que des organisations ne s'aperçoivent qu'elles ont été attaquées que longtemps après que le mal a été fait. C'est pour cela que la fraude électronique est un des crimes économiques les plus dangereux.

### Le coût que vous pouvez évaluer

Notre sondage de 2011 avait été le premier de notre série à révéler que la cybercriminalité était une très grave menace pour les organisations. Le sondage de cette année confirme l'impact important et constant de ce genre de crimes sur les organisations; près de un répondant sur quatre a rapporté que son organisation a été victime de la cybercriminalité (figure 2) – et plus de 5 % d'entre eux ont rapporté des pertes financières de plus de 1 million $ US (figure 9).

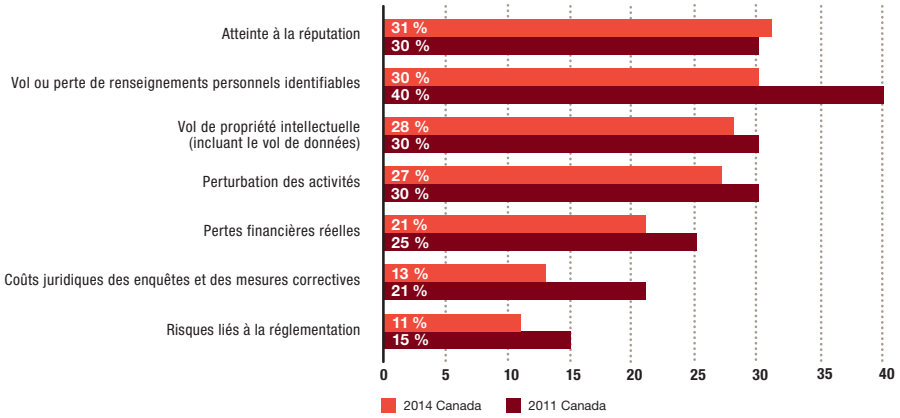
**Figure 9 : Cybercriminalité : pertes estimées**



## Le coût qui fait peur aux organisations

Les résultats de notre sondage confirment les répercussions financières évidentes de la cybercriminalité. Toutefois, comme l'illustre la figure 10, les plus grandes craintes des répondants canadiens à l'égard de la cybercriminalité sont l'atteinte à la réputation (31 %) et les conséquences que pourraient avoir le vol ou la perte de renseignements personnels identifiables (30 %). Ils considèrent les coûts potentiels associés à ces risques plus dangereux que les pertes financières qu'ils pourraient subir en raison de la cybercriminalité (21 %).

**Figure 10 : Coût qui préoccupe les organisations**

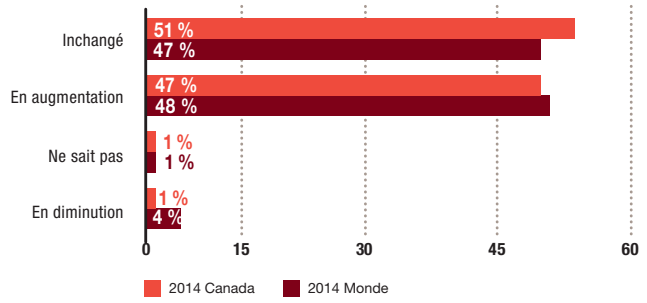



Les résultats de notre sondage soulignent que les organisations sont conscientes que les conséquences indirectes de la cybercriminalité leur font courir un risque beaucoup plus important que les pertes financières associées à ce type de fraude. Par exemple, une attaque lancée sur un réseau de jeux vidéo, qui cause une fuite de renseignements personnels peut éroder la confiance des clients, provoquer des interruptions de service et faire baisser le nombre d'utilisateurs. Tout cela peut causer un préjudice financier à l'organisation. Il est important de souligner que même s'il est parfois impossible d'évaluer sur le champ les conséquences financières de la cybercriminalité, cela n'en diminue pas nécessairement la gravité. Il est rare qu'une attaque n'ait qu'une seule conséquence; les implications peuvent être beaucoup plus graves dans le futur.

## La perception de l'avenir de la cybercriminalité

Il ressort de notre sondage que les organisations continuent de prendre la menace de la cybercriminalité très au sérieux puisque 47 % des répondants canadiens estiment que leur perception du risque associé à ce type de crime économique s'est accrue au cours de la période visée par le sondage. Seulement 1 % de ces mêmes répondants ont indiqué que leur perception de ce risque avait diminué. Globalement, les résultats de notre sondage détaillés dans la figure 11, illustrent la crainte croissante des organisations à l'égard de la cybercriminalité au Canada et ailleurs dans le monde, et la nécessité de demeurer à l'affût des menaces qui font leur apparition ou

**Figure 11 : Perception des risques associés à la cybercriminalité**



sont en émergence.

## L'ignorance peut coûter cher

Qu'environ un quart des répondants déclarent que leur organisation a été victime de la cybercriminalité est assez inquiétant, mais il faut savoir qu'un pourcentage important d'organisations en ont peut-être été victimes à l'insu de leur répondant. La situation est donc très alarmante.

Le tableau se complique encore, car il arrive souvent que des organisations décident de ne pas déclarer les cas de cybercriminalité qu'elles ont détectés. À part les violations touchant certains domaines réglementés, comme le vol d'identité, peu de dispositions réglementaires exigent que ces crimes soient déclarés. Il peut y avoir des raisons impérieuses, liées à la concurrence – dans le cas, par exemple, d'un vol de propriété intellectuelle important – de garder le silence sur de telles pertes pour éviter les embarras publics ou les critiques.

Supposons qu'un document confidentiel sur la planification d'une offre de service soit volé par des cybercriminels et utilisé par un rival pour remporter cette offre, l'organisation propriétaire du document va-t-elle déclarer ce vol? Les organisations se protègent-elles bien contre de tels crimes et si un crime est découvert, comment en évaluer la perte?

En résumé, la plus grande partie des dommages causés par ce genre d'attaques n'est pas révélée, parce qu'elles ne sont pas détectées, parce que les pertes sont difficiles à évaluer ou parce que les victimes n'en parlent pas. Il est évident que ce genre de flou opérationnel fait courir des risques aux organisations qui dépendent de plus en plus de la technologie et de la propriété intellectuelle, et ce, dans un environnement qui valorise la transparence.

Un environnement dans lequel il est plus facile de voler un actif incorporel vital que d'estimer la valeur, de déclarer ou même de détecter une perte est un environnement dangereux.

## L'intégrité des données est menacée

Les données recueillies et conservées par de nombreuses organisations contiennent souvent des renseignements privés, ce qui donne aux criminels la possibilité de voler des données qu'ils peuvent utiliser à toutes sortes de fins; par exemple, pour accéder à des comptes financiers et voler de l'argent.

Les organisations d'aujourd'hui dépendent largement de la technologie et de la connectivité informatiques ce qui amplifie les conséquences des cyberattaques qui affectent la propriété intellectuelle, l'avantage concurrentiel, la stabilité opérationnelle, la conformité à la réglementation et la réputation, sans compter l'intégrité des données. Les données, en tant qu'actif, n'ont pas toutes la même valeur et elles continuent de croître à un rythme extraordinaire. Assurer le plus haut degré de protection à toutes les données n'est ni réaliste ni possible. La perte de certains types de données peut être simplement gênante, alors que la perte d'autres peut détruire des pans entiers d'une organisation.

Vos données sensibles circulent et sont utilisées probablement dans tout l'écosystème de vos affaires, ce qui étend considérablement le domaine à surveiller et à protéger. Aujourd'hui, l'intégrité et la stabilité de votre organisation dépendent plus que jamais de ceux qui ont accès à votre réseau de données.

Une conséquence involontaire de l'accès universel à la technologie dans les organisations a été de créer des vulnérabilités qui sont exploitées par les ennemis – ce qui accroît fortement le degré d'exposition des organisations et les incidences négatives possibles. Parmi les exemples, citons le vol d'informations de recherche et de développement, la reproduction rapide de produits ou de procédés, l'accès à des renseignements stratégiques ou sur les clients et la perturbation de la stabilité opérationnelle. Ces adversités minent la rentabilité à long terme et l'avantage concurrentiel de l'organisation.

Les dirigeants et les conseils d'administration des organisations ne peuvent plus se contenter de considérer les cyberattaques comme un problème de technologie; celles-ci concernent aujourd'hui l'organisation dans son ensemble. Cela doit commencer en haut de l'échelle : les hauts dirigeants doivent intégrer la cybercriminalité dans leur programme d'activités et évaluer leur tolérance face à ce risque.

## La cybercriminalité est un problème humain, pas un problème technologique

Même parmi les organisations généralement conscientes des différents types de menaces informatiques dont elles pourraient être victimes, beaucoup ne comprennent pas très bien les capacités des criminels, les cibles qu'ils peuvent viser et la valeur que peuvent avoir ces cibles. Les organisations cherchent à mettre des données critiques à la disposition de la direction, des employés, des fournisseurs et des clients sur toutes sortes de plates-formes – y compris sur les plates-formes à risque élevé comme les téléphones portables ou l'informatique en nuage – parce que les avantages économiques et concurrentiels semblent si intéressants.

Il est intuitivement facile de comprendre les avantages de la disponibilité des données, et personne ne s'attend à ce que les organisations réduisent leurs volumes de données numériques. Cependant, alors qu'une quantité grandissante de données est accessible sur un nombre sans cesse croissant de plates-formes, il est évident que les données les plus importantes continueront d'être attaquées, et que le coût des atteintes à la sécurité augmentera.

Aujourd'hui, le réseau est le centre nerveux du monde des affaires et il est en constante évolution. Les adversaires sophistiqués en profitent pour s'attaquer à toutes les nouvelles faiblesses. Les organisations doivent donc se maintenir au niveau des forces qui les menacent. En définitive, la cybercriminalité n'est pas un problème technologique; c'est un problème humain qui concerne la stratégie et les processus.

## Les mesures de protection contre les cyberattaques

- **Mobiliser le chef de la direction** – le chef de la direction et le conseil d'administration doivent être sensibilisés aux menaces informatiques et comprendre les risques et les possibilités du cyberespace.
- **Réévaluer** – réévaluer la fonction sécurité et l'état de préparation de l'organisation en cas de crime informatique. Contrairement aux crimes économiques traditionnels, les crimes informatiques évoluent rapidement en raison des avancées technologiques entraînant constamment de nouveaux risques, ce qui contraint l'organisation à adapter continuellement ses procédures.
- **Sensibiliser** – les organisations doivent bien connaître le monde informatique actuel et en émergence. Ainsi, elles pourront prendre des décisions et des mesures éclairées en fonction de leurs priorités.
- **Créer une équipe d'intervention en cas de cyberincidents** – une équipe d'intervention rapide et efficace s'assure, dès le signalement d'un incident n'importe où dans l'organisation, que celui-ci fait l'objet d'un suivi, qu'il est évalué en fonction des risques et que les dirigeants de l'organisation en sont informés.
- **Former tous les employés** – toute organisation doit implanter une culture de « cybersensibilisation » et communiquer à l'ensemble du personnel les politiques, les procédures et les protocoles appropriés.
- **Les organisations doivent adopter une approche plus active et transparente à l'égard de la cybercriminalité** – prendre des mesures en poursuivant les auteurs de crimes informatiques au moyen de poursuites judiciaires et communiquer publiquement les mesures prises par l'organisation contre les menaces et les incidents.

# *La fraude liée à l'approvisionnement*
## Plus la tentation est grande, plus la menace s'accroît

Comme nous l'avons mentionné précédemment, cette année nous avons ajouté la fraude liée à l'approvisionnement – une conduite illégale d'un employé, d'un propriétaire, d'un fournisseur ou d'un dirigeant relativement à l'achat de services, de marchandises ou de biens pour le compte d'une organisation, souvent pour son enrichissement personnel – comme nouvelle catégorie de crimes économiques dans notre sondage.

De façon générale, lorsqu'une organisation s'adresse à un tiers pour se procurer des services, des marchandises ou des biens, il y a risque de fraude liée à l'approvisionnement. Il nous est apparu que deux facteurs seraient à l'origine de cette catégorie de crimes.

Premièrement, comme le soulignait récemment notre « Enquête mondiale 2014 menée auprès des chefs de direction », nous assistons à une interdépendance accrue des entités commerciales – par l'externalisation d'éléments de la chaîne de valeur, l'achat de matières et une dépendance accrue à l'égard de fournisseurs.

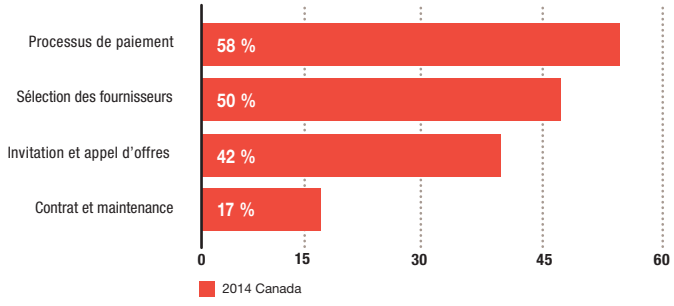
Deuxièmement, depuis que les économies nationales se sont relevées de la crise économique récente, les pratiques d'embauche semblent avoir changé. En effet, les mesures à court terme prises post-crise, comme le remplacement d'un personnel permanent occupant des postes internes par des ressources externes plus malléables et adaptables sont restées en place dans bien des cas, les organisations étant plus enclines à externaliser certaines tâches. Ces changements dans les pratiques d'embauche exposent les organisations à des problèmes de séparation des tâches dans le processus d'approvisionnement.

Le niveau élevé de cas de fraude lié à l'approvisionnement signalés – 33 %, catégorie dépassée uniquement par le détournement de biens (figure 2) – a surpassé nos prévisions. Cela pourrait s'expliquer en partie par le lien entre la fraude liée à l'approvisionnement et le trafic d'influence et la corruption. Dans nos sondages précédents, les commissions secrètes, les trucages d'offres et autres agissements similaires étaient peut-être englobés dans la catégorie trafic d'influence et corruption. Il n'empêche que ce deuxième rang mérite d'être souligné.

### La nature des fraudes liées à l'approvisionnement

La figure 12 montre que les répondants canadiens ont indiqué que la fraude liée à l'approvisionnement se produit essentiellement au cours du processus de paiement (58 %), de la sélection des fournisseurs (50 %) et de l'appel d'offres (42 %).

**Figure 12 : La fraude liée à l'approvisionnement – zones à risque**



*En adoptant quelques stratégies, les organisations pourraient non seulement réduire la fraude liée à l'approvisionnement, mais aussi simplifier leur processus d'appel d'offres et de sélection des fournisseurs.*

## Le processus d'achat et d'approvisionnement sous attaques

Comme il a été mentionné, les appels d'offres et la sélection des fournisseurs constituent un terrain de prédilection pour la fraude. Une personne du service des achats ou de l'approvisionnement peut être de connivence avec un fournisseur qui souhaite décrocher un contrat auprès de l'organisation. L'initié communique des informations sur le processus d'appel d'offres, comme les montants avancés par les concurrents, afin d'avantager le soumissionnaire qu'il privilégie. À l'inverse, l'initié peut approuver un prix inutilement élevé.

La facilité avec laquelle le processus d'achat et d'approvisionnement peut être attaqué est illustrée par le processus d'approvisionnement du secteur public. Ce secteur peut être amené à faire d'importants achats de matériel de pointe sur une longue période et devoir s'adresser à un marché où il existe un nombre limité de fournisseurs ayant la taille voulue pour soumissionner. En matière de services, les organisations du secteur public sollicitent régulièrement des soumissions portant sur une foule de responsabilités de moindre importance comme l'entretien du matériel, les services de logement et de restauration ou le soutien logistique.

Dans des environnements non soumis à la concurrence et souvent opaques, ces soumissions sont fréquemment l'occasion de fraude liée à l'approvisionnement. Nous avons assisté à plusieurs scandales retentissants dans de tels environnements au cours des dernières années et nous nous attendons à en voir davantage dans les années à venir.

## La riposte

Il est pour le moins paradoxal qu'au moment où des politiques de lutte contre le trafic d'influence et la corruption sont mises en œuvre dans bien des organisations – souvent du fait de la pression exercée par la haute direction, attentive aux lois anticorruption publicisées comme la LCAPE –, il existe beaucoup moins de programmes de formation sur la prévention de la fraude liée à l'approvisionnement, qui y est étroitement associée.

Et pourtant, la formation sur la prévention de la fraude liée à l'approvisionnement est sans doute beaucoup moins complexe et coûteuse, les facteurs de risque étant plus simples et plus faciles à cerner.

En adoptant quelques-unes des stratégies suivantes, les organisations pourraient non seulement réduire la fraude liée à l'approvisionnement, mais aussi simplifier leur processus d'appel d'offres et de sélection des fournisseurs :

- S'assurer que l'organisation demande des soumissions cachetées qui seront ouvertes devant un groupe de personnes. Cette façon de procéder assure un meilleur contrôle sur l'intégrité des soumissions et du processus d'appel d'offres;
- Instaurer une séparation des fonctions au sein des services des achats et de l'approvisionnement pour s'assurer que plusieurs personnes participent au processus;
- Envisager de faire appel à différents fournisseurs pour différents projets. Par exemple, le fait de soumettre régulièrement les fournisseurs à un examen ou à un appel d'offres leur indique qu'ils devront se mesurer aux prix du marché. En outre, le donneur d'ouvrage prend ainsi connaissance des prix et des services qu'on trouve sur le marché.

# *La fraude comptable*
## Une menace qui persiste

La fraude comptable a toujours été l'un des crimes économiques les plus fréquemment signalés dans notre sondage. Depuis 2005, ce crime est signalé par plus de 20 % des répondants à l'échelle mondiale qui ont été victimes d'un crime économique.

Cette année n'a pas fait exception. Du côté canadien, 22 % (figure 2) des répondants ont déclaré avoir été victimes d'une fraude comptable, tout comme les 22 % (figure 2) recensés à l'échelle mondiale.

Les états financiers représentent un baromètre fondamental de la situation financière de l'organisation, et le point de départ traditionnel des analyses sur lesquelles s'appuient les décisions de crédit, les attributions de contrats et la mobilisation de capitaux sur les marchés publics. La fraude comptable – notamment la préparation d'états financiers trompeurs ou altérés – peut mener des banques, des prêteurs, des fournisseurs et des investisseurs à prendre des décisions risquées et mal fondées. En raison de l'utilisation systématique des états financiers et des données financières dans le cadre des activités commerciales, ce type de crime économique a des répercussions sur de nombreux processus d'affaires.

# *Le détournement d'actifs*
# Le plus répandu des crimes économiques

Le détournement d'actifs est de loin le crime économique le plus répandu, 58 % des organisations canadiennes répondantes qui ont signalé un cas de fraude en ayant été victimes (figure 2). Ce pourcentage est presque le double du taux de la fraude liée à l'approvisionnement, soit le deuxième crime économique en importance ayant été signalé. Bien que l'incidence de ce type de fraudes soit inférieure à celle de la cybercriminalité ou du trafic d'influence et de la corruption, l'ampleur de la menace est telle que les organisations doivent se montrer vigilantes.

## Des disparitions mystérieuses

Tout le monde a entendu parler de choses qui disparaissent mystérieusement. Cet euphémisme pour parler du détournement d'actifs met généralement en cause l'un des processus de gestion fondamentaux : la distribution, la logistique ou le stockage.

Prenons une organisation de vente au détail à l'échelle mondiale qui possède des entrepôts pour stocker sa marchandise. Cette marchandise passe non seulement entre les mains de membres du personnel, mais aussi de plusieurs organisations tierces, ce qui crée plusieurs points de vulnérabilité le long de la chaîne logistique et de la distribution. Le procédé malhonnête peut se résumer au fait pour un employé de quitter le travail en emportant avec lui un article ou donner lieu à des agissements plus alambiqués comme classer au rebut de la marchandise en parfait état pour ensuite la revendre.

Le détournement d'actifs comprend aussi le vol d'argent par suite d'un détournement de fonds, souvent entre les mains d'une autorité chargée de garder des sommes d'argent en dépôt. Un exemple des nombreux stratagèmes associés au détournement d'actifs est le report différé dans les comptes de clients (« lapping »). Cette fraude consiste à voler de l'argent dans le compte d'un client et à combler le découvert avec de l'argent reçu d'un autre client. Les criminels ont de multiples façons de couvrir leurs crimes – comme de subtiliser de petites sommes afin de ne pas éveiller les soupçons.

## La lutte contre le détournement d'actifs

Comme ce type de fraudes se passe surtout dans les environnements où règne la confiance, le meilleur conseil qu'on puisse donner à une organisation est de mettre en place de saines procédures de gestion :

- **Connaître son employé** : procéder à des contrôles préalables à l'embauche et tenir compte des résultats.
- **Connaître son fournisseur** : tout comme les employeurs font des vérifications des antécédents des employés ayant accès à des actifs de valeur, l'organisation devrait procéder à des vérifications de ces fournisseurs éventuels.
- **Séparer les tâches** : s'assurer que plusieurs personnes participent à tout processus qui débouche sur la distribution de fonds ou de marchandises, ce qui complique la tâche du fraudeur, qui souhaite passer inaperçu.

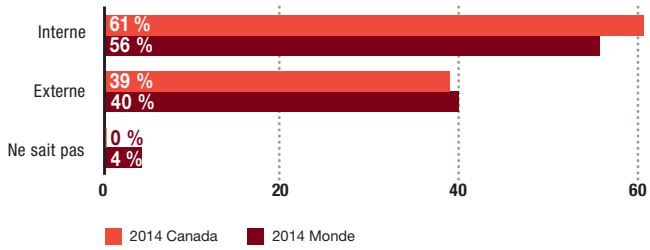
À la lecture de la présente liste de fraudes courantes et de risques auxquels les actifs d'une organisation sont exposés, il est important de se rappeler qu'un plan de gestion des risques de fraude bien conçu permet d'avoir recours à plusieurs contrôles pour prévenir différents types de fraudes. Ainsi, en instaurant par exemple des contrôles liés à la séparation des fonctions dans toute l'organisation, il serait possible de prévenir le détournement d'actifs en limitant les occasions pour les employés de quitter les lieux en emportant de la marchandise, tout en prévenant la fraude liée à l'approvisionnement par un processus d'appel d'offres scindé.

# *Interne ou externe*

## Qui commet la fraude? L'ennemi sous vos yeux

Dans la lutte contre le crime économique, comme dans tout combat, il est un besoin essentiel : connaître l'ennemi. Nous avons demandé aux répondants dont l'organisation a été victime d'un crime économique d'où provenaient les principaux auteurs des fraudes commises les plus graves. Comme le montre la figure 13, 61 % des répondants canadiens ont indiqué que le fraudeur provenait de l'intérieur de l'organisation, et 39 %, qu'il s'agissait de quelqu'un de l'extérieur.

**Figure 13 : D'où provenait le fraudeur?**




L'avantage, lorsque les pertes dues à la fraude sont majoritairement imputables à des personnes de l'intérieur – sur qui l'on peut théoriquement exercer une certaine surveillance – est que le renforcement des politiques, des processus et des contrôles internes peut réduire le risque. Ce n'est pas toujours le cas lorsque le fraudeur vient de l'extérieur.

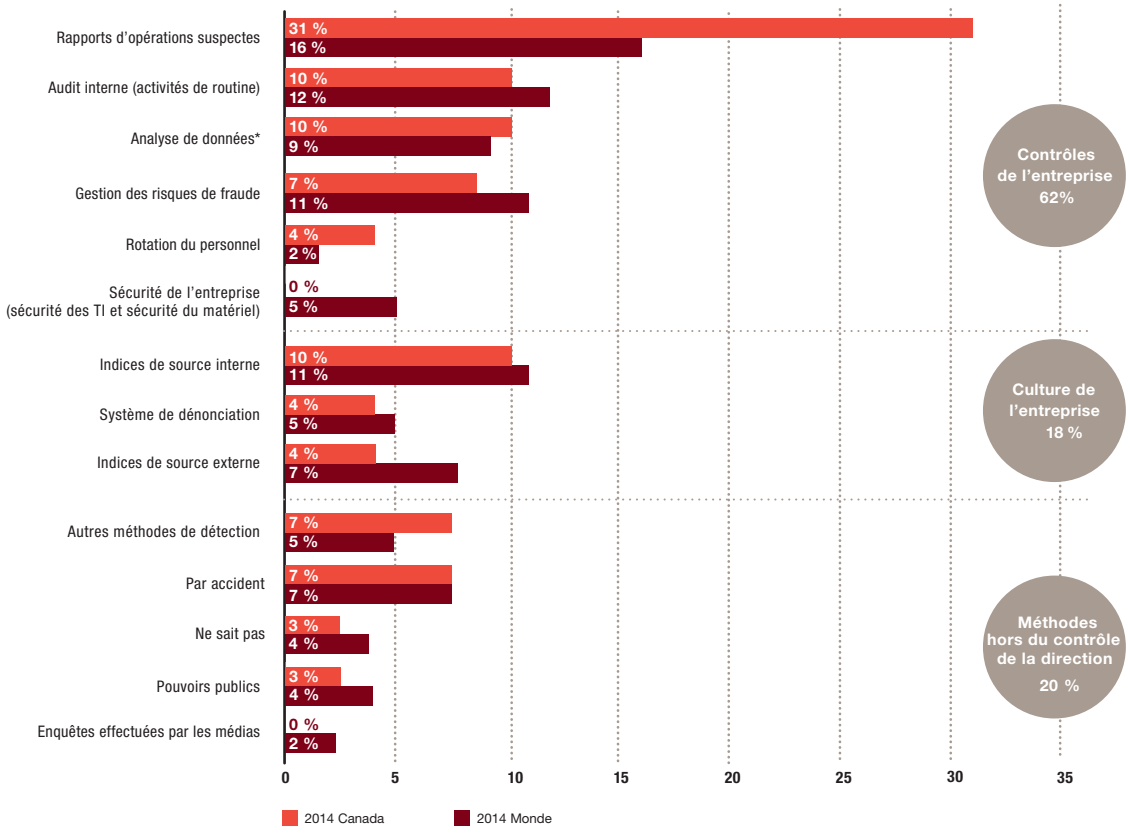
*Une proportion de 31 % des fraudes déclarées par les répondants canadiens ont été détectées grâce à des rapports d'opérations suspectes*

## Détecter la fraude

Comment empêcher un crime économique de survenir – ou, à tout le moins, intervenir pendant qu'il est perpétré?

Les méthodes de détection de la fraude se classent normalement dans l'une de ces trois catégories : les contrôles de l'organisation, la culture de l'organisation et les méthodes hors du contrôle de la direction. La figure 14 présente les méthodes grâce auxquelles les organisations sondées ont détecté des fraudes graves. Son contenu révèle, entre autres, qu'une proportion de 31 % des fraudes déclarées par les répondants canadiens ont été détectées grâce à des rapports d'opérations suspectes.

**Figure 14 : Méthodes de détection de la fraude**




*L'analyse de données a été ajoutée comme catégorie dans le sondage de 2014.

## Le fraudeur interne

Les spécialistes évoquent souvent le « triangle de la fraude » – ces trois éléments souvent réunis lorsqu'il y a acte frauduleux : la motivation, l'occasion et la rationalisation.

Près des trois quarts (73 %) des répondants canadiens ont indiqué que l'occasion ou la possibilité de commettre le crime était l'élément qui avait le plus contribué à la perpétration d'un crime économique par un acteur interne dans leur organisation. Si cela peut à première vue sembler décourageant, il faut savoir que, des trois éléments susmentionnés, l'occasion est celui sur lequel l'organisation a le plus de contrôle. Par conséquent, même si les employés peuvent subir des pressions diverses et trouver des motifs de commettre un méfait, si l'organisation limite les occasions qu'ils ont de passer à l'acte, elle pourrait réussir à empêcher l'engrenage frauduleux de se mettre en marche.

Même si la motivation et la rationalisation varient d'une fraude à l'autre, nous pouvons tout de même dresser un profil du fraudeur interne. Nous avons demandé aux répondants qui ont désigné un acteur interne comme le principal responsable d'un crime économique quels étaient le rang hiérarchique, l'âge, le sexe, l'ancienneté et le niveau d'études de celui-ci. Les figures 15 et 16 présentent les résultats.

**Figure 15 : Fraudeur interne (membre du personnel)**

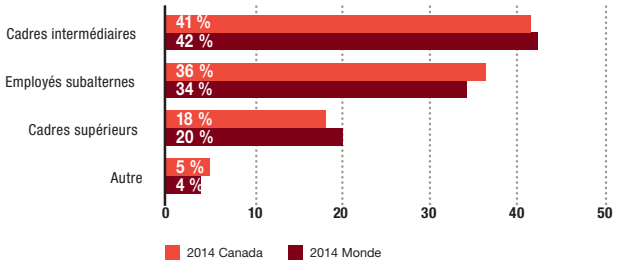
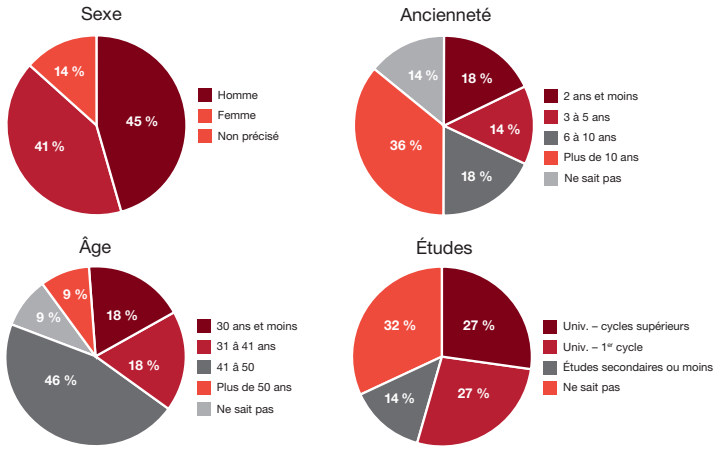



**Figure 16 : Profil du fraudeur interne**




2014 Canada

Les résultats canadiens de 2014 esquissent le profil du fraudeur interne : un homme (45 %) ou une femme (41 %) d'âge moyen qui a fait des études universitaires et qui travaillait dans l'organisation depuis plus de 10 ans occupant, le plus souvent, un poste de cadre intermédiaire.

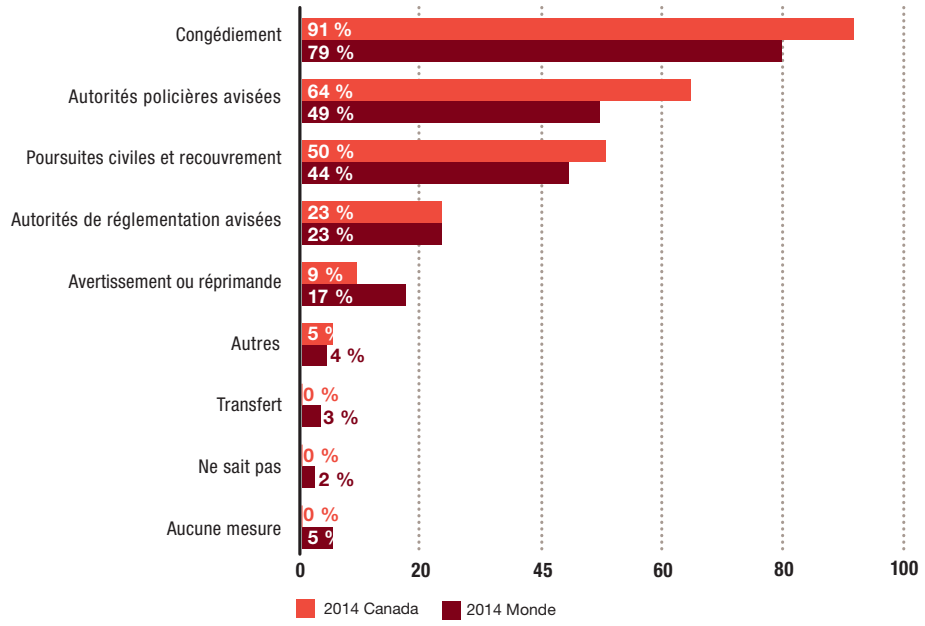
Il importe de noter que les fraudeurs internes tendent à avoir une longue ancienneté et à commettre des crimes complexes. Même si les résultats canadiens montrent que les cadres supérieurs (18 % – figure 15) commettent moins de crimes économiques que les employés subalternes (36 % – figure 15), ces crimes ont tendance à être plus complexes et à impliquer des montants plus élevés. Par ailleurs, le fait que les fraudes complexes soient plus difficiles à détecter pourrait également expliquer que les crimes économiques commis par des cadres supérieurs ne soient pas détectés aussi souvent que ceux imputables à des cadres intermédiaires ou à des employés subalternes.

## Confronter le fraudeur interne

Le sondage de cette année confirme que les organisations continuent de réagir énergiquement à la fraude interne, plus de 90 % des répondants disant congédier les fraudeurs démasqués. Globalement, la figure 17 traduit l'importance des mesures prises contre les fraudeurs internes – congédiement, appel aux autorités policières, poursuite civile, avis aux autorités de réglementation, etc. – par rapport à 2011.

Selon les statistiques, aucune organisation canadienne n'ignorait les mesures à prendre contre les fraudeurs internes ou n'a rien fait. Voilà qui devrait servir d'avertissement aux fraudeurs internes en devenir : s'ils se font prendre, ils en paieront le prix.

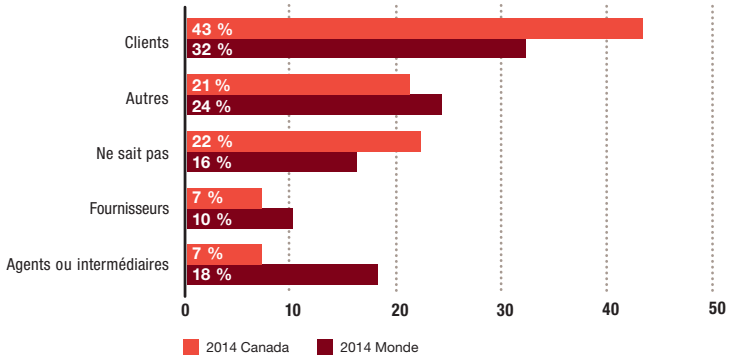
**Figure 17 : Mesures prises à l'encontre des fraudeurs internes**




## Le fraudeur externe

La presque majorité (43 % – figure 18) des organisations canadiennes désigne les clients comme les fraudeurs externes les plus courants.

**Figure 18 : Fraudeur externe (rôle)**

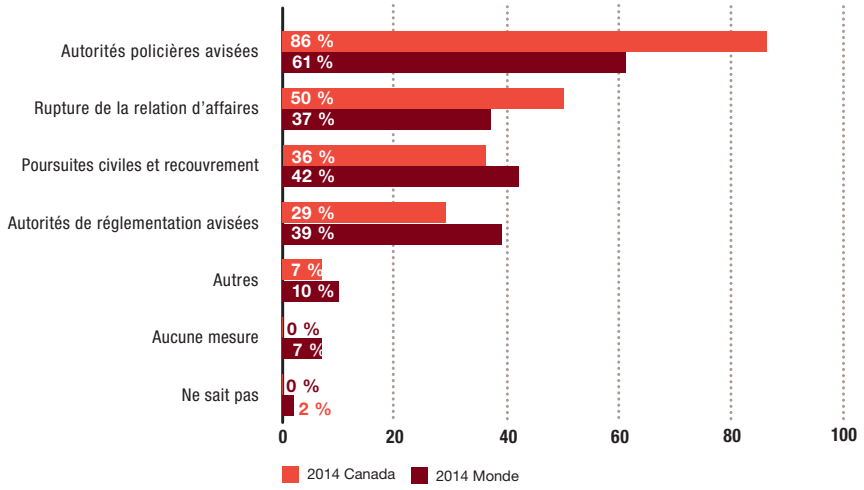



## Mesures prises à l'encontre des fraudeurs externes

À l'échelle canadienne, la mesure la plus courante prise à l'encontre des fraudeurs externes est le signalement aux autorités policières (86 % – figure 19). Selon ce résultat, les organisations canadiennes sont plus susceptibles d'informer la police si le fraudeur provient de l'extérieur (le taux est de 64 % si le fraudeur est interne – voir la figure 17). De multiples facteurs expliquent la diversité des mesures prises à l'encontre des fraudeurs externes, notamment le fait que le congédiement ne soit pas une option dans ces cas.

De nombreuses difficultés entravent les enquêtes portant sur des fraudes, que celles-ci aient été commises par un fraudeur interne ou externe. Entre autres, la capacité d'effectuer une enquête approfondie sur les allégations de fraude fait souvent défaut aux organismes d'application de la loi. Il est donc important que les organisations victimes de fraude aient un protocole d'enquête adéquat en place, afin de mener elles-mêmes des enquêtes complètes avant de se tourner vers les autorités.

**Figure 19 : Mesures prises à l'encontre des fraudeurs externes**

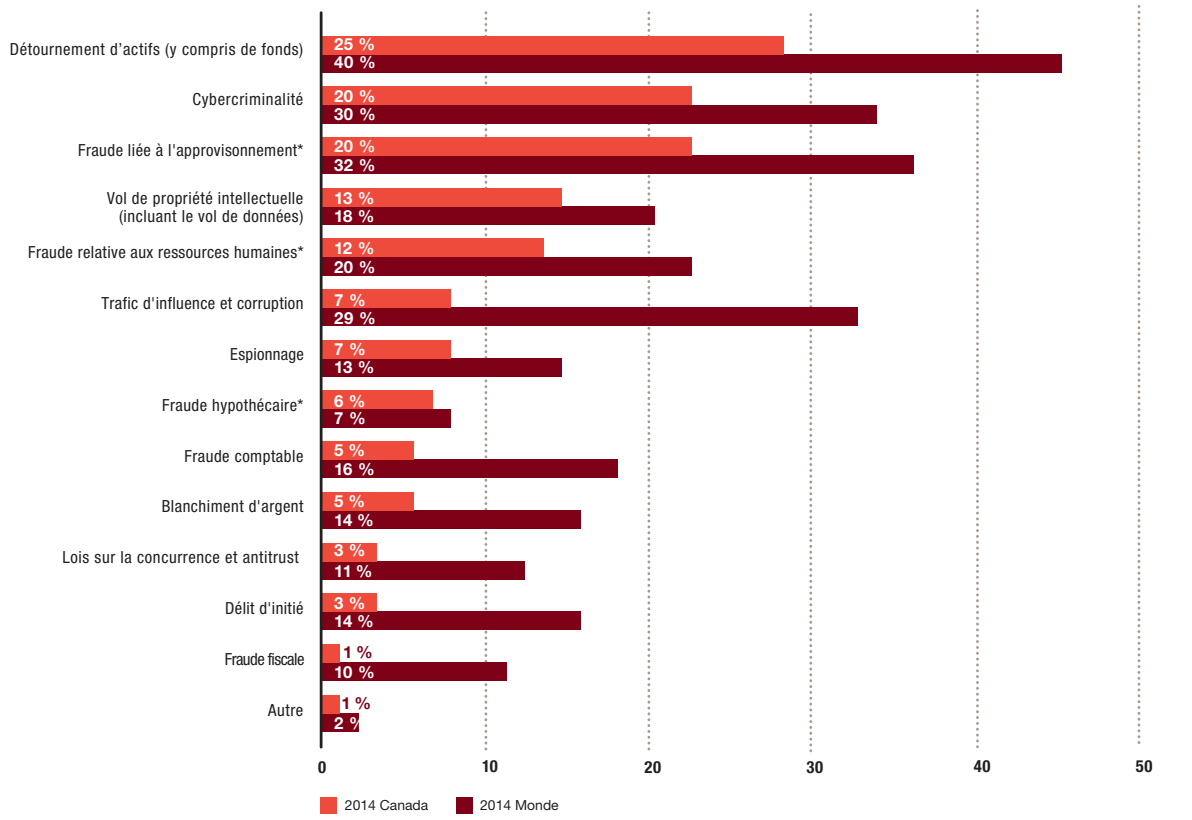


*Près du tiers (30 %) des répondants canadiens ont déclaré que leur organisation n'avait pas procédé à une évaluation du risque de fraude pendant la période visée par le sondage.*

# *Les organisations s'attendent à ce que la fraude persiste*

La figure 20 illustre les menaces de fraude économique auxquelles les organisations estiment qu'elles seront exposées au cours des 24 prochains mois. Une proportion de 25 % des répondants canadiens pensent que leur organisation est susceptible de subir un détournement d'actifs et 20 % de ceux-ci classent ex æquo, à la deuxième place, la cybercriminalité et la fraude liée à l'approvisionnement.

**Figure 20 : Perception de la fraude au cours des 24 prochains mois**




* Les répondants pouvaient sélectionner ces catégories de crimes économiques pour la première fois lors de notre sondage de 2014.

Malgré la persistance des crimes économiques et la perception que le risque de fraude est accru, 30 % des répondants canadiens ont affirmé que leur organisation n'avait pas procédé à une évaluation du risque de fraude pendant la période visée par le sondage. Lorsqu'on leur a demandé les raisons pour lesquelles leur organisation n'avait pas procédé à cette évaluation :

- 53 % ont affirmé que cette évaluation leur semblait présenter peu de valeur;
- 17 % ne savaient pas exactement en quoi consistait une évaluation du risque de fraude;
- 7 % ont cité le coût comme raison principale;
- 7 % ignoraient la raison pour laquelle l'évaluation du risque de fraude n'avait pas été effectuée.

Lorsque les dirigeants s'intéressent vivement à la fraude dans leur organisation et infligent des sanctions disciplinaires sévères à ses auteurs, ils donnent le ton qui convient. Les résultats du sondage de 2014 démontrent que le ton donné par la direction en matière d'éthique combiné à un environnement de contrôle interne solide constitue le meilleur moyen de dissuader les comportements répréhensibles et d'accroître la probabilité de détecter les activités frauduleuses.

Les organisations qui accordent beaucoup d'importance à l'intégrité – là où la haute direction joint le geste à la parole – et mettent en œuvre un programme antifraude complet et bien communiqué sont moins susceptibles d'être victimes de crimes économiques.

## Mettre en œuvre un programme efficace de lutte contre la fraude

Lorsqu'ils évaluent et examinent leur programme antifraude, les dirigeants devraient songer à demander à des professionnels des conseils sur les programmes de conformité et de prévention et de détection des fraudes; l'organisation doit également s'assurer que les lignes directrices et les pratiques de lutte contre la fraude reflètent l'évolution du climat économique, et que les mesures prises tiennent compte des lois et de la culture établies par les autorités compétentes de chaque territoire, sur le marché mondial.

À notre avis, les principaux contrôles antifraudes devraient comprendre les suivants :

1. Gouvernance – surveillance par le comité d'audit et le conseil d'administration;
2. Évaluation du risque de fraude;
3. Code d'éthique et de conduite;
4. Mécanismes de signalement des incidents;
5. Protocole d'enquête (y compris les rapports sur les opérations suspectes);
6. Protocole de mise en œuvre de mesures correctives;
7. Politiques et procédures d'embauche et de promotion;
8. Évaluation et tests de la direction.

*Les organisations qui accordent beaucoup d'importance à l'intégrité – là où la haute direction joint le geste à la parole – et mettent en œuvre un programme antifraude complet et bien communiqué sont moins susceptibles d'être victimes de crimes économiques.*

# Contactez-nous

## *Équipe de juricomptabilité*

**Steven P. Henderson**
Leader national, Services de juricomptabilité
Toronto
416 941-8328
steven.p.henderson@ca.pwc.com

**Lori-Ann Beausoleil**
Leader nationale, Services conseils en juricomptabilité
Toronto
416 687-8617
lori-ann.beausoleil@ca.pwc.com

**Peter Vakof**
Leader, Solutions technologiques en juricomptabilité
Toronto
416 814-5841
peter.vakof@ca.pwc.com

## *Calgary*

**Krista A. Mooney**
Directrice principale
403 509-7336
krista.a.mooney@ca.pwc.com

## *Halifax*

**Paul F. Bradley**
Associé
902 491-7436
paul.f.bradley@ca.pwc.com

**James A. Pomeroy**
Vice-président
902 491-7416
james.a.pomeroy@ca.pwc.com

## *London*

**Chris Gray**
Vice-président
519 640-8011
chris.gray@ca.pwc.com

## *Montréal*

**Marie-Chantal Dréau**
Associée
Montréal
514 205-5407
marie-chantal.dreau@ca.pwc.com

**Benoit Legault**
Vice-président
514 205-5682
benoit.legault@ca.pwc.com

## *Ottawa*

**Kas Rehman**
Associé
613 755-4328
kas.rehman@ca.pwc.com

**Chantal Amyot**
Directrice principale
613 755-4355
chantal.amyot@ca.pwc.com

**Jason Armstrong**
Directeur principal
613 755-8743
jason.r.armstrong@ca.pwc.com

**Steve Malette**
Vice-président
613 755-5979
steven.m.malette@ca.pwc.com

## *Toronto*

**Sarah E. MacGregor**
Associée
416 814-5763
sarah.e.macgregor@ca.pwc.com

**Harm Atwal**
Directrice principale
416 869-2330
harm.k.atwal@ca.pwc.com

**Jeff Bowen**
Directeur principal
416 869-2472
jeff.r.bowen@ca.pwc.com

H. Ray Haywood
**Directeur principal**
416 814-5801
h.ray.haywood@ca.pwc.com

**Roberto Israel**
Directeur principal
416 814-5740
roberto.r.israel@ca.pwc.com

**Kelly Ohayon**
Directrice principale
416 814-5843
kelly.ohayon@ca.pwc.com

**Lloyd Wilks**
Directeur principal
416 687-8115
lloyd.wilks@ca.pwc.com

## *Winnipeg*

**Jeffrey Johnson**
Associé
204 926-2441
jeffrey.b.johnson@ca.pwc.com

**Dave Johnson**
Vice-président
204 926-2423
dave.a.johnson@ca.pwc.com

**Kyla Kramps**
Vice-présidente
204 926-2434
kyla.kramps@ca.pwc.com

*www.pwc.com/ca/fr/crimesurvey*

**Pour voir une copie de nos rapports, numérisez ce code RQ avec une application lisant les codes RQ à l'aide de votre téléphone intelligent ou de votre tablette.**

*La valeur selon vous*

Nous mettons l'accent sur quatre domaines : certification, conseils, transactions et services fiscaux. Cependant, nous sommes d'avis que les produits et services standards ne sont pas toujours la solution appropriée. La façon dont nous utilisons nos connaissances et notre expérience dépend de ce que vous recherchez. PwC Canada compte plus de 5 700 associés et employés, d'un océan à l'autre. Que vous soyez un client ou un membre de l'une de nos équipes, nous cherchons à approfondir nos relations avec vous et à créer de la valeur dans tout ce que nous faisons. Pour commencer, nous aimerions faire connaissance avec vous. Vous parlez et nous vous écoutons. Ce que vous nous direz déterminera comment nous utiliserons notre réseau mondial composé de plus de 184 000 personnes dans 157 pays — ainsi que leurs relations, leurs contacts et leur savoir-faire — pour vous aider à obtenir la valeur que vous recherchez. Pour plus de renseignements, consultez la page suivante : www.pwc.com/ca/fr.

Ces renseignements sont fournis à titre d'information seulement et n'ont pas pour objet de remplacer les conseils d'un professionnel.

© PricewaterhouseCoopers LLP/s.r.l./ s.e.n.c.r.l., une société à responsabilité limitée de l'Ontario, 2014. Tous droits réservés. PwC s'entend du cabinet canadien, et quelquefois du réseau mondial de PwC. Chaque société membre est une entité distincte sur le plan juridique. Pour obtenir de plus amples renseignements, visitez notre site Web à l'adresse : www.pwc.com/structure.
3350-03-0214

*PwC's 2014 Global Economic Crime Survey – Mainland China, Hong Kong, and Macau Supplement*

# *Economic crime: The danger within*

## *4/5*

Economic crimes in Mainland China reported four out of five times are "inside jobs".

## *39%*

In Mainland China, 39% of respondents suffering crime say they have experienced bribery and corruption.

## *99%*

In Hong Kong and Macau, 99% of respondents say they believe cybercrime risk is holding steady, or has increased.

pwc 普华永道

*www.pwc.com/crimesurvey*

# Contents

# Foreword

We are delighted to present the Mainland China, Hong Kong, and Macau supplement to the 2014 PwC Global Economic Crime Survey (GECS or the Survey).

This year's GECS features the perspectives of more than 5,000 respondents from 95 countries on the prevalence and direction of economic crime.

The Mainland China, Hong Kong, and Macau supplement provides a focussed discussion of the issues facing local respondents who participated in the GECS. This analysis is based on responses from 85 executives based in mainland China and 116 based in Hong Kong and Macau, and covers the last twenty-four months.

The Survey demonstrates that some of the challenges facing business in mainland China, Hong Kong and Macau are consistent with the rest of the world whereas in other areas they differ and we have sought to draw this out.

The Survey is not meant to be definitive, nor can it claim to provide the answers to the economic crime-related challenges facing organisations operating in these markets. But it does identify key issues surrounding cybercrime, bribery and corruption, procurement fraud, and money laundering that should be of great relevance to organisations establishing or enhancing systems to reduce the risk of economic crime.

The issues raised and conclusions drawn are by no means all negative. For instance, only 5% of Hong Kong and Macau respondents say they have been asked to pay a bribe, which is almost four times less than the regional and global averages.

Meanwhile, mainland China respondents' levels of reported crime at 27% are substantially lower than those reported Globally (37%) and in the US (45%). Athough lack of economic crime detection capability among mainland China-based organisations may partially explain this.

In mainland China two recurring themes featured heavily within the Survey, namely concerns around bribery and corruption and concerns around procurement fraud and kickbacks.

These concerns, both of which pertain to the issue of corruption, may be partially explained by the mainland authorities' concerted and ongoing anti-corruption drive which has resulted in disciplinary measures against about 182,000 officials nationwide[1] and has involved some multinational corporations (MNCs) and their foreign executives.

As the mainland China market continues to grow, economic crime will continue to threaten processes across all businesses – entering into business relationships, buying and selling, importing and exporting, paying and collecting.

1. http://news.xinhuanet.com/english/china/2014-01/10/c_133034868.htm

# The Global landscape

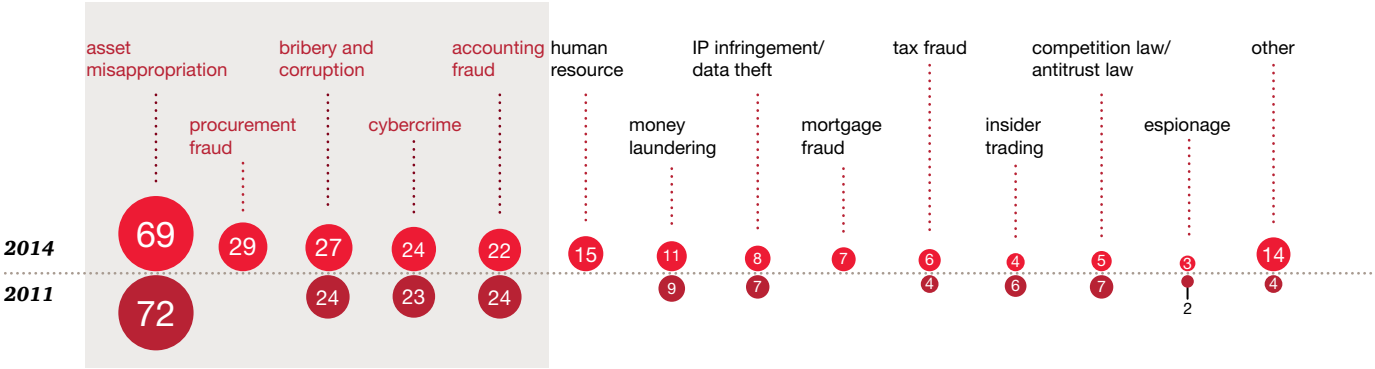
## Types of fraud

Since our initial Economic Crime Survey in 2001, three types of frauds have consistently been highlighted by respondents – asset misappropriation (consistently the largest), bribery and corruption and accounting fraud. Cybercrime was added as a distinct classification in 2011.

This year, procurement fraud has been added as a category, driven, we believe by two trends – more competitive public tender processes from governments and state-owned businesses, and the increasing integration of supply chain into core business activities.

As shown in Figure 3[2], respondents reported procurement fraud to be the second most frequently reported type of fraud experienced.

**Figure 3: Types of economic crime reported**

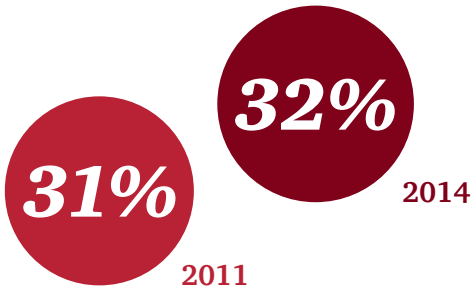



% of all respondents who experienced economic crime over the survey period

2. Extract from PwC's 2014 Global Economic Crime Survey

## The regional story:

Asia Pacific has remained relatively stable with regard to numbers of respondents who have experienced economic crime between the two most recent surveys:

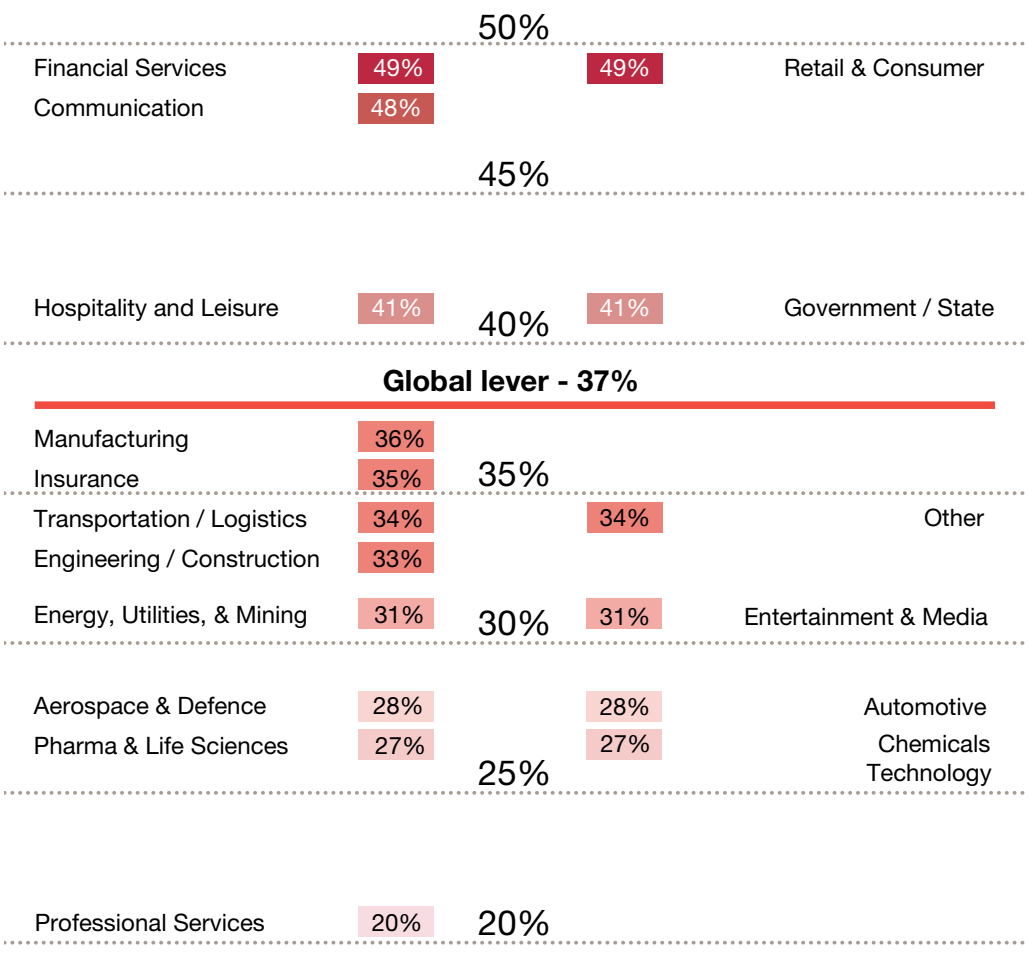



Interestingly, the "Emerging Eight" (Brazil, mainland China, India, Indonesia, Mexico, Russia, Turkey and South Africa) category has increased in reported fraud from 35% in the 2011 survey to 40% in 2014.

## Economic crime across industries

Industry focuses across mainland China, Hong Kong and Macau differ, however each location is impacted by the top 5 industries reporting economic crime in this survey as highlighted in figure 5[3] below.

**Figure 5:Economic crime reported by industry**




% of all respondents who experienced economic crime over the survey period

3. Extract from PwC's 2014 Global Economic Crime Survey

## Highlights

***27% of respondents in mainland China and 16% in Hong Kong and Macau report that they have experienced economic crime, compared to 32% in Asia Pacific and 37% globally.***

# The local landscape

| Mainland China | Hong Kong and Macau |
|---|---|
| Respondents say **four out of every five reported** economic crimes are **'inside jobs'** | The proportion of respondents who reported suffering **money laundering** were **three times regional and global** averages |
| Respondents say **28%** of internal fraudsters identified are aged **under 30** and **22%** have worked in the company for **less than two years** | **37%** of respondents who reported economic crime say they experienced **money laundering**, but only **15%** of all respondents say they think it will **affect them in the next 24 months** |
| **39%** of respondents suffering crime say they have experienced **bribery and corruption**, and **41%** of all respondents expect this to increase | Of the respondents who suffered economic crime **37% experienced cybercrime** and **7%** acknowledge **losses of more than US$1 million** |
| Respondents in mainland China say they were **five times** more likely to be asked to pay a **bribe** than respondents in Hong Kong and **one and a half times** more likely than regional and global averages | **99%** of respondents say they believe **cybercrime risk** has remained steady or increased. |
| **48%** of respondents suffering crime say they encountered **procurement fraud**, mainly during vendor selection /contracting and bid process stages | **14%** of respondents say they believe **cybercrime** attacks are likely, compared to **26% regionally and 30% globally** |
| 26% of respondents say **whistleblower hotlines were not used**, yet **78% rate** these as being **effective** | **28%** of all respondents say their companies **do not** conduct **risk assessments** and **10% say that they do not know if they do. 47%** of those **who do not** conduct them **do not know** what a risk assessment involves |

All of the themes reported in this Survey occur in the context of the mainland authorities' anti-corruption drive, which includes clampdowns on government officials spending public money on gifts and dinners and also actions against private sector companies who act inappropriately. Internationally, the US Department of Justice and the Securities and Exchange Commission have been aggressively enforcing the Foreign Corrupt Practices Act (FCPA). Many of their enforcement actions include substantial mainland China components and have resulted in acute damage to corporate reputations, not to mention financial losses through fines and disgorgements.

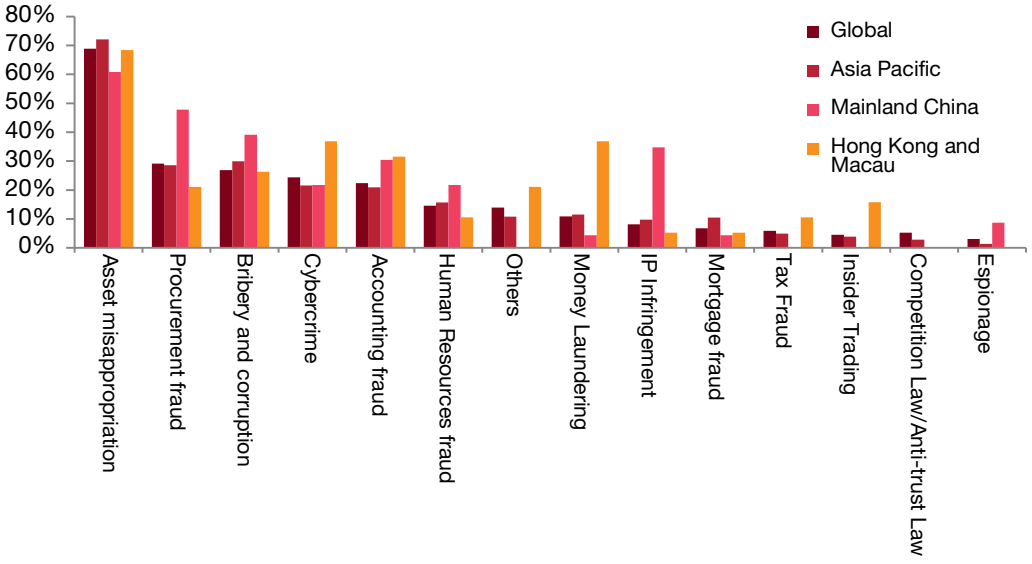
In addition, the more recent UK Bribery Act which was promulgated in 2011 is still in its early stages and therefore seemingly of less immediate significance to many companies. However, it could still have additional far-reaching implications and warrants careful attention for organisations operating in key markets, though one-third of mainland China respondents say they are unaware of the UK Bribery Act or of how their company has responded to it.

In the face of greater regulatory activity in mainland China and globally, the stakes have never been higher. Increasing numbers of companies are beefing up compliance programs and departments. However, more could still be done as this Survey demonstrates.

## Types of Fraud

Asset misappropriation in mainland China, Hong Kong and Macau remains the largest type of fraud reported in line with the global result. In mainland China, procurement fraud was the second largest reported by our respondents who said their organisations had suffered economic crime, with 48% having experienced it. This is closely followed by bribery and corruption and IP infringement in mainland China and money laundering and cybercrime in Hong Kong and Macau.

**Chart 1: Types of Fraud**



# Are companies doing enough to prevent and detect economic crime?

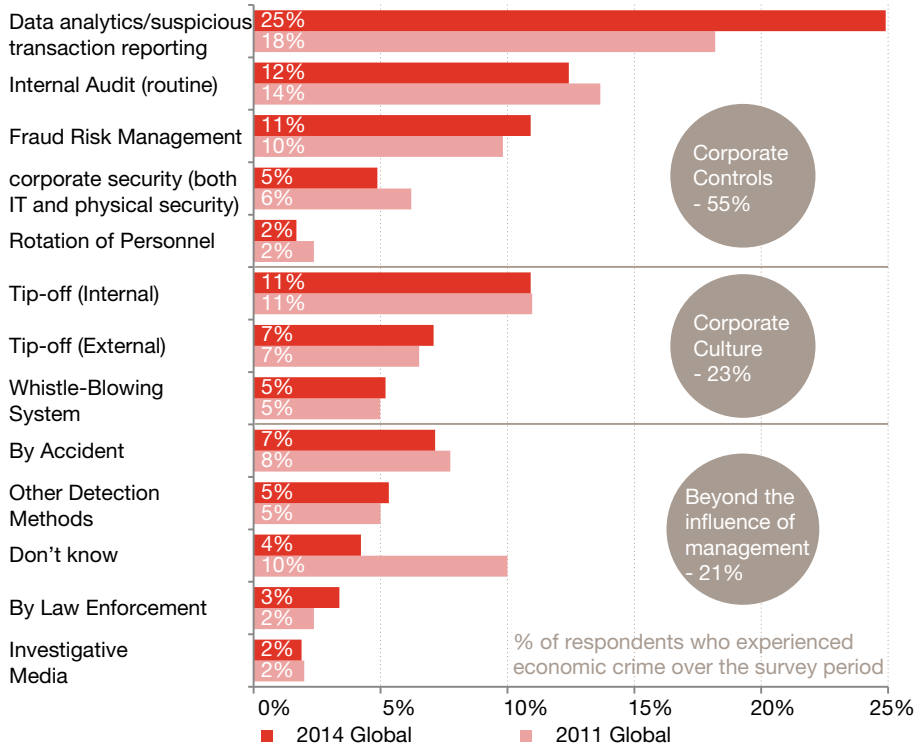
## Proactive vs Reactive

Some of the results of this Survey are surprising and some are a cause for concern as to whether some of the detection tools are operating as effectively as we would hope.

47% of respondents in Hong Kong and Macau and 26% of respondents in Mainland China whose organisations have whistleblower hotlines said that these systems were not used at all. Moreover, only 5% of respondents in Hong Kong and Macau (none in Mainland China) say that economic crimes were detected by whistleblower hotlines.

In addition, Hong Kong and Macau respondents reported that only 5% of economic crime was detected using Suspicious Transactions Analyses (STA) / Data Alalytics technology. This is a different perspective from the Global result where STA / Data Analytics, at 25% is now the most frequent way respondents said the economic crime was detected (see Figure 26[4]). In our 2011 Survey, STA detected 18% of economic crimes indicating that this method for detecting economic crime is increasing over time. This represents an opportunity for the Hong Kong and Macau markets to increase Data Analytics as a technique for looking for economic crime.

**Figure 26: Method of detection of most serious economic crime experienced**




*Data Analytics was added as a category in the 2014 survey.

## Are risks understood?

Interestingly, 28% of Hong Kong respondents claim that their companies do not conduct any risk assessments, and a further 10% say they do not know whether they conduct risk assessments or not. Of those respondents who do not conduct any risk assessments almost half (47%) say they had no knowledge of what a fraud risk assessment actually involved.

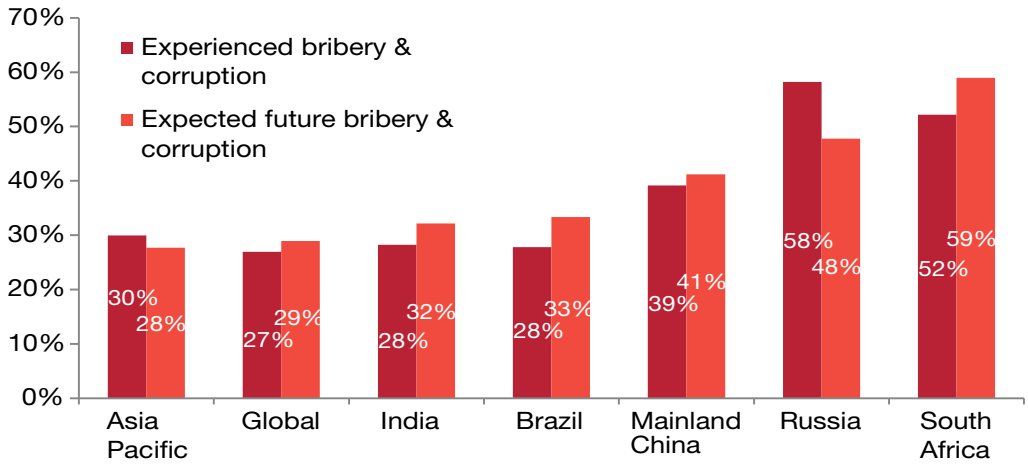
4. Extract from PwC's 2014 Global Economic Crime Survey

# *Bribery, Corruption and the risk of the "inside job"*

While the threat of cybercrime in Hong Kong and Macau is reflected in the GECS, the risk of cybercrime, though very real in the age of social media, does not feature as heavily among mainland China respondents where more traditional frauds are of greater concern. 39% of mainland China respondents who reported economic crime say they experienced some form of bribery and corruption, and 41% say that they expect this to increase, considerably more than Brazil (33%), India (32%), Asia Pacific (28%) and Global (29%), though less than Russia (48%) and South Africa (59%).

Ongoing enforcement of anti-corruption legislation both domestically and internationally has likely done much to raise corporate awareness of, and sensitivity to, bribery in mainland China. Indeed, respondents in mainland China say they were five times more likely to have been asked to pay a bribe than their counterparts in Hong Kong, and one and a half times more likely than in Asia Pacific and globally. Of the other BRICS economies, only Russia respondents experienced more requests for bribes than mainland China (Chart 2 refers).

**Chart 2: Expected and experienced bribery and corruption**



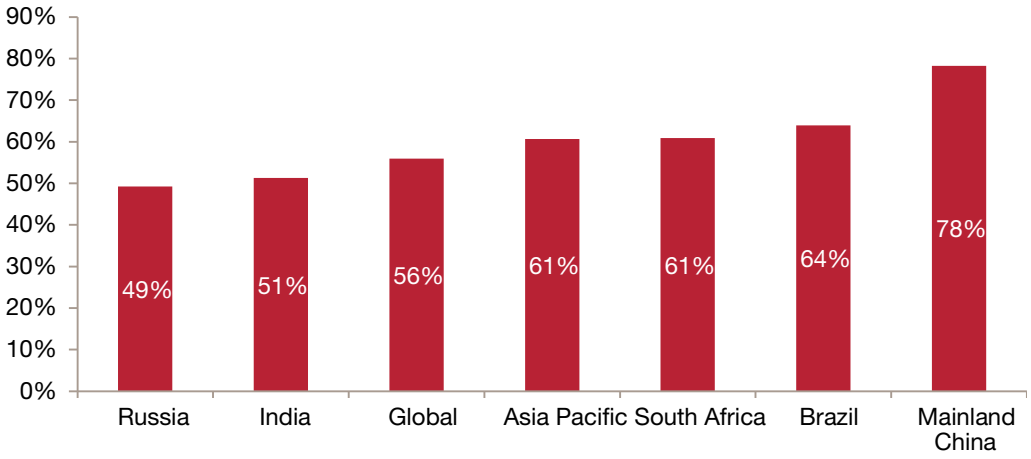

## The inside threat

The Survey also indicates that in almost four out of every five economic crimes reported in mainland China, the perpetrator was identified as someone inside the company. As Chart 3 shows, this is clearly a markedly higher proportion than encountered in other comparable countries. Further analysis of these 'inside jobs' reveals some 28% of these perpetrators were under the age of 30, according to our respondents.

Internal fraud is markedly higher in mainland China than in other BRICS countries according to respondents, with Brazil (on 64%), South Africa (61%), India (51%) and Russia (49%). Such internal fraud typically suggests weakness in an organisation's internal controls. Many organisations have already invested and strengthened their internal controls, but there would appear to be much room remaining for improvement.

Respondents also said that 22% of the perpetrators of economic crimes had worked for the company for less than two years, perhaps not surprising with mainland China's mobile workforce. With this in mind, perhaps we should all be asking ourselves what diligence are we doing over the hires we need to grow our businesses?

**Chart 3: Inside jobs identified**




## Employer beware

Experience of economic crime may also partly reflect the manufacturing, energy, and heavy industry fundamentals which have underpinned mainland China's emergence as a global economic power. These sectors' complex supply chains can be susceptible to bribery and corruption, exacerbated by inconsistent enforcement of existing regulations by comparison to developed economies.

In addition, in instances where internal fraud had been identified, 33% of respondents said that their companies had only reprimanded or transferred the fraudsters. Proving categorically that an employee has committed fraud is rarely a straightforward process. In such instances, employers are often most concerned with corporate reputations and ridding themselves of a bad apple with minimal fuss and publicity. As such, fraudsters may quietly resign (often after a pay-off) leaving little or no public record of their illegal activity. The lack of a public record puts the onus upon the next would-be employer in mainland China to have a strong employee screening process else fraudsters may be able to move relatively easily from one position to another.

Finally, more than a quarter of mainland China respondents say that their whistleblower hotlines were not used once during the period of the Survey, and yet 78% rate their hotlines as ranging from slightly to very effective. An effective whistleblower hotline in a sizable organisation should be in regular use as long it has been marketed effectively and its independence is trusted by employees.

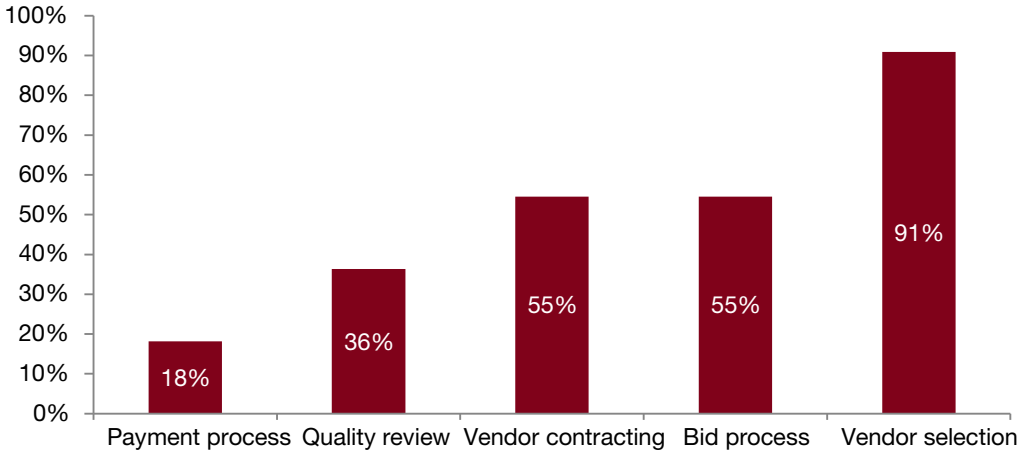
Organisations also need effective, independent and trusted whistleblower hotlines functioning across email, fax and phone and available 24 hours a day in Chinese language. The fact that mainland China respondents say that 26% of their whistleblower mechanisms were not used at all during the two years covered by the Survey, and that these systems did not account for detection of any economic crime, strongly suggests that more could be done to improve this relatively straightforward system.

# *Procurement fraud one of the top economic crimes experienced by mainland China respondents*

Procurement fraud is systemic in nature and can have a long-term and hugely damaging impact on an organisation. It is often associated most closely with supply-chain-dependent businesses, with the likelihood of it occurring increasing as organisations enter into commercial or public tender processes or which seek to acquire goods and services.

As with the risk of bribery and corruption, the risk can be heightened by sometimes inconsistent enforcement of regulations and a business environment that can lack transparency. Organisations in mainland China are also likely to experience a greater threat of procurement fraud during the vendor selection process (in 91% of instances), vendor contracting (55%) and bid process (55%) stages (see Chart 4).

**Chart 4: Occurrence of fraud during the procurement process in mainland China**

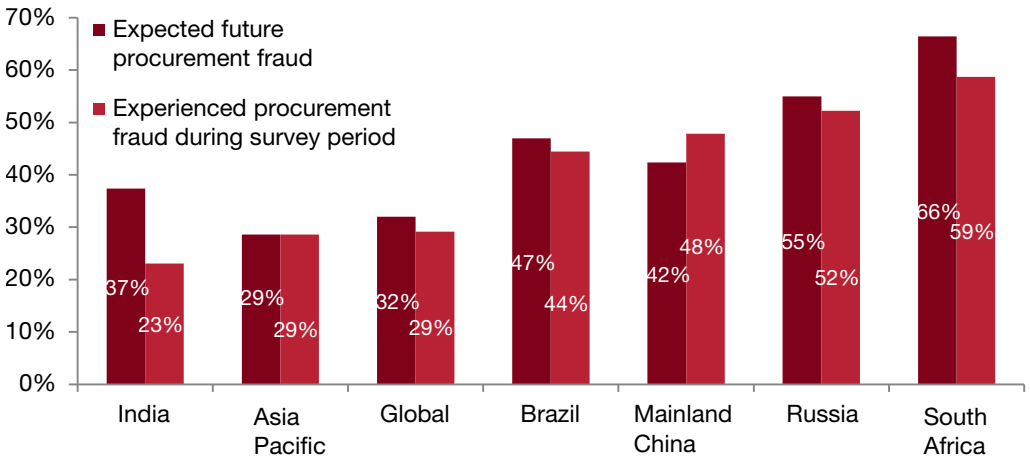


## Kickbacks, Corruption and Controls

It comes as no surprise therefore, that procurement fraud is identified by respondents in mainland China as one of the most frequently experienced economic crimes, with 48% of respondents suffering economic crimes having encountered it. This is significantly higher than the results recorded for Asia Pacific and globally (both 29%).

Procurement fraud involves employees taking kickbacks and other illicit arrangements, and its presence strongly suggests that an organisation has weak internal controls, lack of transparency, and limited monitoring of supplier and employee relationships. This supports earlier observations on bribery and corruption issues whereby respondents report that almost four out of every five economic crimes reported were perpetrated by an employee of the company in question.

**Chart 5: Expected and experienced procurement fraud**

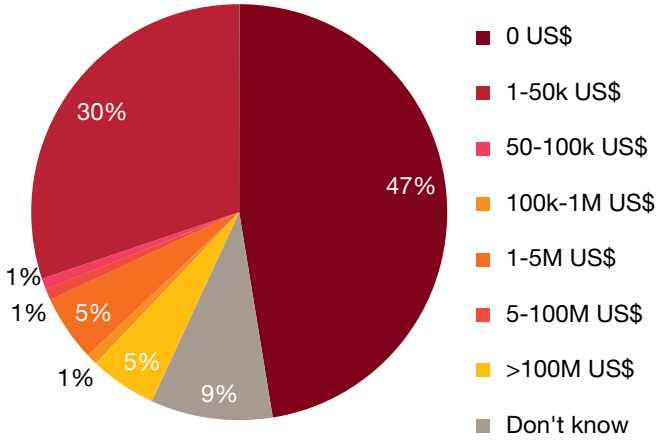


# Hong Kong and Macau respondents remain confident in face of growing cybercrime threat

Difficult to detect and harder to solve, cybercrime is one of the most threatening and least understood of economic crimes to a modern business, where confidential data has been illegally accessed. In many instances, companies are often unaware that they have been targeted, and any detection of the fraud typically occurs sometime after the event.

As might be expected given the data dependant nature of many businesses in their locations, Hong Kong and Macau respondents identify cybercrime as a major and growing threat. 37% of Hong Kong and Macau respondents who reported economic crime say they have experienced cybercrime, and nine in ten respondents say the consequences they most fear are reputational damage, financial loss, and regulatory risk. Furthermore, 7% of all Hong Kong and Macau respondents say their companies lost more than US$1 million through cybercrime (see Chart 6).

**Chart 6: Estimated financial losses from cybercrime in Hong Kong and Macau**




## Hi-tech, high stakes and high risk

In light of these figures, it is of little surprise that 99% of Hong Kong respondents say that they perceive the risk of cybercrime to have remained unchanged or to have increased in their market, echoing similar concerns in Singapore where the figure is 100%.

However, only 14% of the Hong Kong and Macau respondents feel that their organisation will be attacked in the next twenty-four months (11% in Singapore). This is significantly below the global and Asia Pacific responses of 30% and 26% respectively where respondents feel that their organisation is at risk of a cyber-attack.

The growing threat posed by cybercrime in Hong Kong and Macau is underlined by statistics from the Hong Kong Police Force. They report instances of cybercrime increasing to 5,133 in 2013, up by 70% over the 3,015 cases in 2012. This has been primarily fuelled by 1,153 reports of e-mail scams which cost businesses about HK$760 million in losses - a significant increase on the 2012 figures when there were 430 such cases resulting in HK$180 million in losses[5].

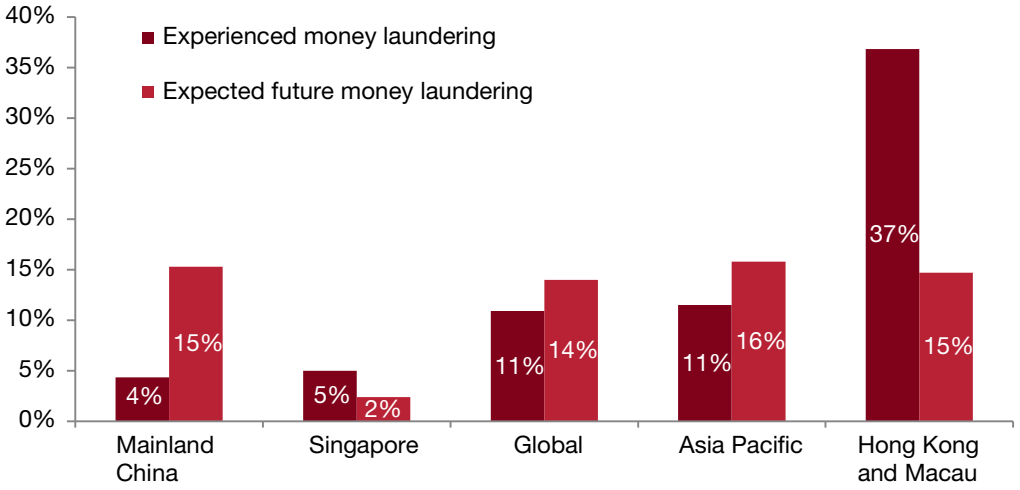
5. Hong Kong Police Force press conference: http://www.police.gov.hk/ppp_en/01_about_us/cp_ye.html

# Economic crime reflective of industry focus

The Survey highlights the risk posed by money laundering to global business, especially within the financial sector. Hong Kong and Macau respondents cite money laundering as a frequent form of economic crime. Hong Kong's concentration of banks and financial institutions means that, as a type of economic crime suffered, money laundering is a much more significant threat to the Hong Kong respondents. Likewise, money laundering remains a concern for Macau's vast gaming sector.

According to the Survey, 37% of those in Hong Kong and Macau respondents who had experienced economic crime pointed towards money laundering. This is significantly higher than others in the region.

**Chart 7: Expected and experienced money laundering**




## Justifiable confidence or complacency?

Despite the relatively high numbers of respondents who say their organisations have suffered from money laundering, respondents nonetheless report a relatively optimistic view of future risk. Whether this is due to confidence in their organisations' proven anti-money laundering systems, or whether it reveals an element of complacency is unclear. But only 15% of respondents say they expect to experience money laundering in the future, and 75% say they think a reoccurrence of money laundering is unlikely.

## *Methodology*

PwC carried out the Global Economic Crime Survey between August 2013 and February 2014. The Survey consisted of a globally accessible web based questionnaire on a secure site. Executives wishing to respond to the Survey were directed to the site, and responded to the four sections as follows:

The survey has four sections:

- General profiling questions
- Comparative questions looking at what economic crime organisations had experienced
- Cybercrime fraud threats
- Corruption/bribery, money laundering and competition law/antitrust law

## *About the survey*

The 2014 GECS - Mainland China, Hong Kong and Macau supplement is based upon responses from 201 respondents (85 from mainland China and 116 from Hong Kong and Macau). 51% of respondents from mainland China and 53% from Hong Kong and Macau were senior executives of their respective organisations. 55% of respondents from mainland China and 49% from Hong Kong and Macau represented listed companies. 70% of respondents from mainland China and 64% from Hong Kong and Macau represented organisations with more than 1,000 employees.

Research techniques:

1. Survey of executives in the organisation. The findings in this Survey come from executives' reports of their experiences of economic crimes in their organisations. We obtained information from them on the different types of economic crime, their impact on the organisation (both the financial loss and any collateral damage), the perpetrator of these crimes, what action the organisation took and how they responded to the crime.

2. Questions relating to cybercrime, bribery and corruption, money laundering and competition law/antitrust law. This Survey takes a detailed look at these threats which are often systemic in nature and thus are more prone to cause long-term damage to the organisation.

3. Comparisons with other countries with similar economic conditions. Where relevant Hong Kong and Macau findings were compared with Singapore, and likewise mainland China with the other BRICS nations (Brazil, Russia, India and South Africa) to identify any inconsistencies or other matters of note.

4. For the purposes of the Survey, economic crime is described as "the intentional use of deceit to deprive another of money, property or legal right".

5. Whilst general profiling questions concerning industry, geographical area of responsibility and size of business operations were posed, participants were able to respond to the Survey anonymously.

For the global report, see www.pwc.com/crimesurvey.

# Contacts

## *Hong Kong*

**John Donker**
***Partner, Forensics Services***
+852 2289 2411
john.donker@hk.pwc.com

**Megan Haas**
***Partner, Forensics Services***
+(852) 2289 1911
megan.l.haas@hk.pwc.com

**Antoinette Lau**
***Partner, Forensics Services***
+ (852) 2289 2403
antoinette.yy.lau@hk.pwc.com

## *Shanghai*

**Jean Roux**
***Partner, Forensics Services***
+86 (21) 2323 3988
jean.roux@cn.pwc.com

**Ramesh Moosa**
***Partner, Forensics Services***
+86 (21) 2323 8688
ramesh.moosa@cn.pwc.com

## *Beijing*

**Brian McGinley**
***Partner, Forensics Services***
+86 (10) 6533 2171
brian.mcginley@cn.pwc.com

*www.pwc.com/crimesurvey*

© 2014 PricewaterhouseCoopers Management Consulting (Shanghai) Limited. All rights reserved. PwC refers to the China member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

# 經濟犯罪：危機四伏

## 4/5

中國大陸受訪者表示，每五宗所呈報的經濟犯罪個案，有四宗屬「內部人員作案」

## 39%

曾經歷經濟罪案的受訪者中，39%的中國大陸受訪者表示曾經歷賄賂和貪污

## 99%

99%的香港及澳門受訪者相信網絡罪行的風險將維持不變或有所增加

# 目錄

# 前言

我們很高興為「羅兵咸永道2014年全球經濟犯罪調查–中國大陸、香港及澳門補充文件」(GECS或本調查)進行發佈。

今年的GECS包含來自95個國家的5,000多名受訪者對經濟犯罪的發生比率和趨勢的觀點與評論。

「全球經濟犯罪調查–中國大陸、香港及澳門補充文件」就GECS受訪者所面對的問題,提供了一個集中討論的平台。文中的分析以中國大陸的85位行政人員和香港及澳門的116位行政人員的回應作為基礎,並涵蓋過去24個月的情況。

本調查體現出中國大陸、香港及澳門跟全球商界所面對的某些挑戰是一致的;至於其他相異之處,我們力求於本文列舉出來。

本調查的目的並非為當地商界就經濟罪行所帶來的挑戰提供明確的答案,但它指出了有關網絡罪行、賄賂和貪污、採購舞弊和洗黑錢的關鍵問題,相信有助於正在建立或加強體制的機構減低經濟罪行的風險。

調查結果亦反映出一些正面的信息。例如,只有5%港澳受訪者表示被要求支付賄款,這較亞太區和全球平均比例低近四倍。

與此同時,表示曾有呈報經濟罪案的中國大陸受訪者比率為27%,較全球相同調查的37%及美國相同調查的45%為低。但二者差距的部分原因可能是中國大陸機構欠缺檢測經濟犯罪的能力。

中國大陸的調查結果圍繞兩個議題:一、對賄賂及貪污的關注,二、對採購舞弊和回佣的關注。

這些問題均涉及貪腐。而對大陸貪腐問題的關注亦促使當局進行全面及持續的反貪腐運動,全國已有約182,000官員[1]面臨紀律處分,當中涉及跨國企業(MNCs)和其外籍高層管理人員。

隨著中國大陸市場日益壯大,經濟犯罪將繼續對所有商業活動構成威脅,從建立商業關係、採購和銷售、進出口活動、到款項交收各方面均受影響。

1. http://news.xinhuanet.com/english/china/2014-01/10/c_133034868.htm

# 環球趨勢

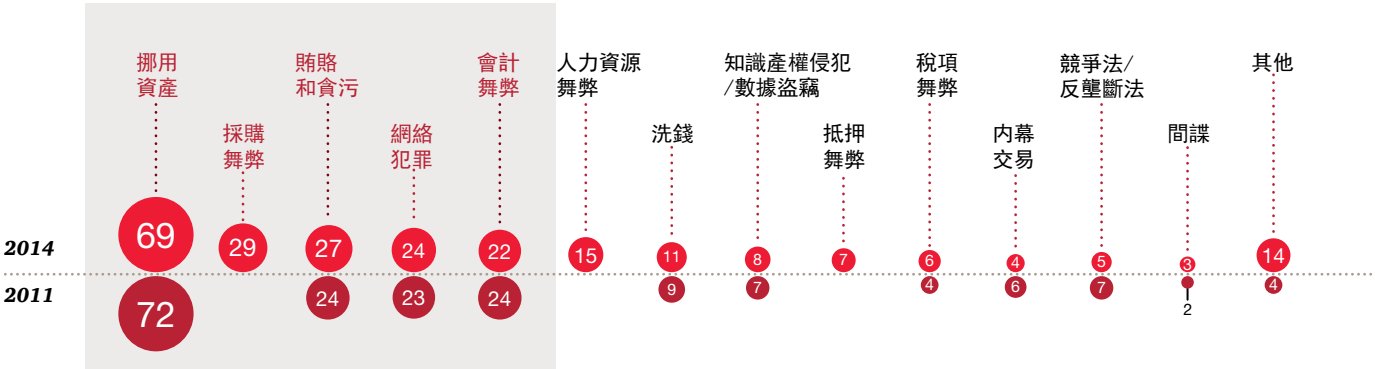
## 各欺詐案類型

經濟犯罪調查始於2001年，至今，三類最普遍的欺詐行為是：挪用資產（為歷屆調查中最常見）、賄賂和貪污、會計舞弊行為。自2011年起，網絡罪行被新增為獨立分類。

今年的調查則增加了一項目為採購舞弊，相信與兩種現象有關：一是政府和國有企業公開招標過程競爭越趨激烈；二是供應鏈於企業核心業務佔有更重要的位置。

正如圖3[2]所示，受訪者指採購舞弊屬最常面對的欺詐行為的第二位。

**圖3: 舉報的欺詐案類型**

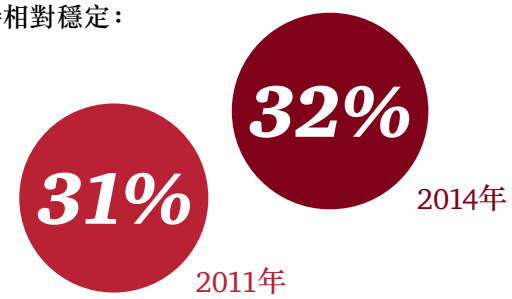



曾於調查期間面對經濟犯罪的受訪者百分比

2. 摘錄自「羅兵咸永道2014年全球經濟犯罪調查 (GECS)」

## 區域事例

在最近的兩次調查中，亞太地區曾經歷經濟罪案的受訪者人數比率保持相對穩定：

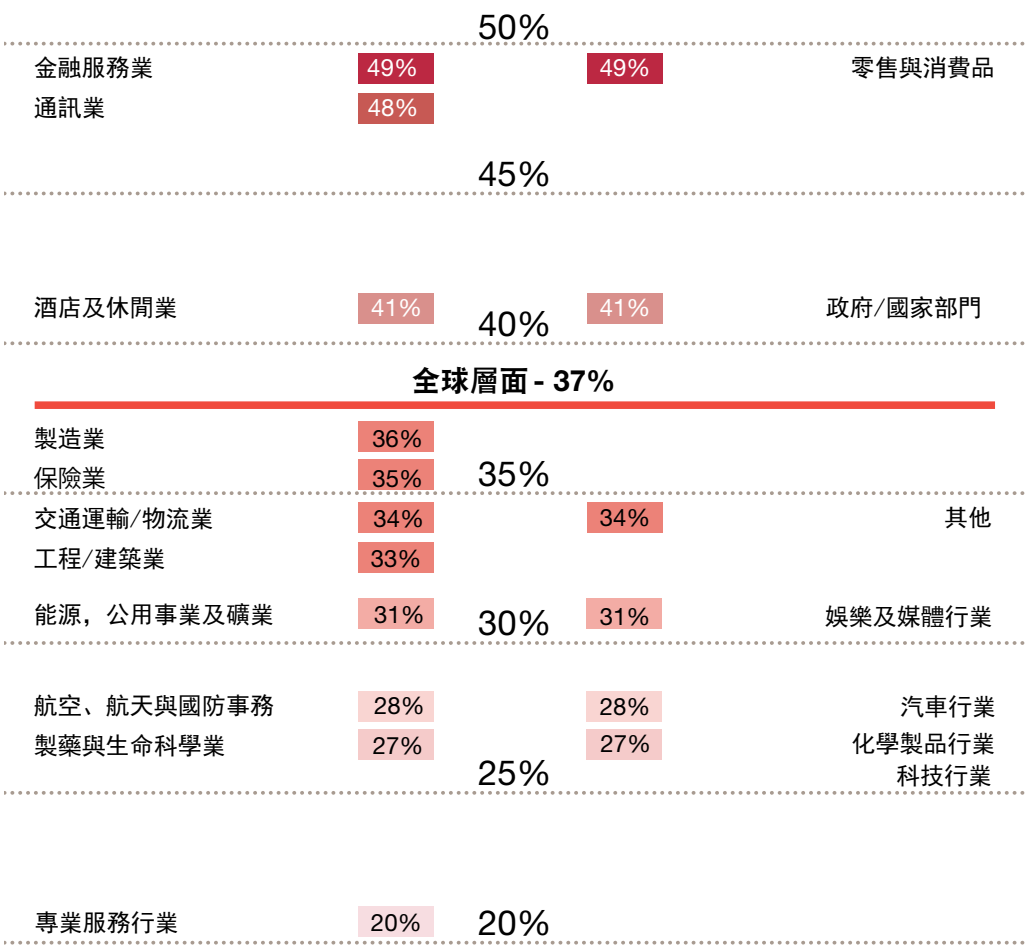



而「新興八景」 地區（巴西、中國大陸、印度、印度尼西亞、墨西哥、俄羅斯、土耳其和南非）的舞弊情況則由2011年調查中的35%上升至2014年的40% 。

## 各行業的經濟罪行

縱然中國大陸、香港及澳門三地的主要行業不同，但以下行業為是次調查三地中首五個最常面對經濟罪行的行業（圖5[3]）。

**圖5: 行業經濟犯罪發生率**




曾於調查期間面對經濟犯罪的受訪者百分比

3. 摘錄自「羅兵咸永道2014年全球經濟犯罪調查 (GECS)」

## 要点

**27%的中國大陸受訪者和16%的香港及澳門受訪者表示，他們曾面對經濟罪案，而具相同經歷的亞太地區及全球的受訪者則分別有32%及37%。**

# 本地趨勢

| 中國大陸 | 香港及澳門 |
|---|---|
| 受訪者表示**每五宗所呈報的經濟犯罪個案，有四宗屬「內部人員作案」** | 曾受**洗黑錢**影響的受訪者**為亞太區及全球**平均比例的**三倍** |
| 受訪者指，**30歲以下**的內部作案者佔**28%**，在公司**就業不足兩年**的佔**22%** | 曾舉報經濟罪案的受訪者中，**37%**表示他們曾有面對**洗黑錢**的經歷；而所有受訪者中，只有**15%**認為會在**未來24個月受到洗黑錢的影響** |
| 曾面對經濟罪案的受訪者中，**39%**表示曾經面對**賄賂和貪污**；而所有受訪者中，**41%**預期這比例將會增加 | 曾面對經濟罪案的受訪者中，**37%**表示曾**經歷網絡罪行**，**7%**確認**損失多於100萬美元** |
| 中國大陸受訪者表示，他們被要求**支付賄款**的可能性較香港受訪者**高五倍**、亦較亞太區和全球平均比例**高一點五倍** | **99%**的受訪者相信**網絡罪行**的風險將維持不變或有所增加 |
| 曾面對經濟罪案的受訪者中，**48%**表示他們主要在選擇供應商/承包和投標程序的過程中曾面對**採購舞弊** | **14%**的受訪者相信有機會受**網絡罪行攻擊**，而**亞太區及全球**的受訪者則分別有**26%及30%** |
| 受訪者中，26%表示**沒有使用舉報熱線**，但**78%**認為**熱線有效** | 所有受訪者中，**28%**表示他們的機構**沒有進行風險評估**，**10%**表示他們**不清楚企業有沒有進行風險評估**。而**沒有進行風險評估**的受訪者中，**47%不知道**風險評估涉及哪些內容 |

是次調查的所有議題正值中國大陸當局進行各類反貪腐運動，包括禁止政府官員使用公帑購買禮物和支付餐費和阻止私營公司進行不當行為。國際方面，美國司法部和證券交易委員會正積極執行反海外腐敗法（FCPA）。不少執法行動均牽涉多家中國大陸的附屬公司，導致這些企業聲譽嚴重受損，並須面臨罰款及非法得益等經濟損失。

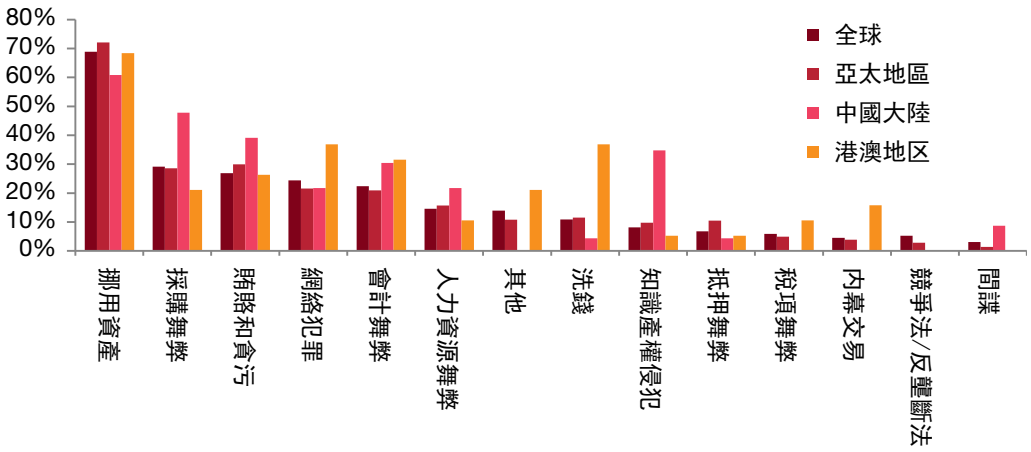
此外，於2011年頒布的英國反賄賂法（UK Bribery Act），其執法仍處於早期階段，因此對許多公司來說，看似有較少的即時影響。有三分之一的中國大陸受訪者表示，他們不認識英國反賄賂法（UK Bribery Act）或不知道他們公司應如何應對。儘管如此，英國反賄賂法對於關鍵市場營運的機構影響深遠，值得重視。

隨著中國大陸以及全球日益增加的監管活動，經濟罪行得到前所未有的關注，越來越多公司正加強他們的合規計劃及相關部門。但是，本調查結果反映中國大陸以及全球的機構於這方面有改善空間。

## 各欺詐案類型

在中國大陸，香港及澳門，挪用資產仍然是最常見的欺詐類型，與全球結果相符。曾遇上經濟罪案的中國大陸受訪者表示採購舞弊為第二常見，當中48%曾經歷採購舞弊。在中國大陸，緊隨其後的是賄賂和貪污及侵犯知識產權；在香港及澳門，則為洗黑錢及網絡罪行。

**圖表1: 欺詐案類型**



# 公司有否採取足夠措施防止及偵查經濟罪行？

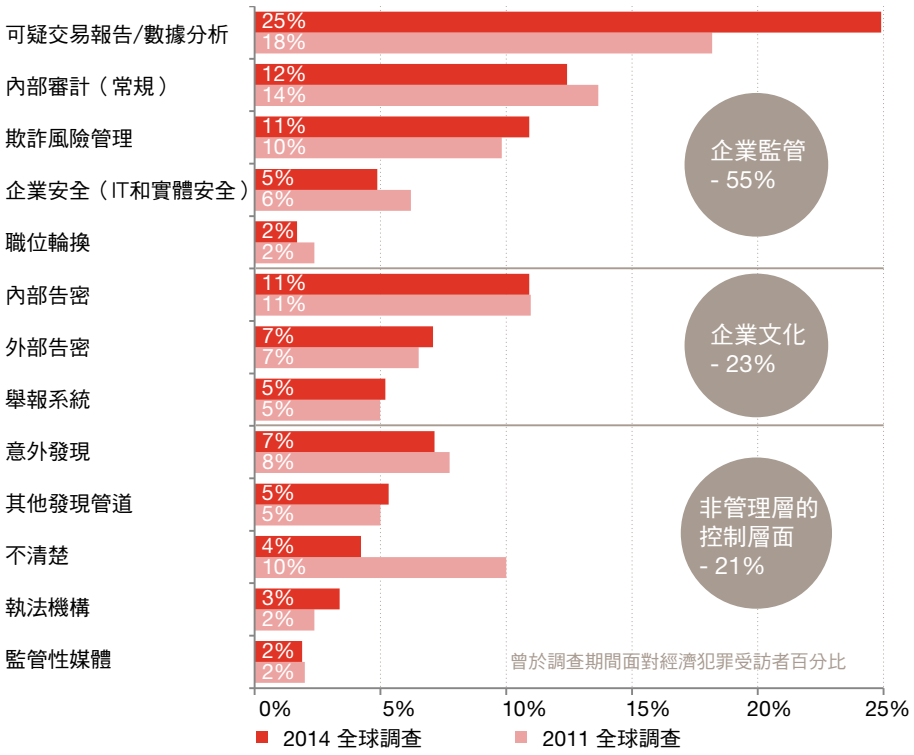
## 主動與被動

這次調查有關的結果出人意表，促使我們關注防止及偵查經濟罪行的措施是否如預期般有成效。

47%的香港及澳門設有舉報熱線的機構受訪者及26%的中國大陸設有舉報熱線的機構受訪者表示這些系統並從未被實際使用。此外，只有5%的港澳受訪者表示舉報熱線曾有效揭發經濟罪案，中國大陸則無任何這類的案例。

另外，港澳受訪者表示可疑交易分析（STA）/數據分析技術只揭發5%的經濟罪案。這調查結果與國際調查結果並不一致。國際調查結果顯示，在受訪者曾經歷最嚴重的經濟罪案中，STA/數據分析技術是最常用於檢測犯罪的方法，此類分析目前有效地檢測25%的犯罪行為（圖26[4]所示）。在2011年的調查中，STA有效地掀出18%的經濟罪案，顯示出該方法愈趨普遍。香港及澳門市場應以此為鑑，讓數據分析技術在檢測經濟罪行的過程中擔當更重要的角色。

**圖26: 發現最嚴重經濟犯罪的方法**




*自2014年，新增數據分析分類

## 對風險的了解？

有趣的是，香港受訪者中，28%聲稱他們公司沒有進行任何風險評估，他們當中有近一半人（47%）表示不清楚舞弊風險評估所包含的內容。另外，亦有10%的受訪者稱他們不了解公司有沒有進行風險評估。

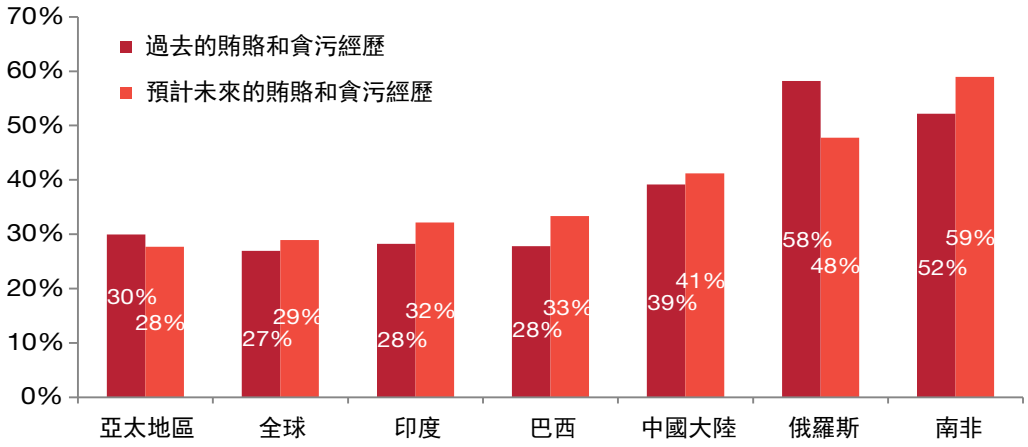
4. 摘錄自「羅兵咸永道2014年全球經濟犯罪調查 (GECS)」

# 賄賂、腐敗和“內部人員作案”風險

儘管GECS充份反映出香港及澳門在當下社交媒體時代面臨的網絡犯罪危機，中國大陸受訪者卻不為所動，傳統的舞弊詐騙行為才是他們着眼之處。39%曾舉報經濟罪案的中國大陸受訪者回覆他們曾經歷賄賂及貪污罪行，41%受訪者預計此情況將持續增長，雖低於俄羅斯（48%）和南非（59%），但仍較巴西（33%）、印度（32%）、亞太地區（28%）和全球（29%）為高。

國際間及本地持續的反貪腐立法工作相信已成功提高中國機構對貪污罪行的意識和敏感度。事實上，中國受訪者表示他們被要求支付賄款的比率為香港受訪者的五倍，亦較亞太地區和全球受訪者高一點五倍。其他金磚四國中只有俄羅斯的受訪者較中國經歷更多的受賄要求（參見圖表2）。

**圖表2：預期及經歷過的賄賂和貪污**



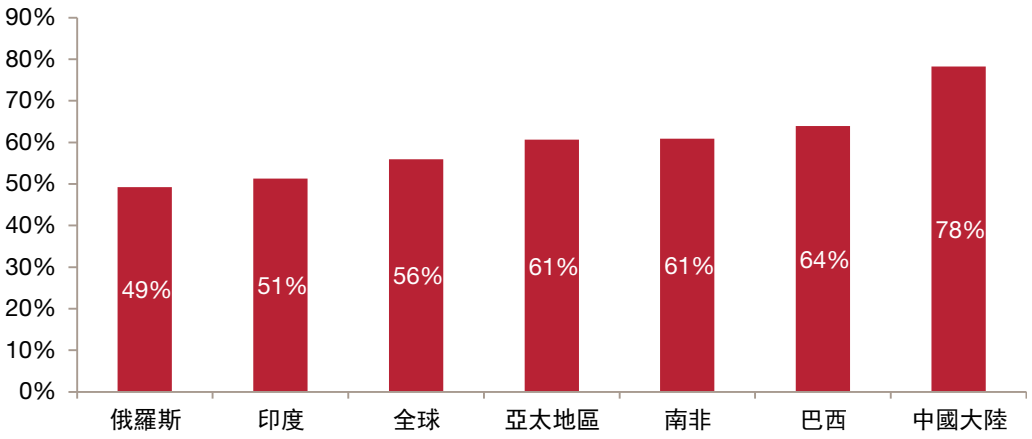

## 內部隱憂

調查更指出，在中國大陸，每五宗所呈報的經濟犯罪個案就有接近四宗的罪犯查明為機構內部員工。如圖表3所示，這一比例遠較其他國家為高。受訪者進一步透露這些「肇事者」中約28%年齡為30歲以下。

內部欺詐罪行在中國大陸比其他金磚四國更見普遍，依次為：巴西（64%）、南非（61%）、印度（51%）和俄羅斯（49%）。發生內部欺詐行為通常揭示機構的內部監控存有漏洞。許多機構已為加強內部監控系統而投放資源，但似乎仍有改善空間。

受訪者透露，22%經濟罪案「肇事者」在涉案機構內工作不到兩年時間。惟中國勞動人口流動性高，就業者在機構服務年期稍短屬正常現象。有鑑於此，我們是否該重新審視就招聘人才所進行的盡職調查？

**圖表3：「內部人員作案」發生情況**




## 僱主當心

經濟罪案的經歷或多或少反映了製造業、能源業以及重工業作為中國崛起成為環球經濟勢頭的奠基石之運作原理。這些行業背後的供應鏈甚為複雜，加上地方執法不一致，相比其他發達經濟體系更易讓貪污賄賂有機可乘。

除此之外，33%曾發生內部欺詐行為的受訪者表示其公司只曾訓斥或向詐騙者作出工作或職位上的調動。常言道捉賊要拿贓，可是要證明僱員涉及欺詐行為絕非易事。案件發生時，資方往往最關心的是保障機構聲譽和如何能不動聲色的擺脫害群之馬。於是，不法之徒可能（大多數在結清工資後）悄然離職，甚少留下任何公開的犯罪記錄。在缺乏公開記錄的情況下，下一位僱主則肩負起在招聘過程中嚴格篩選僱員的重任，防止詐騙者輕易進入另一職場再次作奸犯科。

最後，超過四分之一的中國大陸受訪者指他們公司的舉報熱線於調查期間從未被使用，但78%指其熱線電話效用為輕微到非常有效。一般來說，僱員若對其獨立性予以信賴，配合充分宣傳和鼓勵，則大型機構的舉報熱線應被廣泛及恰當使用。

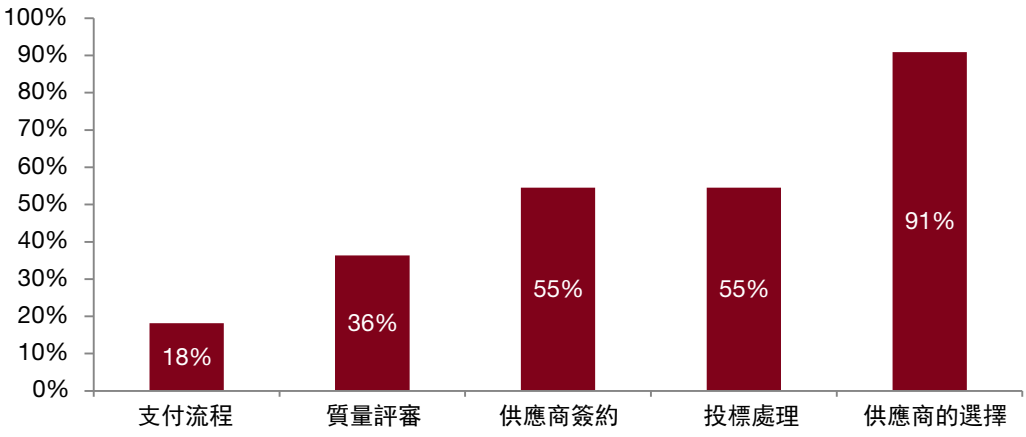
機構需設立24小時以中文操作的舉報渠道，包括電子郵件、傳真及電話，並需為有效、獨立且被員工信賴，以達致持續運作的目標。26%中國大陸受訪者的舉報機制在兩年調查期間從未被使用，及這些系統未能交代任何經濟罪行的檢測結果，足以證明機構需多下功夫改善這相對直接且簡易的機制。

# 採購舞弊—中國大陸受訪者最常見經濟罪行之一

採購舞弊是系統性的，能夠對機構造成長遠而巨大的破壞。採購舞弊於依賴供應鏈的機構中最為常見，隨機構參與商業或公開招標、尋求商品和服務供應而增加。

因執法不一致和欠缺透明度的營商環境，賄賂和貪污的風險相應提高。中國大陸的機構在挑選供應商（佔採購舞弊的91%）、供應商承包（55%）和投標過程（55%）三個階段遇到較大的採購舞弊威脅（參見圖表4）。

**圖表4：中國大陸地區採購階段舞弊的發生情況**

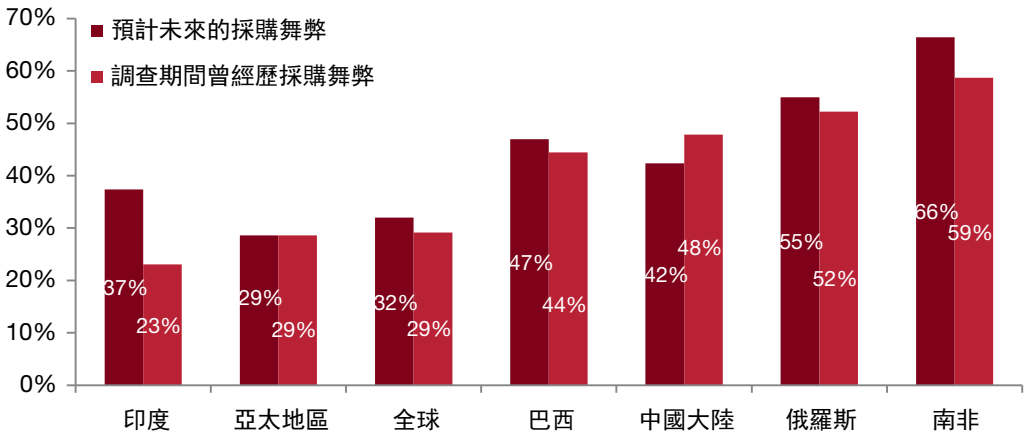


## 回佣，貪污和內控

因此，採購舞弊是中國大陸受訪者認為最常見的經濟罪行之一。48%曾有經濟罪案經歷的受訪者曾遇上採購舞弊，比亞太地區和全球範圍內錄得的結果顯著較高（兩者皆為29%）。

採購舞弊涉及員工收受回佣等非法行為。其發生表明機構的內部監控存有漏洞，欠缺透明度，和對供應商與員工之間的關係監管不足。這亦印證於較早有關賄賂和貪污的篇幅中，受訪者指出每五宗所呈報的經濟犯罪個案便有將近四宗案件為公司內部員工作案的調查結果。

**圖表5：預期或曾經面對有關採購舞弊的經歷**

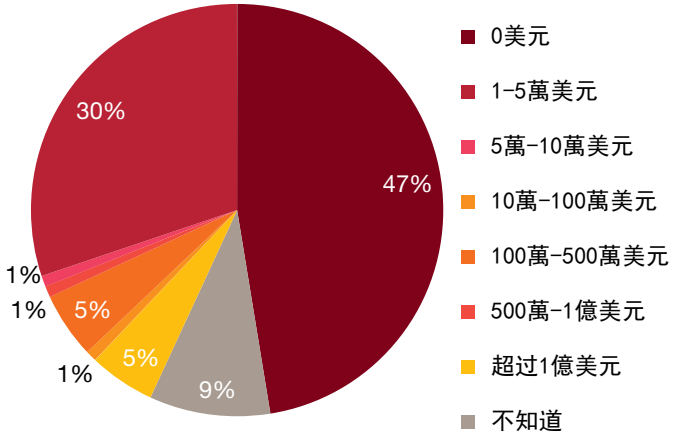


# 面對網絡罪行威脅日益增長，香港及澳門受訪者仍抱有信心

網絡罪行難被發現，加上棘手的處理方法，成為現代機構要面對的其中一項最具威脅和最不為人所理解的經濟罪行，以致機密資料有機會被非法獲取。許多情況下，機構往往不知道它們已經成為攻擊對象，待察覺到任何欺詐行為已為時已晚。

正因當地眾多機構依賴資料數據庫協助日常營運，港澳兩地的受訪者皆認為網絡罪行帶來日趨嚴重的威脅。37%曾舉報經濟罪案的港澳受訪者表示他們有面對網絡罪案的親身經歷。當中九成受訪者稱最憂慮機構因此聲譽受損，蒙受經濟損失和需承擔規管風險。此外，所有港澳受訪者中，有7%的人表示其公司因網絡罪案損失多於100萬美元（參見圖表6）。

**圖表6：網絡罪行在香港及澳門引致的經濟損失估算**




## 高科技，高賭注，和高風險

從以上分析來看，不難明白99%的香港受訪者認為香港的網絡犯罪風險將維持不變或有所增加至100%。新加坡也有類似情況。

然而，只有14%的香港和澳門受訪者認為他們機構將在未來24個月會受網絡罪行攻擊（新加坡為11%）。30%的全球和26%的亞太地區受訪者同意其所屬機構正面臨網絡攻擊的危機，比例大幅高於香港。

就香港及澳門日益嚴重的網絡威脅，香港警務處提供了進一步的數據予以支持。網絡犯罪案件由2012年的3,015宗上升至2013年的5,133宗，升幅逾七成。這主要歸咎於電子郵件詐騙案的顯著增加，從2012年的430宗引致共1.8億港元商業損失，大幅躍升至2013年的1,153宗，造成約7.6億港元損失[5]。

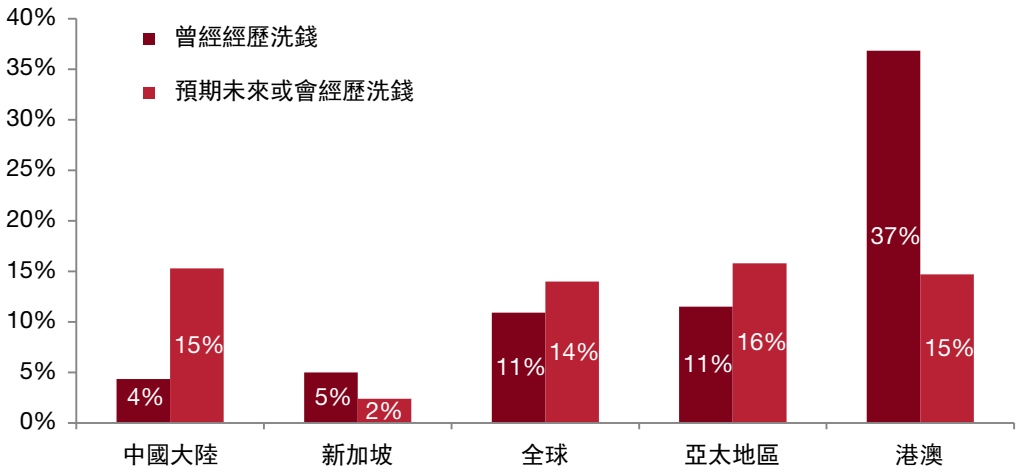
5. 香港警方記者招待會
http://www.police.gov.hk/ppp_en/01_about_us/cp_ye.html

# 經濟罪行反映行業焦點

本調查突出洗黑錢對全球各行業所帶來的風險，尤其針對金融行業。香港及澳門的受訪者皆表示洗黑錢是常見的經濟罪行。由於多間銀行和金融機構在香港營商，洗黑錢為各項經濟罪行中對香港受訪者構成更顯著的威脅。同樣地，洗黑錢也是澳門龐大的博彩業的擔憂之處。

據調查，曾經歷經濟罪案的港澳受訪者中，37%指出他們曾面對洗黑錢的威脅。這比率顯著高於其他亞太地區國家。

**圖表7：預期或曾面對洗黑錢的經歷**




## 過分自滿或故步自封？

儘管相對較多的受訪者表示曾遭洗黑錢帶來的損失，然而受訪者對未來所面對的風險仍抱持較樂觀的態度。我們並不清楚這正面的看法是因為受訪者對機構的反洗黑錢措施成效抱有信心，或是因為他們對該等措施過分自滿。但是，只有15%的受訪者預期將來會面對洗黑錢罪行，而75%認為再經歷洗黑錢的可能性不大。

## 調查方法

羅兵咸永道在2013年8月至2014年2月期間進行「全球經濟犯罪調查」。本調查包括一份儲於加密網站而全球可連結的問卷。對調查作出回覆的高級管理人員瀏覽該網站，並回答了以下四個部分的問題：

- 有關機構的大致背景
- 針對面對經濟罪案經歷的機構作出比較
- 分析網絡欺詐的威脅
- 貪污/賄賂、洗黑錢及競爭法/反壟斷法

## 關於全球經濟犯罪調查

共有201名受訪者參與「2014年GECS-中國大陸、香港及澳門補充文件」的調查（85名受訪者來自中國大陸及116名受訪者來自香港及澳門）。

- 51%中國大陸受訪者和53%香港及澳門受訪者為機構的高級管理人員。
- 55%中國大陸受訪者和49%香港及澳門受訪者代表上市公司參與調查。
- 70%中國大陸受訪者和64%香港及澳門受訪者代表聘用超過1,000名員工的機構。

我們使用了以下研究方法：

1. 機構高級管理人員調查：從這些管理人員在其機構所面對的經濟罪行經驗，我們得出了是次調查結果。從他們的回覆中，我們得到各類型經濟罪行的資訊，如經濟罪案對公司造成的經濟及其他附帶損失、經濟犯罪的涉案者、公司面對經濟罪案而採取的相應行動等。

2. 有關網絡罪行、賄賂和貪污、洗黑錢和競爭法/反壟斷法的問題：由於這些問題的出現一般較為有系統性，並可對不同機構造成長遠兼具破壞力的威脅，本次調查對這些問題進行了深入的詳細探討。

3. 與其他具有相似經濟條件的國家進行比較：我們比較了新加坡與香港及澳門的調查結果；中國大陸則與其他金磚國家（巴西，俄羅斯，印度和南非）的情況進行比較。這些比較有助我們分辨出任何不一致的情況及其他重要事項。

4. 經濟罪行在本調查中被定義為「蓄意欺騙以剝奪金錢，財產或法律權利」。

5. 雖然調查問題對受訪者提出有關的行業，地域及機構經營規模的一般性問題，受訪者能以匿名回應調查。

見www.pwc.com/ crimesurvey以參閱全球調查報告。

# 聯絡我們

## 香港

**董家俊 (John Donker)**
合伙人
中國大陸和香港法務會計服務主管
+852 2289 2411
john.donker@hk.pwc.com

**Megan Haas**
法務會計服務, 合伙人
+852 2289 1911
megan.l.haas@hk.pwc.com

**劉甄甄 (Antoinette Lau)**
法務會計服務, 合伙人
+852 2289 2403
antoinette.yy.lau@hk.pwc.com

## 上海

**盧迅然 (Jean Roux)**
法務會計服務, 合伙人
+86 (21) 2323 3988
jean.roux@cn.pwc.com

**Ramesh Moosa**
法務會計服務, 合伙人
+86 (21) 2323 8688
ramesh.moosa@cn.pwc.com

## 北京

**麥健倫 (Brian McGinley)**
法務會計服務, 合伙人
+86 (10) 6533 2171
brian.mcginley@cn.pwc.com

*www.pwc.com/crimesurvey*

© 本文僅為提供一般性資訊之目的, 不應用於替代專業諮詢者提供的諮詢意見。

© 2014 羅兵咸永道。版權所有。羅兵咸永道乃指羅兵咸永道網絡香港成員機構，有時也指羅兵咸永道網絡。每家成員機構各自獨立。詳情請瀏覽 www.pwc.com/structure。

# 经济犯罪：内在危险

## 4/5

在中国大陆地区，报告的经济犯罪中，有五分之四是“内部人作案”。

## 39%

在中国大陆地区，39%曾经历犯罪的受访者表示他们经历过腐败和贿赂。

## 99%

在港澳地区，99%的受访者表示他们认为网络犯罪的风险与过去相同或有所提高。

# 目录

# 前言

我们很荣幸为您呈现普华永道2014年全球经济犯罪调查（GECS或本调查）中国大陆及港澳地区专刊。

今年的全球经济犯罪调查体现了来自95个国家的5，000多个受访者对目前经济犯罪普遍发生的现状以及未来趋势走向的观点。

在中国大陆及港澳地区专刊中，我们收集了85位来自中国大陆、116名来自港澳地区高层管理人员的反馈，根据受访者提供的来自过去24个月中，他们与经济犯罪相关的经历为依据，对当地受访者所面临的问题进行了集中的讨论与分析。

本调查报告显示，中国大陆与港澳地区的企业所面临的挑战，在一些领域与世界其它地区基本一致；然而在另外一些领域也有所差异。我们在文中会对这些差异进行详细的描述。

本调查报告的结果不是决定性的，也不能为在这些市场中经营的机构提供解决方案以应对与经济犯罪相关的挑战。但本报告的确揭示了一些有关网络犯罪、腐败和贿赂、采购舞弊和洗钱的关键性问题。这些问题与正致力于建立或加强经济犯罪风险防范体系以降低风险的机构息息相关。

本报告揭示的问题和得出的结论并不全是负面的。例如，只有5%的港澳受访者表示他们曾被要求去行贿，这个比例低于地区及全球平均水平近四倍。

同时，中国大陆受访者举报经济犯罪的比重占27%，远远低于全球（37%）和美国（45%）的结果。虽然这一结果可以部分解释为中国大陆的机构缺乏经济犯罪侦查能力。

在本调查中，中国大陆有两个反复出现的主题表现得比较突出，分别是对腐败和贿赂问题的担忧以及对采购舞弊和回扣问题的担忧。

这两类问题都与贪污腐败问题有关，可能部分是由于中国大陆当局正在大力进行反贪污运动。此次运动已经对全国范围内182,000官员[1]进行了纪律处分并涉及了一些跨国企业（MNCs）及它们的外籍高管。

在中国大陆市场继续发展的同时，经济犯罪也将继续威胁各行各业的发展进程--包括建立商业关系，采购与销售，进口与出口，支付与收款。

1. http://news.xinhuanet.com/english/china/2014-01/10/c_133034868.htm

# 全球情况

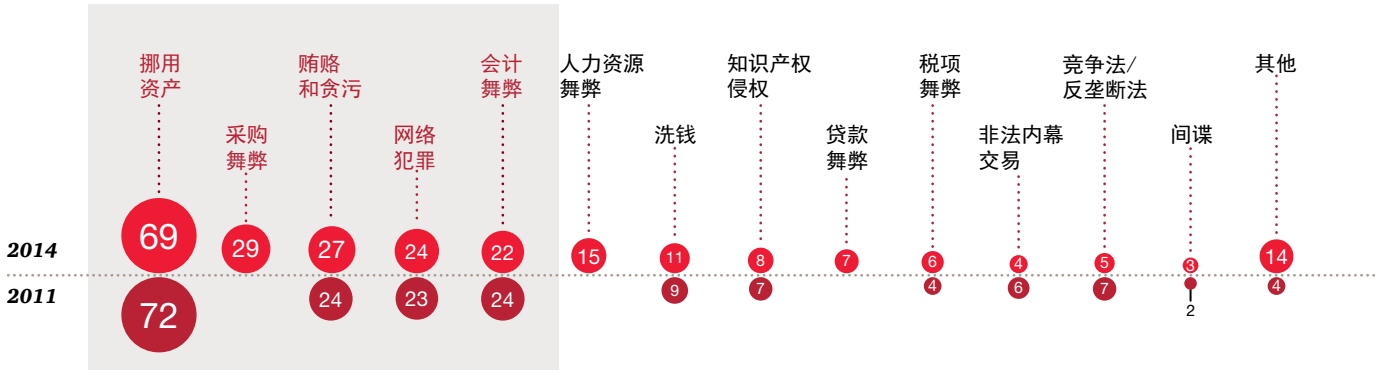
## 舞弊的形式

自2001年我们初次开展经济犯罪调查以来，受访者们一直反复强调三种舞弊形式，分别是挪用资产（一直占最大比重），腐败和贿赂以及会计舞弊。网络犯罪在2011年被新增为一个单独的分类。

今年，采购舞弊也被新增为一个类别。我们认为这是由两种趋势造成的--来自政府及国有企业的公开招标流程竞争日趋激烈，以及供应链逐步融入核心商业活动。

从图3[2]中可以看出，受访者指出采购舞弊是他们所经历的第二常见的舞弊行为。

**图3：各欺诈案类型**

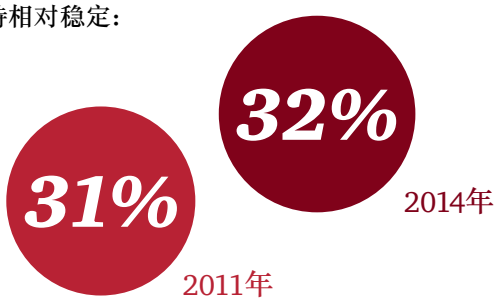



曾于调查期间面对经济犯罪受访者百分比

2. 摘自普华永道2014年全球经济犯罪调查

## 地区的事例：

近两次调查中，亚洲及太平洋地区经历过经济犯罪的被调查受访者数量保持相对稳定：

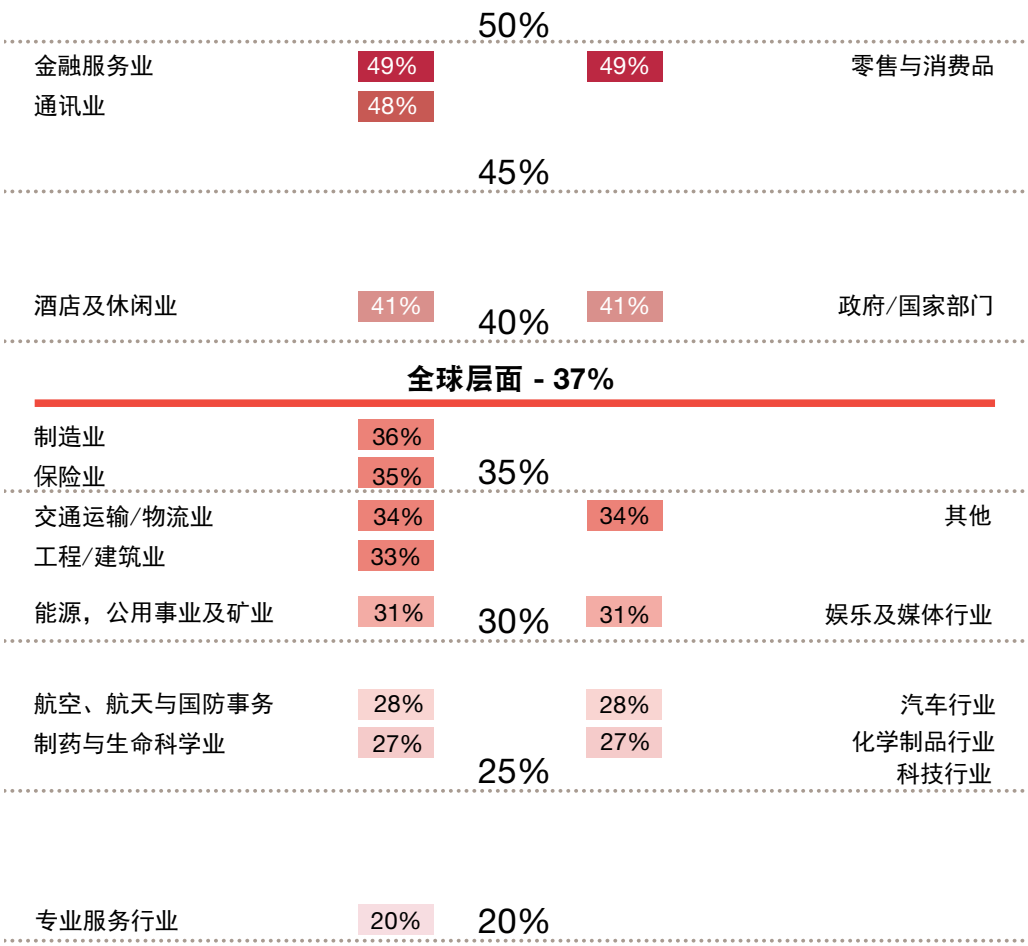



有趣的是，“新兴八国”（巴西，中国大陆，印度，印度尼西亚，墨西哥，俄罗斯，土耳其和南非）报告的舞弊有所增长，从2011年调查中的35%增长至2014年的40%。

## 行业中的经济犯罪

中国大陆地区，港澳地区各行业的集中度有所不同，但是从下面的图5[3]中显示出，每个地区都会受到在此调查中报告经济犯罪最多的前五位个行业的影响。

**图5:行业经济犯罪发生率**




曾于调查期间面对经济犯罪受访者百分比

3. 摘自普华永道2014年全球经济犯罪调查

## 要点

**27%的中国大陆的受访者和16%港澳地区的受访者指出他们都曾遇到经济犯罪，与此相比，该比例在亚洲及太平洋为32%，在全球为37%。**

# 地区情况

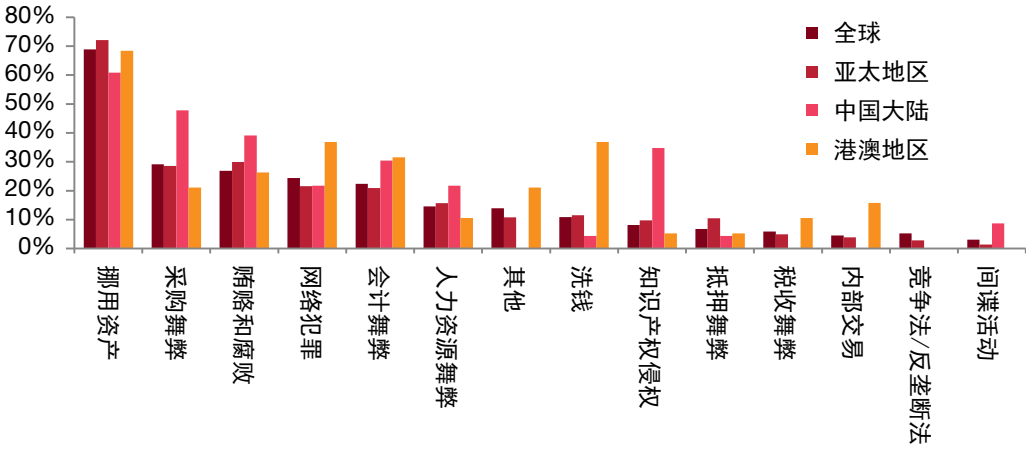
| 中国大陆地区 | 港澳地区 |
| --- | --- |
| 受访者表示报告的经济犯罪中，有**五分之四是“内部人作案”** | 受访者中，洗钱活动受害者的比例是地区及**全球水平的3倍** |
| 受访者表示**28%**的内部舞弊人员年龄在**30岁以下，22%**在本公司工作经历**少于2年** | **37%**报告过经济犯罪的受访者表示他们经历过洗钱，但其中只有15%的受访者认为在未来**24个月中洗钱会再次影响他们** |
| **39%**曾经历犯罪的受访者表示他们经历过**腐败和贿赂**，其中**41%**的人预期这个比重会有所增长 | 在遭受经济犯罪的受访者中，**有37%的人经历过网络犯罪，7%的人承认损失超过一百万美元** |
| 中国大陆的受访者表示他们被要求行贿的可能性是香港被调查人员的**5倍**，是地区及全球平均水平的**1.5倍** | **99%**的受访者表示他们认为**网络犯罪**的风险与过去相同或有所提高 |
| **48%**的遭受过犯罪的受访者表示他们遇到过**采购舞弊**，主要发生在供应商的选择/签约以及招标过程阶段 | **14%**的受访者表示他们认为受到**网络犯罪**攻击的可能性很大，相比较而言，**地区比率为26%，全球比率占30%** |
| 26%的受访者表示**检举热线未被使用过**，但仍有**78%**的人认为这种方式是有效的 | 在所有受访者中有**28%**表示他们的公司**不会进行风险评估，10%表示他们不清楚公司是否进行风险评估**。在那些表示**不会进行风险评估**的受访者中，有**47%**的人**不知道**风险评估涉及哪些内容 |

在本调查中报告的所有主题均出现在中国大陆当局推动反腐运动的大背景下，其中包括严禁政府官员使用公款购买礼品和宴请，以及民营企业的不当行为。在国际上，美国司法部和证券交易监督委员会已经大力度地强制执行《海外反腐败法》（FCPA）。其中的很多强制行为包括大量专门针对中国大陆地区制定的组成部分，这使得公司的声誉严重受损，更不用说通过罚款和追缴非法所得带来的经济损失。

此外，由于最近的在2011年被公布的英国《反贿赂法》仍处于初级阶段，因此，对于许多公司都没有太大的直接意义，然而它仍可能对那些在重要市场经营的机构产生其他深远的影响，因而值得高度关注。但是三分之一的中国大陆受访者表示他们不知道英国反贿赂法或者不清楚他们的公司是如何应对这条法律的。

面对中国大陆地区以及全球范围内越来越强的监管活动，经济犯罪的风险达到了前所未有的高度。越来越多的公司正在加强合规计划以及新增合规部门。然而本调查显示，面对经济犯罪我们要做的还有很多。

**表1: 舞弊的形式**




在中国大陆以及港澳地区，挪用资产仍然是经济犯罪中最常见的舞弊形式，此结果与全球调查的结果相一致。在中国大陆，所在机构遭受过经济犯罪的受访者表示，采购舞弊在经济犯罪数量中居第二位，其中48%的受访者指出他们亲身经历过采购舞弊。在中国大陆地区，紧随采购舞弊之后的是贿赂和腐败以及知识产权侵权，在港澳地区则是洗钱与网络犯罪。

# 公司在防御和侦查经济犯罪方面是否做得足够?

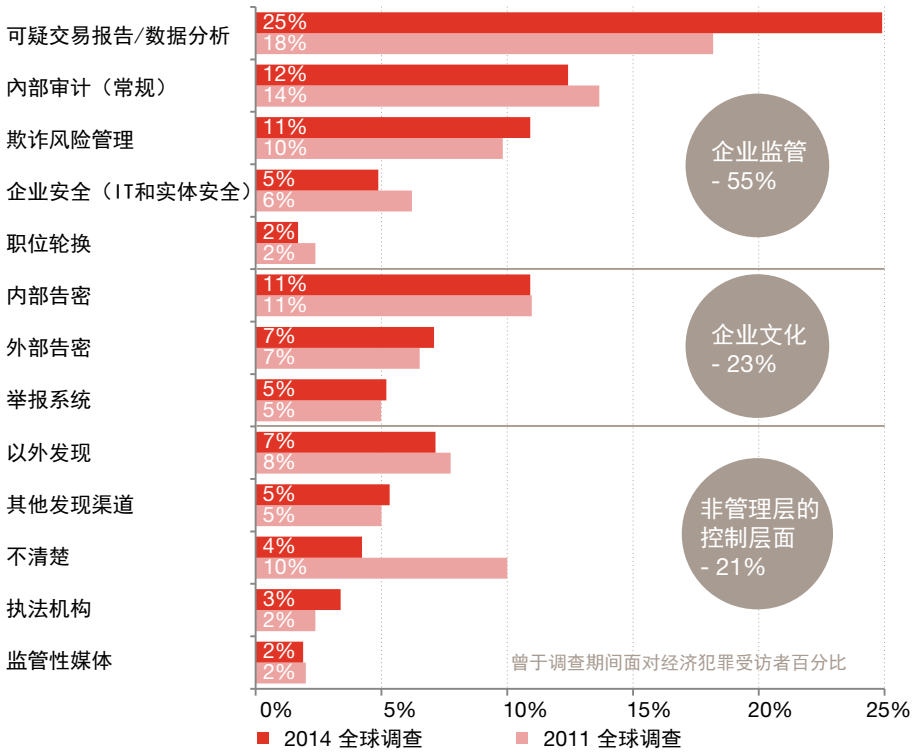
## 主动与被动

在本调查中，有些结果令人颇感意外，有些结果令人担忧是否一些正在使用的侦查手段像我们想象的那样有效。

在那些有检举热线的机构中，有47%的港澳地区受访者以及26%的中国大陆受访者表示这些举报系统完全没有被使用，而且只有5%的港澳地区受访者表示通过检举热线侦查到了经济犯罪，中国大陆则没有。

此外，港澳地区的受访者报告说只有5%的经济犯罪是通过可疑交易分析（STA）/数据分析手段侦查出来的，这是一个与全球调查结果截然不同的观点。在全球范围内，受访者认为25%的严重的经济犯罪是通过可疑交易分析（STA）/数据分析手段侦查出来的。这一比例高于其它手段（见图26[4]）。在我们2011年的调查中，通过可疑交易分析（STA）侦查出的经济犯罪占18%。这意味着这种侦查手段的应用在这些年呈增长趋势。对于港澳市场，这是一次提升数据分析技术从而发现经济犯罪的机会。

**图26:发现最严重经济犯罪的方法**




*自2014年，新增数据分析分类。

## 你明白这些风险吗?

有意思的是，28%的香港受访者声称他们的公司不进行任何风险评估，有10%表示他们不知道公司是否有进行风险评估。在这些表示没有进行过任何风险评估的受访者中，几乎有一半（47%）表示他们完全不知道风险评估涉及哪些内容。

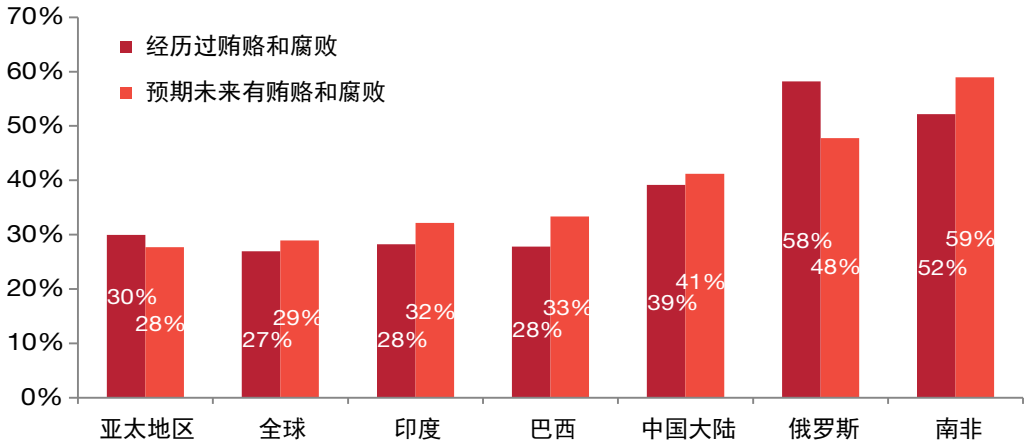
4. 摘自2014普华永道全球经济犯罪调查

# 贿赂、腐败和“内部作案”的风险

港澳地区网络犯罪的威胁在全球经济犯罪调查中有所体现；尽管网络犯罪风险在如今社交媒体的时代真实存在，但中国大陆受访者对此不太关注，因为他们更为关心比较传统的舞弊行为。39%的报告过经济犯罪的中国大陆受访者表示他们经历过一些形式的贿赂和腐败，41%预期贿赂和腐败的情况还会增加，这一比率虽然比俄罗斯（48%）和南非（59%）低，但是显著高于巴西（33%）、印度（32%）、亚太地区（28%）和全球（29%）。

在中国大陆地区，国内和国际上反腐败立法的持续执行有可能提升了公司对贿赂的意识以及敏感度。的确，中国大陆的受访者表示他们被要求行贿的可能性比香港受访者多5倍，可能比亚太地区和全球多1.5倍。在其他金砖五国中，只有俄罗斯受访者被要求行贿的次数比中国大陆多（见表2）。

**表2：预期及经历过的贿赂和腐败**



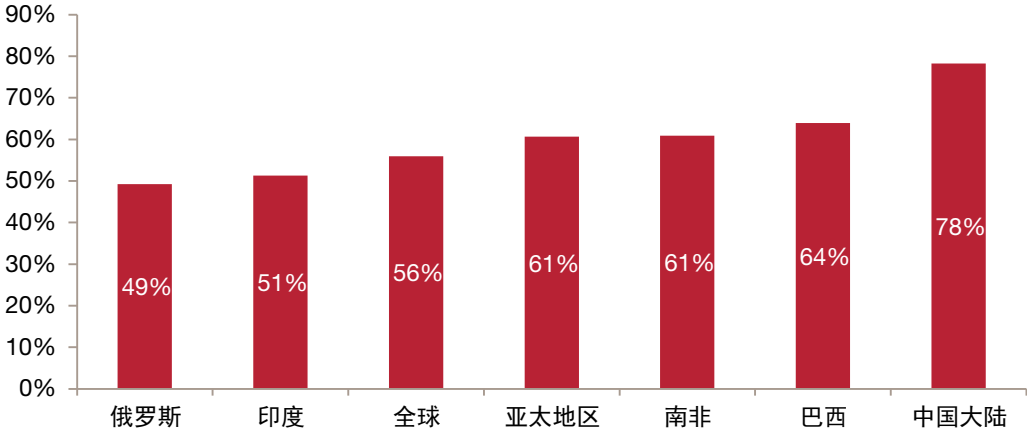

## 内部威胁

调查也表明，在中国大陆，几乎五分之四被报道的经济犯罪的作案者都是内部员工。如表3所示，这一比例显著高于比其他对比国家。根据我们的受访者提供的情况，对于这些内部人作案的进一步分析揭示出28%的作案者小于30岁。

据调查，中国大陆内部舞弊的比例明显高于其他金砖五国，其中巴西为64%、南非为61%、印度为51%、俄罗斯为49%。这些内部舞弊很有代表性地显示了机构中内部控制的缺陷。很多机构已经投资并加强了他们的内部控制，但看起来仍有相当大的提升空间。

受访者表示经济犯罪中有22%的作案者在该公司工作少于两年，不过这对中国大陆的员工流动性来说并不为奇。考虑到这一点，拓展业务时或许我们应该问自己我们对需要的雇员应做哪些尽职调查？

**表3: 发现的内部人作案**




## 雇主要当心

经济犯罪的经历也能部分地反映在制造业、能源和重工业基础上，这些基础行业支撑中国发展为全球经济强国。这些行业的复杂的供应链容易受到贿赂和腐败的影响，与发达国家相比，现有法规的执行不一致性也使贿赂和腐败更为严重。

另外，在确认的内部舞弊实例中，33%的受访者表示他们的公司只会谴责和调离舞弊者。证明员工舞弊不是一件简单的事情。事情发生时，雇主通常会最关心企业声誉，选择不动声色地摆脱害群之马。同样地，舞弊者也许会悄然地辞职（通常是付清工资之后），留下很少甚至不留下他们非法行为的公共记录。在中国大陆，公共记录的缺失会让可能继任的雇主有责任进行严格的员工筛选，否则舞弊者可能或相对容易地从一个职位转到另一个职位。

最后，超过四分之一的中国大陆受访者表示他们的检举热线在调查期间没有被用过，78%的受访者认为他们的检举热线从略微有效到十分有效不等。在规模较大的机构里，有效的检举热线只要能够被有效推广并且其独立性为员工所信任，就能够被经常地使用。

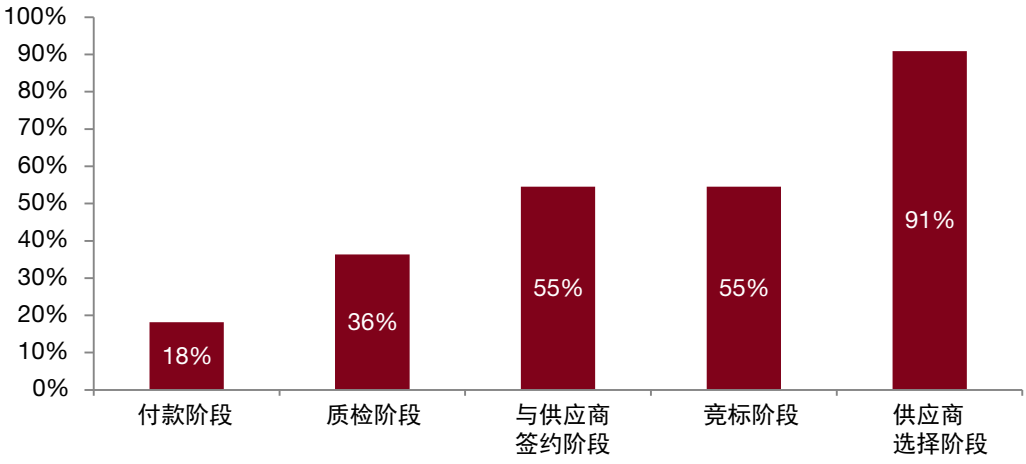
机构也需要有效、独立并且可信的检举热线，比如邮件、传真和电话等，要提供24小时的中文服务并且能持续使用。事实上，在调查进行的两年间，中国大陆受访者表示他们26%的检举机制从来没有被使用过，而且认为这些系统在检测经济犯罪方面没有作用。这表明改善这种相对直接的系统任重道远。

# 中国大陆受访者经历最多的经济犯罪之一：采购舞弊

采购舞弊本质上是系统的，能够对机构有长远且重大破坏性的影响。采购舞弊通常与供应链依赖型企业紧密相关，在机构进行商业或者公开招标或者采购商品和服务的时候，采购舞弊发生的可能性就会增加。

法规执行不一致与缺乏透明度的经营环境会加强贿赂和舞弊的风险。中国大陆的机构在以下阶段可能会面临更大的采购舞弊威胁：供应商选择阶段（占实例的91%）、与供应商签约阶段（55%）以及竞标阶段（55%）（见表4）。

**表4：中国大陆地区采购阶段舞弊的发生情况**

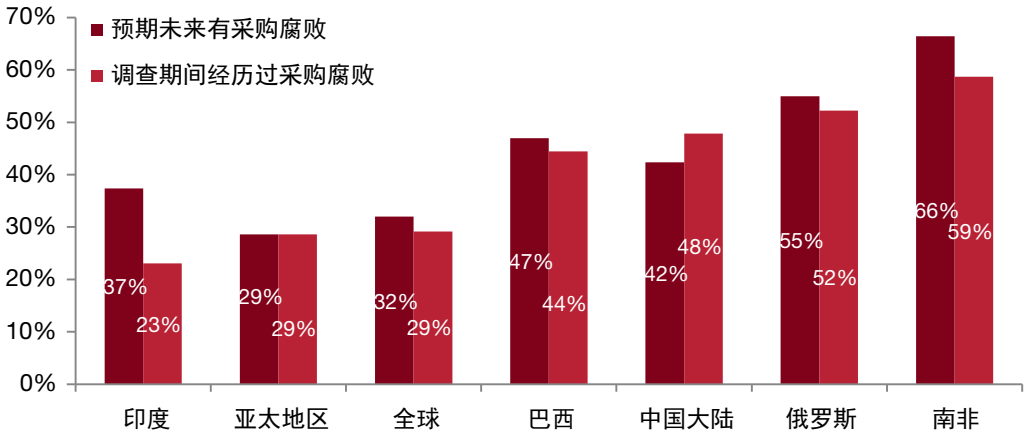


## 回扣，腐败和内控

采购舞弊被中国大陆受访者认为是最经常经历的经济犯罪之一，这并不令人惊讶。48%的遭受过经济犯罪的受访者遇到过采购舞弊，这一比例显著高于亚太地区和全球的记录（两者均为29%）。

采购舞弊包括员工拿回扣以及其他非法安排等。它的存在有力地表明机构的内控薄弱，透明度缺乏，对供应商以及员工关系的监视有限等问题。这些问题支持了之前对贿赂和腐败的观察结果。根据受访者描述，五分之四的经济犯罪的作案者是该公司的员工。

**表5：预计的以及经历过的采购舞弊**

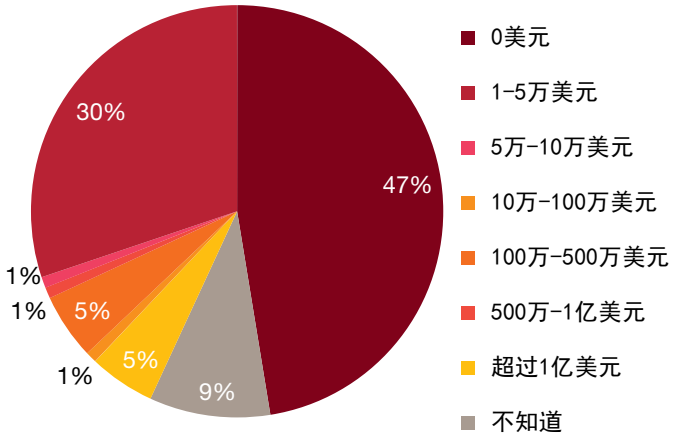


# 面对日益增长的网络犯罪威胁，港澳地区受访者表示很有信心

网络犯罪难以被侦查更难被解决，它对现代企业来说是最具威胁也最缺乏理解的经济犯罪之一。机构通常不愿披露诸如系统被入侵或者机密数据被非法获取之类的事件，因为这些事件可能会引发大量的声誉和商业问题。在许多情况下，公司通常意识不到他们已经成为了网络犯罪的目标，而且舞弊经常在犯罪已经发生之后才被发现。

也许是由于对数据的依赖性很强，港澳地区受访者把网络犯罪看作一种重大并日渐增长的威胁。37%的报告过经济犯罪的港澳地区受访者表示他们亲身经历过网络犯罪，并且有十分之九说他们最害怕网络犯罪导致声誉受损、经济损失以及监管风险。此外，在所有的港澳地区受访者中，有7%表示由于网络犯罪，他们的公司损失超过1,000,000美元（见表6）。

**表6：港澳地区网络犯罪导致的预计经济损失**




## 高科技，高投注和高风险

从以上分析来看，39%的香港地区受访者表示他们察觉到他们市场上的网络犯罪风险将会保持不变或有所增加，这并不令人吃惊；与之呼应，新加坡有100%的受访者有类似的担忧。

然而，只有14%的港澳地区受访者感觉他们的机构会在未来24个月内会遭受网络犯罪攻击（该比例在新加坡为11%）。这些数据都显著低于全球和亚太地区受访者的反馈。有30%的全球受访者和26%的亚太地区受访者认为他们的机构正面临网络攻击。

更多的关于港澳地区网络犯罪威胁日益增长的证据来自香港警方。香港警方透露，2013年网络犯罪有5,133起，比2012年的3,015起增加超过70%。电子邮件诈骗主要加剧了网络犯罪。2013年1,153起电子邮件诈骗对企业造成760,000,000港币的损失，与2012年430起造成180,000,000港币的损失相比有大幅增加[5]。

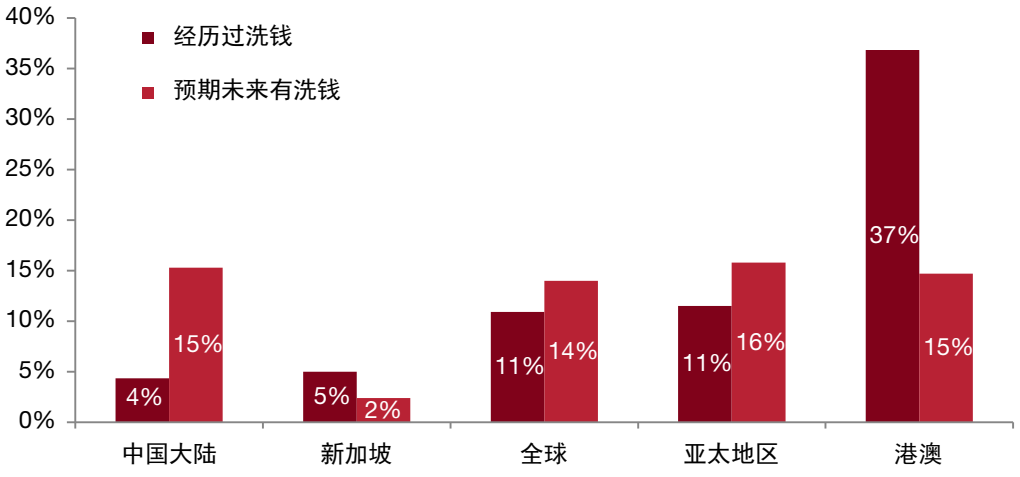
5. 香港警方记者招待会：http://www.police.gov.hk/ppp_en/01_about_us/cp_ye.html

# 经济犯罪反映行业焦点

本调查强调了洗钱对于全球企业的风险，特别是在金融领域。港澳地区受访者将洗钱视为经济犯罪的一种惯常形式。香港在银行和金融行业的专注也意味着洗钱诈骗对香港受访者来说是更重大的威胁。类似地，洗钱也仍是澳门广大博彩业的担忧之处。

据调查，在经历过经济犯罪的港澳地区受访者中，有37%的人将他们的经历指向洗钱。这个比例比其他地区都高很多。

**表7: 预计及经历过的洗钱**




## 是合理的自信还是自满?

即使认为自己机构有遭遇过洗钱的受访者的人数相对较多，受访者们对未来的风险还是持乐观态度。目前不太明确这种乐观是来自他们对机构成熟的反洗钱体系的自信还是揭示了他们的自满。但是只有15%的受访者表示他们预计未来会遭遇洗钱，有75%的受访者认为洗钱不太可能再次发生。

## 方法论

普华永道在2013年8月至2014年2月间进行了此次全球经济犯罪调查。本调查包括了一个在安全网址上全球均可访问的问卷，愿意参与调查的高层管理人员可以直接访问该网址来回答以下四方面的问题：

- 一般概要性问题
- 关于机构所经历的经济犯罪的比较性问题
- 网络舞弊威胁
- 腐败/贿赂、洗钱以及竞争法/反垄断法

## 关于本调查

《2014全球经济犯罪调查——中国大陆、香港和澳门专刊》有201名受访者参与（其中85名来自中国大陆，116名来自港澳地区）。51%的中国大陆受访者和53%的港澳地区受访者是他们所属机构的高层管理人员，55%的中国大陆受访者和49%的港澳地区受访者代表了上市公司，70%的中国大陆受访者和64%的港澳地区受访者代表了有超过1000名员工的机构。

研究技巧：

1. 调查对象是机构里的高层管理人员。调查结果都是来自高层管理人员们对其所属机构所经历过的经济犯罪的报告，我们从中获取的信息有：不同的经济犯罪类型、不同类型对机构的影响（包括经济损失和所有并发损失）、这些犯罪的作案者以及机构对犯罪采取何种措施和对犯罪作何反应。

2. 有关网络犯罪、贿赂和腐败、洗钱以及竞争法/反垄断法的问题。本调查认真分析了这些威胁。它们本质上具有系统性因而对机构更倾向有长期的破坏性。

3. 与其他具有类似经济状况的国家进行比较。我们通过将与相关的港澳地区相关的调查结果与新加坡进行比较，将与有关的中国大陆有关的调查结果与其他金砖五国（巴西、俄罗斯、印度和南非）进行比较，以此来帮助识别任何不一致或者发现的其他问题。

4. 在本调查中，经济犯罪指故意通过欺诈等手段使剥夺他人或机构丧失的金钱、财产资产以及合法权利等。

5. 虽然问卷里的一般概念性问题涉及行业、责任的地理划分以及企业运营规模等，但参与者可以匿名完成调查。

全球报告请参见：www.pwc.com/crimesurvey

# 联系方式

## 香港


**董家俊 (John Donker)**
合伙人
中国大陆和香港 法务会计服务主管
+852 2289 2411
john.donker@hk.pwc.com



**Megan Haas**
法务咨询, 合伙人
+(852) 2289 1911
megan.l.haas@hk.pwc.com



**刘甄甄 (Antoinette Lau)**
法务咨询, 合伙人
+ (852) 2289 2403
antoinette.yy.lau@hk.pwc.com


## 上海


**卢迅然 (Jean Roux)**
法务咨询, 合伙人
+86 (21) 2323 3988
jean.roux@cn.pwc.com



**Ramesh Moosa**
法务咨询, 合伙人
+86 (21) 2323 8688
ramesh.moosa@cn.pwc.com


## 北京


**麦健伦 (Brian McGinley)**
法务咨询, 合伙人
+86 (10) 6533 2171
brian.mcginley@cn.pwc.com

*www.pwc.com/crimesurvey*

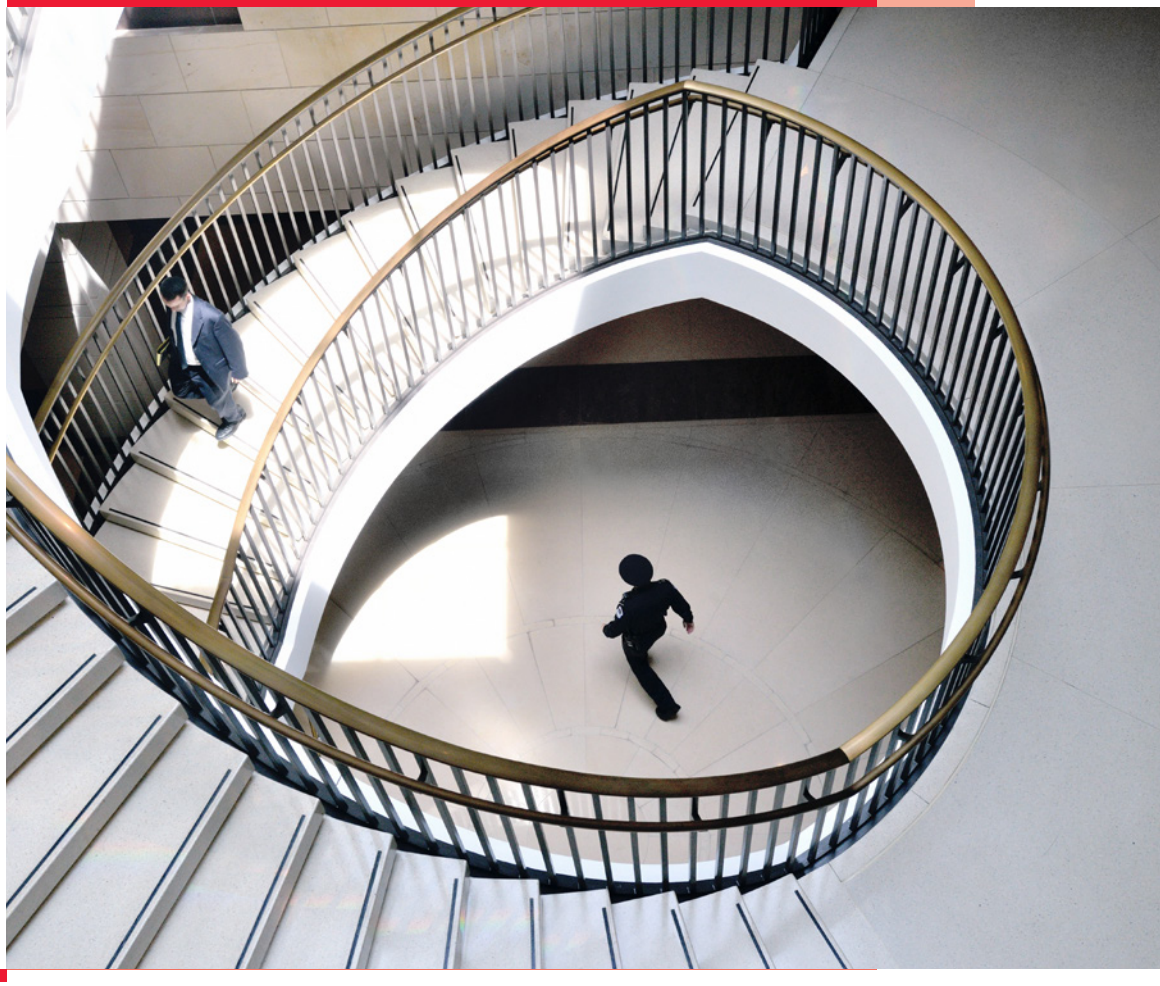
© 2014 普华永道管理咨询（上海）有限公司。 版权所有。普华永道系指普华永道网络中国成员机构，有时也指普华永道网络。每家成员机构各自独立。详情请进入www.pwc.com/structure。

www.pwc.cz/crimesurvey

# *Global Economic Crime Survey 2014*

## The Evolution of Fraud

*Czech Republic*



pwc

# Contents

***The Global Economic Crime Survey 2014 was carried out by PwC. It is the largest survey of its kind with 5,128 survey participants from 99 countries.***

***The survey is intended not only to describe the current state of economic crime but also to identify trends and perception of future risks.***

# Preface

In Lewis Carroll's Alice Through the Looking-Glass, the Red Queen is reported to say: *"Now, here, you see, it takes all the running you can do, to keep in the same place"*. In modern times, this has been used as an analogy for the theory of evolution.

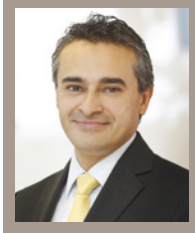
We can take Mr Carroll's words as a very fine description of the development in the area of economic crime. Economic crime is constantly evolving and seeking new ways to thrive. Companies need to find new and more efficient ways to protect their assets or else they will be outpaced by the evolution of fraud.

The Global Economic Crime Survey 2014 supports this observation: economic crime is more common in the Czech Republic and takes more diverse forms. Procurement fraud and cybercrime have gradually emerged as standalone major categories of fraud. We strongly advise companies to adjust their risk assessments accordingly.

Other interesting observations include a rise in the cost of economic crime, an increase in the share of fraud committed by agents or intermediaries, and generally strict measures taken by companies against identified fraudsters.

We invite all entrepreneurs and managers to read through the report and to draw conclusions relevant to their undertaking. A global report and local variants for different countries are available to help companies doing business globally.

Last but not least, we would like to thank the survey participants who were kind enough to share their observations of fraud and provide their insights. We are especially thankful to the 94 responding entities from the Czech Republic. All respondents share our belief that economic crime is too costly to ignore.



***Sirshar Qureshi***
Partner responsible for Forensic Services in CEE
PwC Czech Republic

***Michal Kohoutek***
Head of Forensic Services
PwC Czech Republic

# Main Findings

## The Dangers of Crime

**Crime around us.** Economic crime is more common in the Czech Republic than we would like to think. 48% of respondents indicated their company experienced economic crime within the last 24 months. This is clearly above the regional and global average (38% and 37%, respectively). For the Czech Republic, this represents an increase by more than two thirds compared to the results of our previous survey from 2011. 44% of organisations who suffered economic crime estimated the resulting total financial loss to be USD 100,000 or more.

**Crime evolves.** Traditionally, asset misappropriation is the main observed type of crime (80%). However, fraudsters seek out new avenues from which to defraud their victims. The distribution of various types of economic crime is becoming more diverse, seeing an increase in the share of other types of crimes: cybercrime (31%), procurement fraud (29%), money laundering (27%), bribery and corruption (27%), mortgage fraud (24%).

### *Cybercrime*

**Occurrence.** Companies are more likely to suffer cybercrime than at any time in the past. Compared to the previous survey, cybercrime occurence has more than doubled. In the previous survey, there were 6 companies reporting asset misappropriation (the most common economic crime) for each company reporting cybercrime. This year the ratio is 2.5:1.

**Risks of cybercrime.** In business practice, more and more reliance is being put on web applications, remote access and clouds. This increases the potential impact of cybercrime.

**High frequency of undetected cases.** Moreover, cybercrime is dangerous as the victim companies might not detect the fraud taking place. We believe the latency is higher than the latency of asset misappropriation. Therefore, the real occurrence is most probably significantly higher than the number reported.

### *Procurement fraud*

**Occurrence.** Procurement fraud emerged as a standalone category of fraud, having been reported by 29% of respondents that became a victim of economic crime. The top reported risk factor is the process of selecting a supplier.

**Risks of procurement fraud.** Procurement fraud usually includes collusion between business parties. Therefore, the detection of this type of fraud is often difficult. However, there are ways to mitigate the risks. For example, companies with a large number of transactions and vendors may take advantage of complex data analytics to identify potential frauds or inefficiencies in procurement.

### *Corruption and bribery*

**Risks of corruption.** 27% of companies that experienced fraud reported bribery and corruption. In comparison with the last survey, this represents an increase by 6 percentage points. Corruption is seen as the greatest risk in doing business globally, both in terms of loss of reputation and monetary loss. This is supported by PwC's 17th Global CEO Survey 2014: 69% of Central and Eastern Europe ("CEE") Chief Executive Officers ("CEO") are concerned about the impact of corruption and bribery on their business. According to the PwC CEO Survey, corruption and bribery was the top threat to growth in the CEE region.

## What companies do and not do

**Remedial actions.** Companies take strict measures against fraudsters. They usually do not hesitate to terminate the rogue employee when identified (91%). Quite often, law enforcement authorities are notified (46%) or a civil action is sought (36%). When fraud by an external subject is discovered, law enforcement authorities are usually notified (83%), the business relation is ceased (70%) or civil action is sought (65%).

**Prevention and detection.** Czech companies seem to rely on specific traditional methods of fraud detection while methods such as data analytics and reporting suspicious transactions play a less significant role. In addition, there is a relatively large number of crimes detected without active involvement on the part of the company. In total 42% of serious frauds were detected outside the corporate controls.

It would seem that there is room for improvement in terms of crime detection. Czech companies should definitely start thinking of increasing the efficiency of detection methods.

Methods of fraud detection usually fall into one of three categories: corporate controls, corporate culture, or actions beyond the influence of management.

GECS 2014 shows that the significant share of fraud in Czech companies (30%) was detected by fraud risk management which is significantly above the regional and global average (9% and 4%, respectively). However, the survey shows that other methods such as rotation of personnel, whistle-blowing system or data analytics are not fully utilised in the Czech environment.

Literally, hundreds of thousands of records, scores of disconnected worksheets, many different systems... Where should the company begin? All the information one could possibly want is available but how to analyse it?

Although companies store and analyse more data than ever before, finding insights within the data are often difficult to achieve using traditional analytic methods. While spreadsheets are easy to prepare and understand, the ability to draw conclusions from the data diminishes as the volume and complexity of data grows.

Visualisation, or visual analytics, is the concept of using pictures, charts, diagrams and maps to reveal key relationships, communications, trends and patterns within large amounts of data. Some companies are starting to appreciate the power of visualisation to detect fraud and abuse; from detecting fictitious employees and conflicts of interest, to detecting inappropriate travel expense expenditures.

**Pavel Jankech**
Senior Manager in Forensic Technology Services

**Do you think that the measures that companies use to combat fraud are sufficient?**
Currently, companies primarily use preventative measures to combat fraud. This, however, increases the risk that fraud will remain undetected longer. Our experience shows that fraud is usually identified, on average, only after it has already been taking place for two years. The impact of such fraud can be really serious, and it's not just a pure financial loss. A company's reputation, employee morale, or business relationships with business partners are also at risk.

**What would you recommend to companies?**
A robust control environment is an absolute necessity. Nevertheless, it is never 100% bulletproof so we recommend the companies also implement detection mechanisms, such as regular data analytical tests or a continuous fraud detection system. Using detection measures will help a company to identify fraud sooner and thus reduce losses.

**What data test do you have in mind?**
Traditional methods seek to identify suspicious transactions (red-flags) through rule-based testing. Classic examples include round-sum invoices and late-night postings. The challenge is that red-flags are typically not unusual events, and therefore the outputs from the tests are long lists of exceptions with many false-positives, leading to a costly manual investigation. Moreover, these rules are already well known, so the fraudster can easily avoid them.

**How to proceed in these cases?**
Based on our experience, each fraud scheme can be classified into one of several categories. Each of the different types of fraud leaves a specific "footprint" in the data. Using advanced analytical techniques and visualisation, we can identify different patterns of behaviour that correspond to these tracks. This approach can be used proactively to identify potential weak areas of control in the company, or reactively in the investigation of a specific incident.

**What kind of advanced analytical techniques are they?**
These are advanced statistical methods or data mining techniques. These can help identify hidden patterns in the data behaviour. Each of the patterns indicates the behaviour of the supplier or user, and is compared with standard behaviour in the dataset. Unusual or anomalous patterns indicating fraud are subsequently investigated. Using a combination of techniques to visualise the data and detailed knowledge of the company, the investigation should just focus on unusual or anomalous behaviour. The results of detailed investigations shall apply retroactively to increase the accuracy of the search algorithm.

**What data is required for this type of testing?**
During the initial phase of the project we would seek to understand the specifics of the company and its business and its existing control environment to identify key risk areas for fraud. Based on those we would decide where to start looking for fraud. The main sources are typically data from ERP and accounting systems, or actual cash flows gathered directly from bank statements, but also other, less usual sources of data like car GPS records, physical entry access records, or call or network traffic logs can be utilised for analysis.

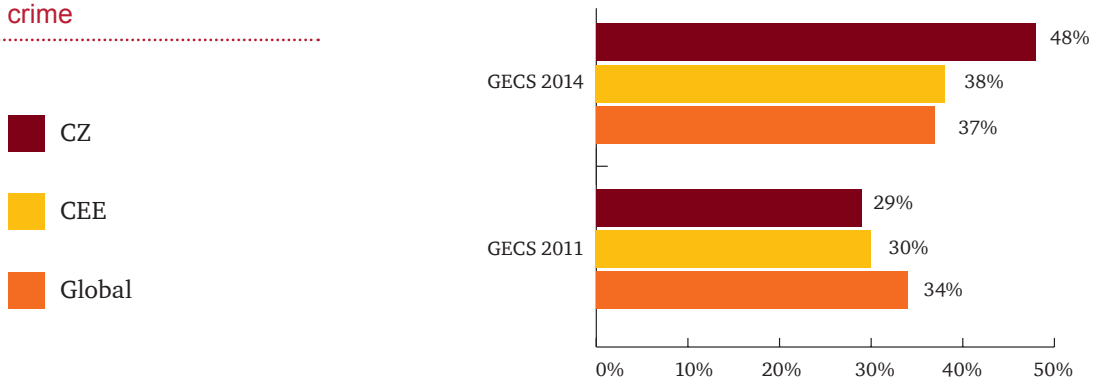
# Economic Crime in the Czech Republic

## Central themes

### Dangerous territory?

Since the previous survey, we have seen a steep rise in the number of reported economic crimes. In 2011, the number of Czech companies detecting frauds (29%) was below the regional and global average (30%, respectively 34%). This year, 48% of respondents indicated their companies had experienced economic crime in the past 24 months, well above the regional and global average (38% and 37%, respectively).

How many companies experienced economic crime

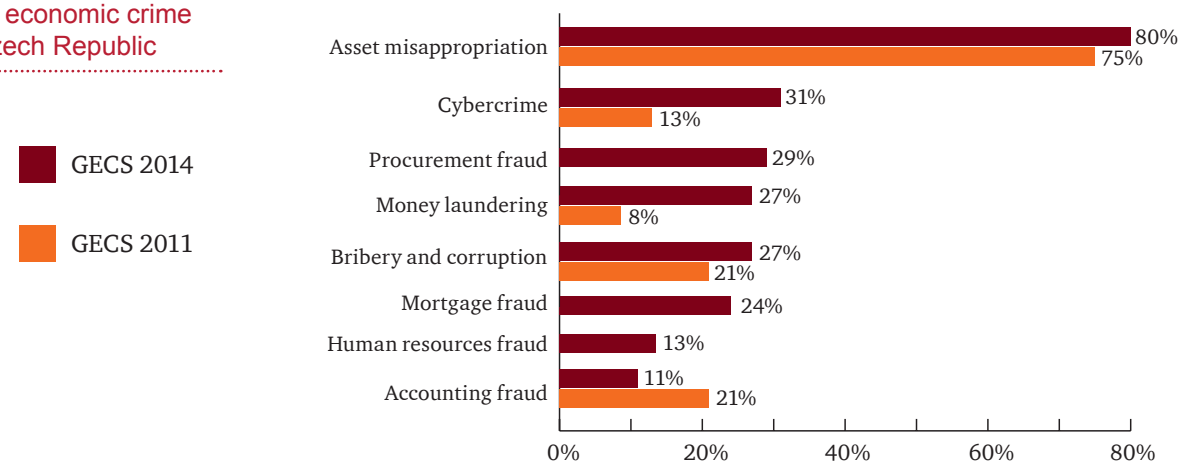



In order to understand the underlying reasons behind the increase, let us have a look at the changes in individual fraud categories.

### Greater propensity to types of economic crime

Attacks against corporate assets are more and more ”creative”. The relative share of asset misappropriation as the traditionally most common and simplest type of crime is decreasing in favour of more “creative” types of fraud.

Types of economic crime in the Czech Republic



Since our first global economic crime survey, in 2001, three types of fraud have consistently registered as leaders among respondents – asset misappropriation (usually by a wide margin), bribery and corruption, and accounting fraud. We added cybercrime as a distinct classification in 2011 and it immediately registered at 13%. In line with our expectation (and predictions), the number of companies reporting cybercrime has increased significantly (reaching 31%) in the Czech Republic, even above the global average (24%).

This year, we added another new category – mortgage fraud, human resources fraud and procurement fraud. Potentially driven by the on-going megatrend of outsourcing and organisational interconnectivity, procurement fraud received a significant response (29%), becoming the third most-reported type of fraud in the Czech Republic.

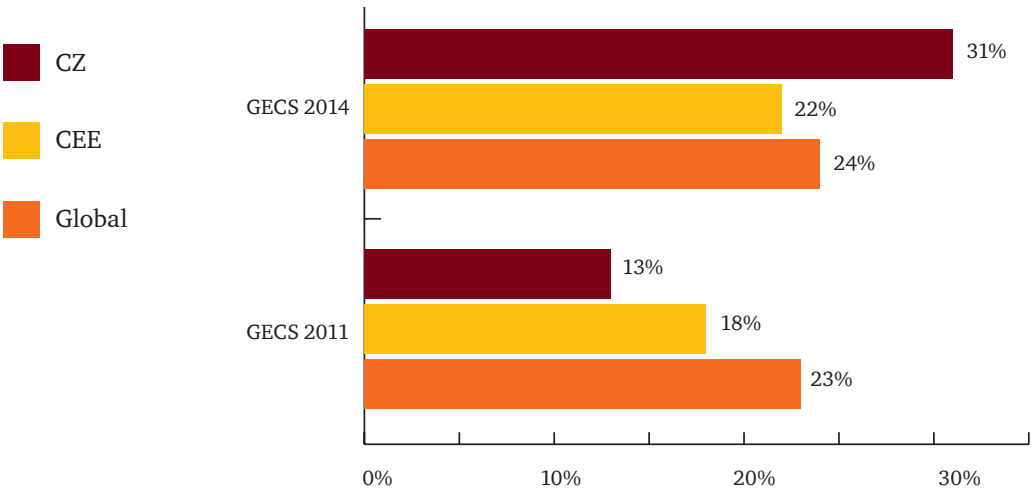
With an increase observed in each single reported fraud category, including the two other newly added categories of mortgage fraud and human resources fraud, it comes as no surprise that the overall number of organisations reporting economic crime in the Czech Republic has increased so dramatically.

It is also quite likely that the relative occurrence of crimes such as bribery, cybercrime or procurement fraud is even higher. These types of crimes are difficult to detect. During our own forensic engagements, we encountered numerous instances of long-term schemes which were accidentally detected by the victim company.

Therefore, companies should pay adequate attention to the different fraud schemes they may be facing. Control over cash and other physical assets might not be enough.

## *Cybercrime*

Share of cybercrime on fraud reported



Cybercrime can be described as the most dangerous crime of this century. This is supported by:

- survey results on actual occurrence;
- survey results on perception of future threats; and
- the very nature of today's business transactions and the increasing dependence on computer applications.

Modern companies are following trends in utilising technology to its full potential and to give their employees more freedom. People work from home using their own smart devices connected to cloud, respond to emails from internet cafes while on vacation, and review reports at airports. This is basically enlarging the perimeter that needs to be protected and deal with environments that are not fully under company control.

This is also a reason for a shift in security paradigm:

- 90s - respond after the breach;
- 00s - get ready for the breach; and
- 10s - assume the breach has happened or is underway.

It is not a question of whether the company will be subject to cyberthreat, but when and how it will happen.

Successful companies are prioritising what matters most – guarding their crucial data against organised targeted attackers in the global business ecosystem covering fluid data moving around internally as well as to/ from business partners and other stakeholders.

More than one half of respondents indicated that their perception of cybercrime risks has increased over the last 24 months. Theft of intellectual property, personal data or damage to reputation is of the greatest concern when it comes to cybercrime.

We can describe one of the cases we have worked on in the past. IT personnel in a large energy company found a computer in their server room, which they did not have in their books and they could not access it. At the same time they started to experience drop outs in internet connectivity, which was a significant issue due to online banking.

Through the investigation we have established the function of the unknown computer – one of the IT administrators was running a side internet business and he was misusing company resources for that. His cyber activity actually affected the whole business because they were not able to reconcile client payments as the online banking was not functioning.

**Tomáš Kuča,** Risk Assurance Partner leading our cyber security

**Aren't cybercrime and cybersecurity just more buzzwords?**
These are labels for the current phenomena in the information technology world. The rise of cybercrime is evident and supported by thousands of cases happening around us all the time. Cybersecurity is a preventative measure used to respond to this situation.

**What has changed in this field in the last couple years?**
In the past, companies responded after an incident occurred. In better cases they were building their protection in anticipation of a future incident. It would seem the current best approach for development of a cybersecurity policy is to assume a security breach has already happened.

The attackers have changed, which means they use sophisticated and persistent methods, they target specific information for strategic gains, they work across the globe, they are structured and organised and some of them act on behalf of states.

**What can be done to improve our situation?**

- Employ a chief information security officer and get him involved at the board level "the top of the house".
- Clarify roles and responsibilities in this area.
- Create a cyberincident response team.
- Invest in cyberskills of your employees.
- Set up cooperation with cybercrime experts.

***Modern communication methods and new technologies are enlarging the perimeter that needs to be protected. Companies are dealing with environments that are not fully under company control.***

## *Procurement fraud*

For the first time, GECS 2014 included procurement fraud as a separate economic crime category. 29% of Czech companies which suffered fraud indicated that their companies experienced at least one instance of procurement fraud. This ranks procurement fraud as the third most common reported type of fraud in the Czech Republic. The reported high occurrence of procurement frauds exceeded even our expectations.

The most vulnerable point, both in the Czech Republic and globally, is the vendor selection process. This underscores even more the importance of knowing your business partners, a point we have emphasised in our last survey.

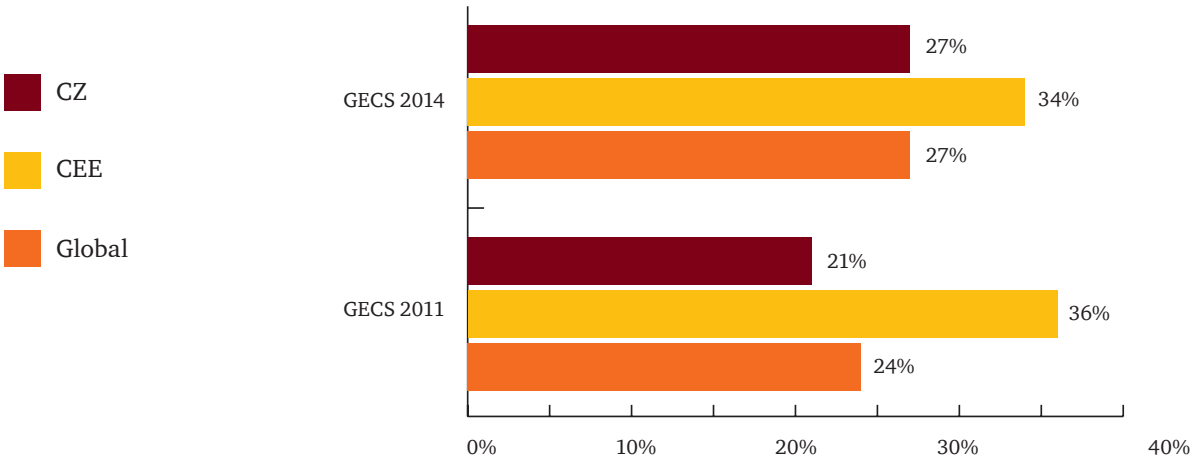
Generally speaking, when an organisation goes outside its walls for services, goods or assets, the potential for procurement fraud exists.

An increasing interconnectedness of business entities together with more common outsourcing make companies more vulnerable to procurement frauds than before. Moreover, there are numerous ways a procurement fraud can be committed. As a result, procurement fraud is one of the more difficult frauds to be detected and investigated.

## *Corruption and bribery*

In recent years, corruption has become a topic of public discussion in the Czech Republic, and for good reason. Corruption is among the most serious economic crimes and is seen as the greatest risk in doing business globally, both in terms of loss of reputation and monetary loss. In terms of occurrence, it is the fourth most noted type of economic crime in the Czech Republic (27%) and the third globally in GECS 2014 (27%). CEE are, along with Africa, the regions with the largest prevalence of corruption.

Share of corruption and bribery on fraud reported




PwC's 17th Global CEO Survey 2014 indicated that corruption awareness is on the rise, more than half of CEE CEOs considered corruption and bribery to be a threat. According to GECS 2014, 16% respondents indicated their company has been asked to pay a bribe in the last 24 months. 35% of respondents believe their company has lost an opportunity to a competitor which they believe had paid a bribe in the same period.

## *Impact of economic crimes*

No discussion of economic crimes would be complete without trying to quantify the impact of fraud. After all, the anti-fraud effort is just another function of the company which should pay off to justify its existence.

44% of respondents that experienced economic crime reported a total loss of at least USD 100,000. This represents a 6 percentage point increase compared with GECS 2011. This is a reported loss by companies that usually care and try to prevent and detect fraud. How greater would the actual loss be if the company did not care and there were no counter fraud measurements?

There are also other ways that a company could suffer besides losses that are purely financial. Consistent with the global results, companies would report a negative impact on corporate reputation as the greatest non-financial issue. However, the impact on employee morale shall be also considered.

In this respect, we would like to point out that a negative impact on employee morale might serve as a trigger to secondary actions (frauds being perpetrated by frustrated or demotivated employees). “Everybody does it” or “they deserved it” has been observed many times as a handy rationalisation of first-time fraudsters!

## Managing fraud

### *Who commits fraud*

We tried to make a profile of the perpetrator of the most serious economic crime that the respondents' companies had experienced.

There is an almost perfect balance between internal and external perpetrators (49% against 51%).

It should come as no surprise that middle to senior managerial persons are more likely to commit the most serious internal fraud than junior staff members. The most typical fraudster is male, 31 to 40 years old and who has spent 3 to 5 years in the company.

In the case of external perpetrators, the share of agents or intermediaries (22%) is higher than that of customers (17%) or that of vendors (9%).

Generally speaking, agents and intermediaries are entrusted by the victim company, they may have a detailed knowledge of the victim company's procedures, and they work more or less independently so it is more difficult to oversee their work.

Therefore, we advise companies to think about procedures that can be used to prevent fraud from being committed by agents or to identify such fraud as soon as possible. One notorious example would be fraud orchestrated by agents of insurance or loan companies, sometimes being perpetrated by organised rings of fraudsters who infiltrated the company's pool of agents. Background checks in justified cases might be a worthy option.

### *Prevention of fraud*

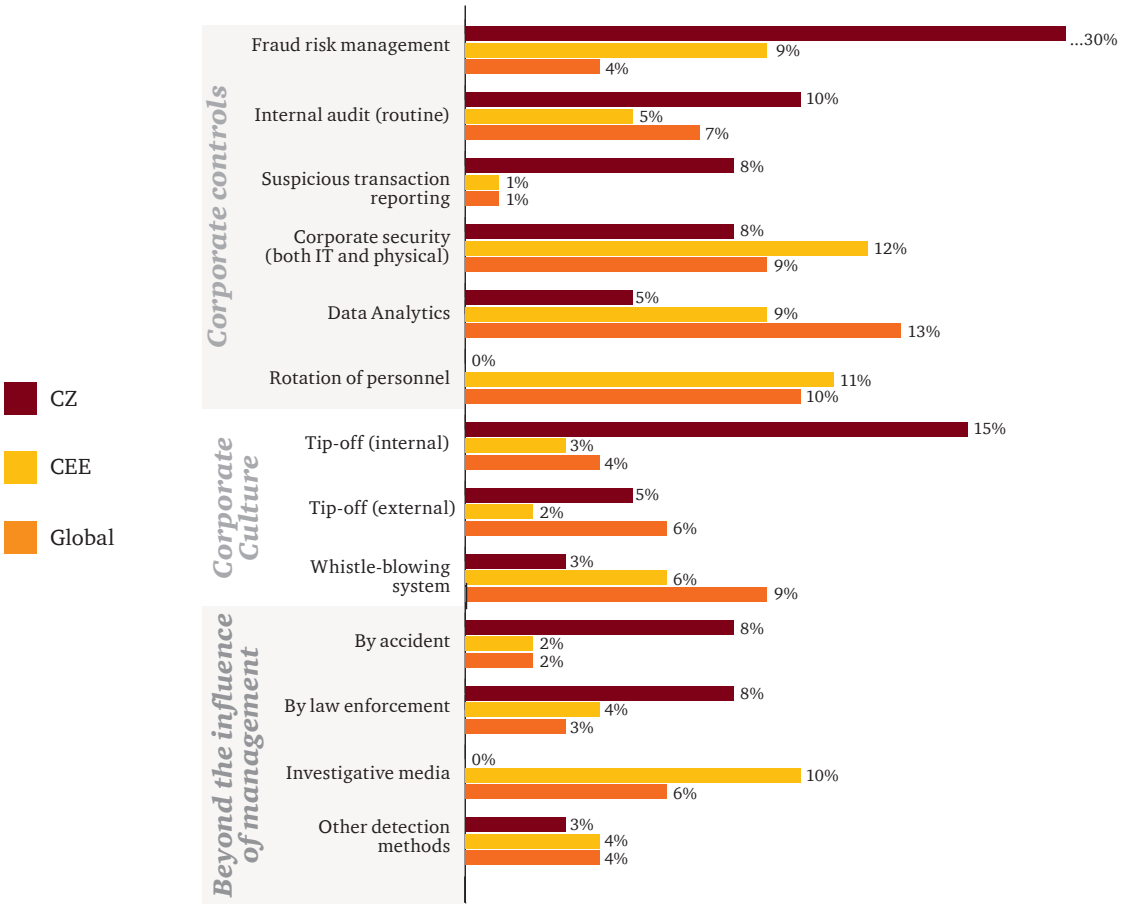
Why would someone decide to commit a fraud? Our survey indicates that, by far, the most significant contributing factor for internal fraudsters is simply opportunity (86%).

At the same time, out of possible contributing factors, opportunity is the one most within a company's control. Therefore, a review of procedures in the areas most vulnerable to fraud may be an effective way to reduce the risk of falling victim to fraud.

## *Detection of fraud*

The results show that companies do not take economic crime lightly. It is encouraging that 40% of Czech organisations that reported economic crime have detected fraud via Fraud risk management or routine internal audit procedures. Similarly as with the 2011 results, this is significantly above the global average (11%).

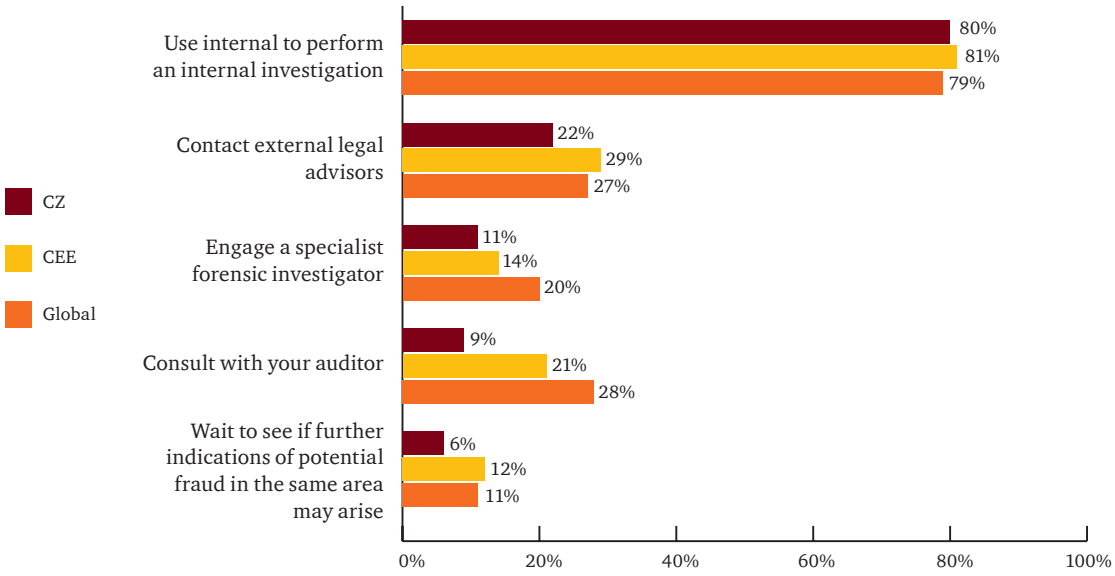
On the other hand, there is still room for more directed actions. The share of data analytical methods (5%) is below the global average (13%). This suggests understated importance of IT detection systems within Czech organisations, although these systems can be a very cost-effective supplement to traditional methods, when employed correctly.




Numbers are rounded to the nearest whole number.

The first reaction of most companies in the Czech Republic when a potential fraud is detected is to resort to internal investigations (80%). In many cases companies are also seeking specialised piece of advice from external legal advisors (22%). The survey indicated that Czech companies are more relying on their internal sources or legal counsel than engaging specialist forensic investigators (only 11% compared to 20% globally) or consulting the case with their auditor (9% Czech Republic, 21% CEE region, 28% globally).

## Reaction of companies when a fraud is identified



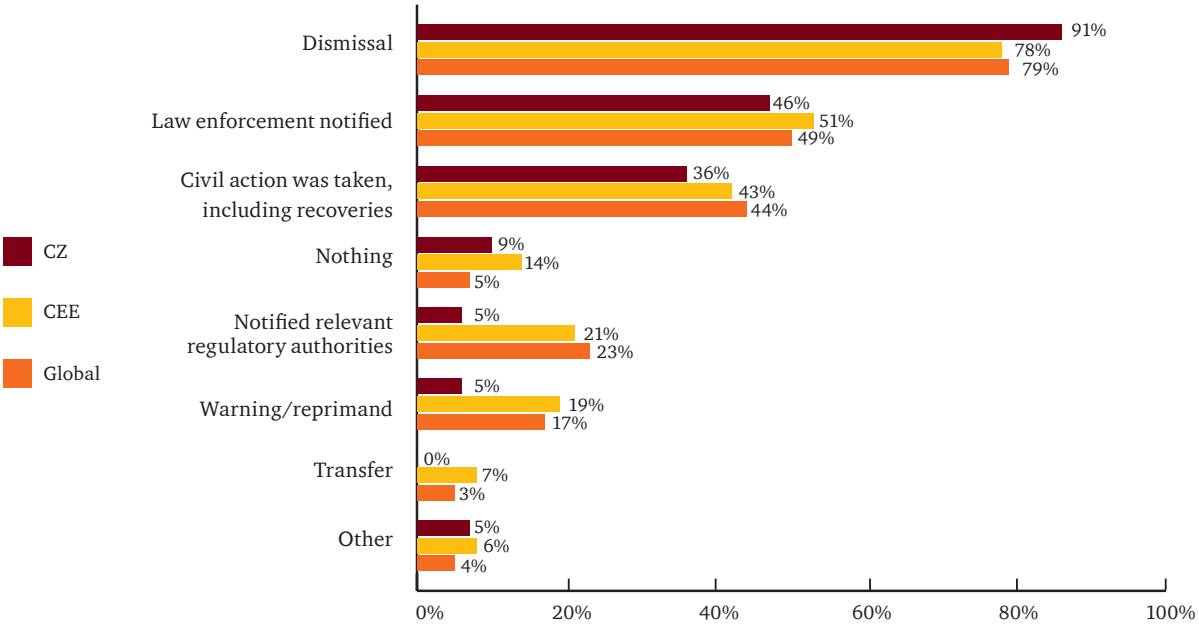

## *Remedial actions*

The survey indicated a clear stance by most companies against fraudsters, both internal as well as external. The occurrence of dismissals of internal perpetrators (91%) is even higher than in the previous survey (81%) and in the 2009 survey (65%).

This would suggest a better awareness of companies that fraud is costly. Especially in times of economic turmoil, there are few reasons to take fraud lightly.

With an external perpetrator, dismissal is obviously not an option. However, 70% of Czech organisations did cease a business relationship in response to an external fraud perpetrator. It is also encouraging that the occurrence of law enforcement notifications is rather high (83%), well above the global average of 61%.

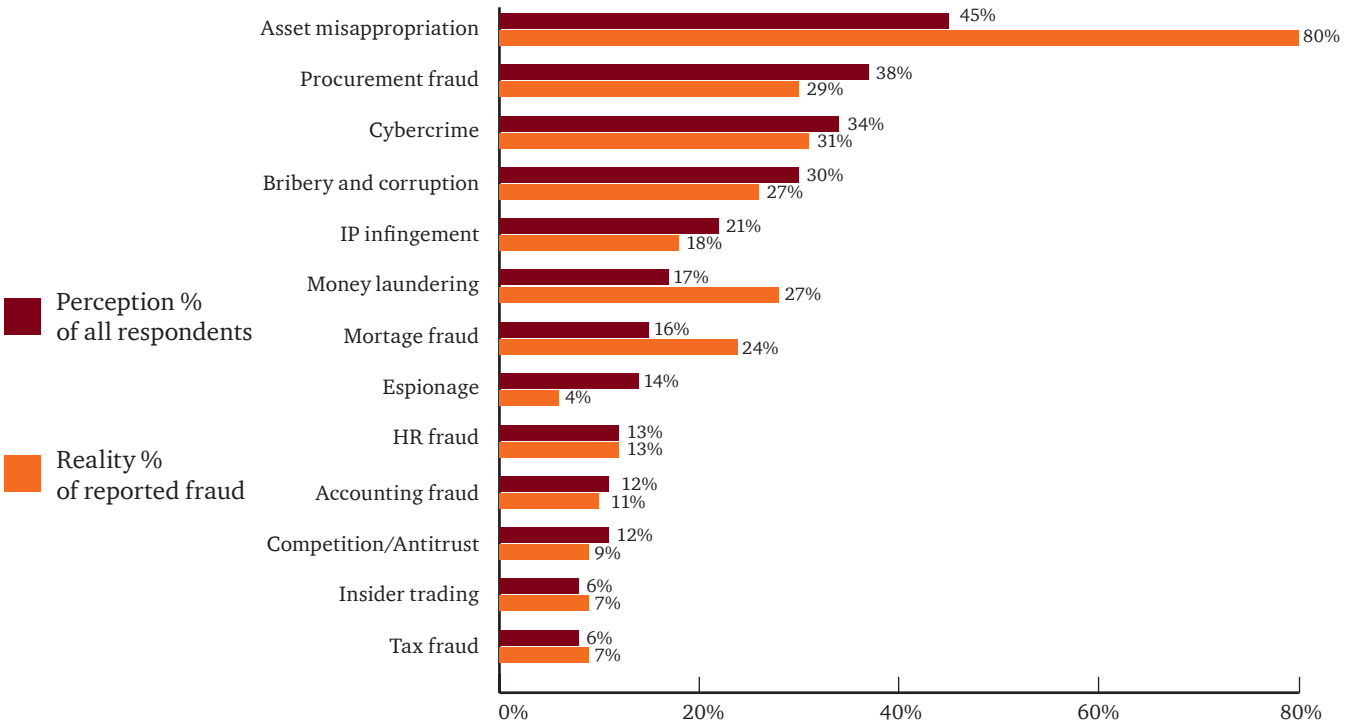
### Remedial actions against internal perpetrator



## Expectations

We also asked which types of crime companies expect to face in the next 24 months. The following data depend on the perception of risks by the companies. This is not the same as the real extent of the risk. Still, it is interesting to compare the perception of risks with the real occurrence.

It would seem that companies underestimate the risk of asset misappropriations in spite of its reported occurrence.



# *Contact*

***Sirshar Qureshi***
Partner, CEE Forensic Leader
+420 251 151 235
sirshar.qureshi@cz.pwc.com

***Michal Kohoutek***
Head of Forensic Services
+420 251 151 231
michal.kohoutek@cz.pwc.com

***Pavel Jankech***
Senior Manager
Forensic Technology Solution
+420 251 151 336
pavel.jankech@cz.pwc.com

***Kateřina Halásek Dosedělová***
Senior Manager, Forensic Services
+420 251 151 293
katerina.halasek-dosedelova@cz.pwc.com

***Jiří Urban***
Senior Manager, Forensic Services
+420 251 151 627
jiri.urban@cz.pwc.com

***Filip Volavka***
Senior Manager
Forensic Technology Solution
+420 251 151 269
filip.volavka@cz.pwc.com

pwc

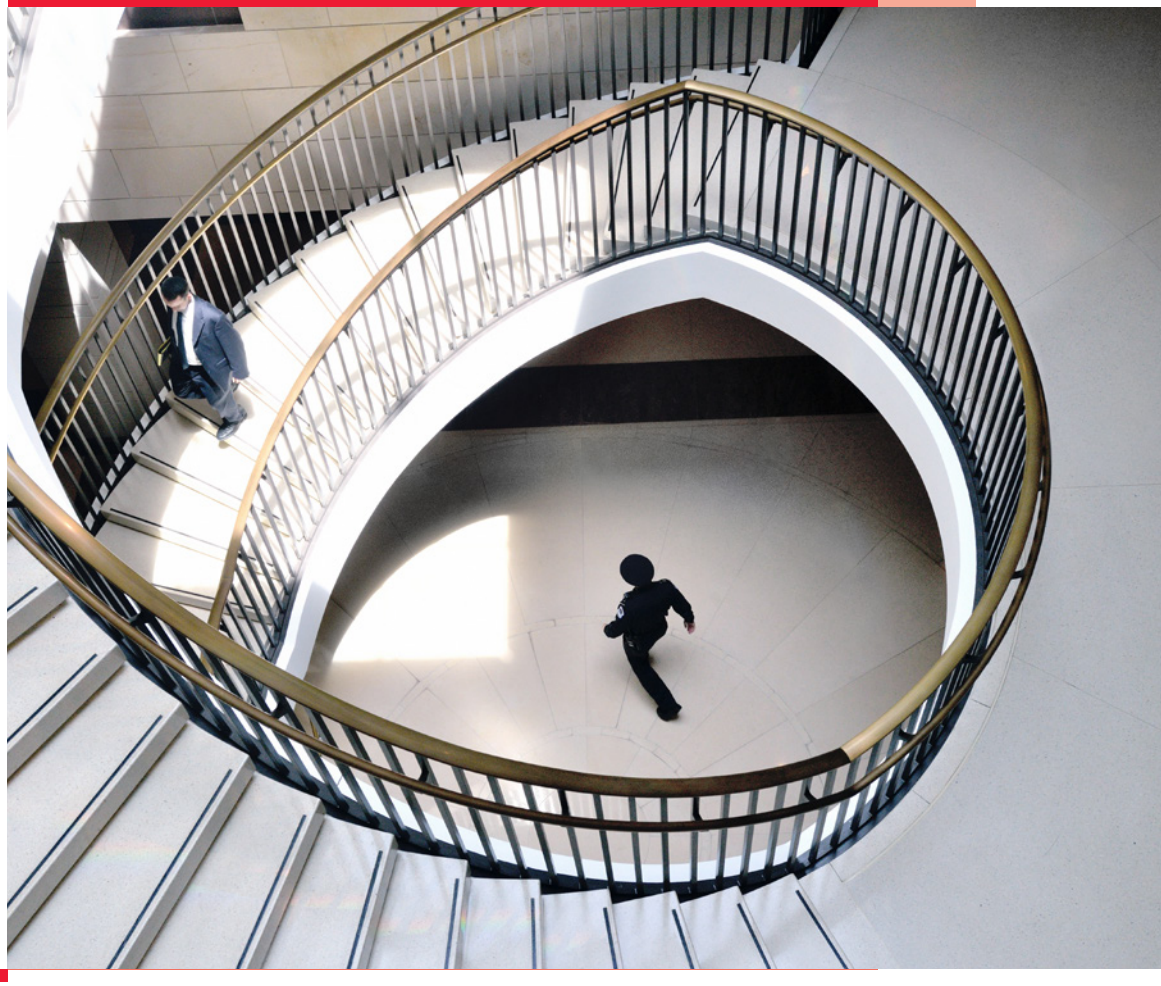
© 2014 PricewaterhouseCoopers Česká republika, s.r.o. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Česká republika, s.r.o., which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.

www.pwc.cz/crimesurvey

# *Celosvětový průzkum hospodářské kriminality 2014*

## Hospodářská kriminalita a její „evoluce“

*Česká republika*



pwc

# Obsah

***Celosvětový průzkum hospodářské kriminality 2014 byl vypracován společností PwC. Jedná se o největší průzkum svého druhu na světě, kterého se zúčastnilo 5 128 respondentů z 99 zemí.***

***Cílem průzkumu byla nejen analýza současného stavu hospodářské kriminality, ale také identifikace trendů a změn ve vnímání budoucích rizik.***

# Úvod

V knize Lewise Carrolla – Za zrcadlem a co tam Alenka našla, černá královna řekla: *„… vidíte, musíte běžet, jak nejrychleji umíte, abyste zůstala na místě. Chcete-li se posunout, měla byste utíkat aspoň dvakrát rychleji!“* V moderní době se tento citát začal používat jako analogie teorie evoluce.

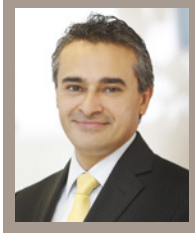
Slova pana Carrolla můžeme použít jako velmi výstižný popis vývoje v oblasti hospodářské kriminality. Hospodářská kriminalita se neustále vyvíjí a útočí novými směry. Společnosti proto musí přijímat nové a efektivnější způsoby ochrany svých aktiv, aby se držely o krok napřed a nestaly se její obětí.

Celosvětový průzkum hospodářské kriminality 2014 tyto poznatky potvrzuje: hospodářská kriminalita v České republice se stává čím dál běžnějším jevem a bere na sebe rozmanitější podoby. Podvody v nákupním procesu či počítačová kriminalita se postupně staly samostatnými hlavními kategoriemi podvodu. Vzhledem k tomuto doporučujeme společnostem přizpůsobit jejich systém hodnocení rizik.

Mezi další zajímavé poznatky patří nárůst nákladů hospodářské kriminality, zvýšení podílu podvodů páchaných zástupci či zprostředkovateli nebo přísná opatření přijímaná společnostmi proti zjištěným pachatelům podvodů.

Budeme velmi rádi, pokud se manažeři a majitelé společností seznámí s detailními výsledky našeho průzkumu, které jsou obsaženy v této zprávě tak, aby si mohli sami vytvořit závěry relevantní pro své podnikání. Společnosti, které působí na mezinárodní úrovni, mohou pro své podnikání využít jak výsledky celosvětového průzkumu, tak i zprávy zaměřené na konkrétní země.

Závěrem bychom rádi poděkovali všem účastníkům průzkumu, kteří byli ochotni podělit se s námi o své poznatky a zkušenosti z oblasti hospodářské kriminality. Zvláštní poděkování patří 94 respondentům z České republiky, kteří sdílejí náš názor, že hospodářská kriminalita je příliš nákladná na to, abychom ji ignorovali.



***Sirshar Qureshi***
partner zodpovědný za Forenzní služby v CEE regionu
PwC Česká republika

***Michal Kohoutek***
vedoucí oddělení Forenzních služeb
PwC Česká republika

# Hlavní zjištění

## Nebezpečí kriminality

**Kriminalita kolem nás.** Hospodářská kriminalita v České republice je jevem mnohem běžnějším, než bychom si mysleli. Celkem 48 % respondentů uvedlo, že za posledních 24 měsíců se jejich společnost stala obětí hospodářské kriminality. To je jednoznačně nad regionálním i celosvětovým průměrem (38 %, respektive 37 %). V porovnání s výsledky předchozího průzkumu z roku 2011 jde o výrazný nárůst, a to o více jak dvě třetiny. Celkem 44 % organizací, které čelily hospodářské kriminalitě, odhadlo, že jejich finanční ztráty dosáhly 100 tisíc amerických dolarů nebo více.

**Kriminalita se vyvíjí.** Majetková zpronevěra tradičně zůstává nejběžnějším typem hospodářské kriminality (80 %). Pachatelé však vyhledávají stále nové způsoby, jak společnosti poškodit. Hospodářská kriminalita se stává pestřejší. Zaznamenali jsme nárůst podílu podvodů jako počítačová kriminalita (31 %), podvody v nákupním procesu (29 %), praní špinavých peněz (27 %), podplácení a korupce (27 %) nebo hypoteční podvody (24 %).

### *Počítačová kriminalita*

**Výskyt.** V současné době, více než kdykoliv v minulosti, jsou společnosti náchylné k tomu, aby se staly obětí počítačové kriminality. V porovnání s předchozím průzkumem se výskyt počítačové kriminality více jak zdvojnásobil. V předchozím průzkumu připadalo šest společností, které zaznamenaly majetkovou zpronevěru (nejběžnější typ hospodářské kriminality), na jednu, která se setkala s počítačovou kriminalitou. Tento rok se však poměr dostal až na hodnotu 2,5 : 1.

**Rizika počítačové kriminality.** V podnikatelské sféře je kladen stále větší důraz na využívání webových aplikací, vzdálených přístupů do infomačních systémů a cloudů. Tento trend zvyšuje potenciální dopad počítačové kriminality.

**Skrytá hrozba.** Počítačová kriminalita je nebezpečná mimo jiné i proto, že poškozené společnosti nemusí probíhající útok vůbec odhalit. Domníváme se, že počet „skrytých“ (neidentifikovaných) případů počítačové kriminality je větší než například v případě majetkové zpronevěry. Z tohoto důvodu je pravděpodobné, že její skutečný výskyt je mnohem vyšší než ten, který společnosti uvádějí.

### *Podvody v nákupním procesu*

**Výskyt.** Podvody v nákupním procesu se postupně vyvinuly v samostatnou kategorii podvodů, s níž se setkalo 29 % společností, které byly obětí hospodářské kriminality. Jako nejrizikovější fázi nákupního procesu společnosti označily zejména výběr dodavatele.

**Rizika podvodu v nákupním procesu.** Tento typ podvodu často spočívá ve skryté dohodě s obchodními partnery, kteří jsou do nákupu zapojeni. Proto je odhalení takového podvodu často velmi obtížné. Existují však způsoby, jak jeho rizika snížit. Například společnosti s velkým množstvím transakcí a obchodních partnerů mohou pro identifikaci potenciálně podvodných transakcí či neefektivního využití prostředků v nákupním procesu využít pokročilých datových analýz.

### *Podplácení a korupce*

**Rizika korupce.** Celkem 27 % společností, které se setkaly s podvodem, uvedlo, že byly obětí korupce a uplácení. V porovnání s předchozím průzkumem došlo k nárůstu o šest procentních bodů. Korupce je celosvětově vnímána jako největší riziko pro podnikání, a to jak z hlediska ztráty dobrého jména společnosti, tak i z pohledu finančních ztrát. Tato skutečnost je také podpořena výsledky sedmnáctého ročníku celosvětového Průzkumu názorů generálních ředitelů 2014 vypracovaného společností PwC: 69 % všech generálních ředitelů v regionu střední a východní Evropy se obává dopadů korupce na svou firmu. Korupce a uplácení představuje podle generálních ředitelů největší hrozbu pro hospodářský růst regionu.

## Co společnosti dělají, a co naopak ne

**Nápravná opatření.** Společnosti podnikají proti pachatelům hospodářské kriminality razantní kroky. Pokud identifikují interního pachatele, téměř vždy s ním ukončí pracovní poměr (91 %). Rovněž poměrně často kontaktují orgány činné v trestním řízení (46 %) nebo podají občanskoprávní žalobu (36 %). V případě, že dojde k identifikaci podvodu spáchaného externím pachatelem (tj. subjektem z vnějšího prostředí společnosti), dochází obvykle k oznámení případu orgánům činným v trestním řízení (83 %), k ukončení obchodních vztahů (70 %) a podání občanskoprávní žaloby (65 %).

**Prevence a detekce.** Na základě našeho průzkumu se zdá, že české společnosti spíše spoléhají na tradiční metody identifikace podvodu, zatímco například datové analýzy nebo systémy automatického hlášení podezřelých transakcí hrají méně významnou roli. Navíc poměrně velké procento všech typů podvodů je odhaleno bez aktivního přispění samotné společnosti. K odhalení 42 % závažných podvodů došlo mimo firemní kontrolní systémy.

Ukazuje se tedy, že společnosti mají ještě značný prostor pro zlepšení svých schopností odhalovat případy hospodářské kriminality. České firmy by měly rozhodně začít přemýšlet nad zvýšením efektivity detekčních metod.

Metody odhalování podvodů je možné rozdělit do tří kategorií: firemní kontroly, podniková kultura a dění mimo oblast vlivu vedení společnosti. Náš průzkum ukázal, že díky systému řízení rizik podvodů byla v českých společnostech odhaleno 30 % podvodů. To je výrazně více než na regionální nebo globální úrovni (9 %, respektive 4 %). Na druhé straně potenciál ostatních metod, jako například rotace zaměstnanců, anonymní informační linky nebo datové analýzy, není v českém prostředí v porovnání se světem plně využíván.

Společnosti mají k dispozici doslova desítky tisíc záznamů, spousty neprovázaných dat v souborech, mnoho různých systémů… Kde mají tedy začít? Jak analyzovat data?

Přestože společnosti shromažďují a analyzují mnohem více dat než v minulosti, pochopit podstatu dostupných informací lze pouze za pomoci tradičních analytických metod jen obtížně. Zatímco podklady lze připravit bez větších obtíží, schopnost vyvodit z nich závěry se postupně ztrácí s tím, jak roste objem a komplexita dostupných dat.

Vizualizace neboli grafická analýza je koncept používání obrázků, grafů, schémat a map pro odhalení klíčových vztahů, spojení, trendů a vzorů chování v obrovském množství dat. Některé společnosti si začínají cenit výhod těchto nástrojů pro detekci podvodů; od identifikace fiktivních zaměstnanců a případných konfliktů zájmů, až po odhalování neoprávněných cestovních nákladů.

**Pavel Jankech**, senior manažer v oddělení Forenzních technologií

**Domníváte se, že opatření, která společnosti používají k odhalování podvodů, jsou dostatečná?**
V současné době používají společnosti pro ochranu před podvody primárně preventivní opatření. Tím však zvyšují riziko, že podvod zůstane delší dobu neodhalený. Naše zkušenost ukazuje, že podvodné chování ve společnosti probíhá průměrně po dobu dvou let, než dojde k jeho odhalení. Dopady takového podvodu mohou být opravdu vážné a nejedná se pouze o finanční ztráty. V ohrožení je dobré jméno společnosti, morálka zaměstnanců či vztahy s dodavateli.

**Co byste společnostem doporučil?**
Silné kontrolní prostředí je naprostou nutností, avšak ani to nebude vždy 100% spolehlivé. Doporučujeme proto společnostem, aby zavedly detekční mechanismy, jako jsou například pravidelné datové testy nebo systémy průběžné detekce podvodů. Využívání detekčních opatření pomůže identifikovat podvod dříve, a tím omezit ztráty.

**Jaké datové testy máte na mysli?**
Tradiční metody se snaží identifikovat podezřelé transakce, takzvané „red flags“, pomocí testů založených na sadě předem definovaných pravidel. Typickým příkladem je fakturace zaokrouhlených částek nebo transakce zaúčtované mimo běžnou pracovní dobu. Problém však nastává v momentě, kdy „red flags“ nejsou neobvyklou událostí. V takovém případě je výsledkem testů dlouhý seznam výjimek s velkým množstvím falešných signálů, které vedou k nákladnému manuálnímu vyšetřování. Tato pravidla jsou navíc již všeobecně známá, proto se jim pachatel může jednoduše vyhnout.

**Jak tedy postupovat v takových případech?**
Na základě naší zkušenosti mohou být podvodná schémata klasifikována do jedné z několika kategorií podvodů. Každý typ podvodu za sebou zanechává v datech specifickou stopu. Při použití pokročilých analytických metod a vizualizace můžeme identifikovat různé vzory chování dat odpovídající těmto otiskům. Takový přístup může být kromě vyšetřování specifického incidentu využit také proaktivně pro identifikaci potenciálně slabých míst v kontrolních mechanismech společnosti

**Můžete popsat tyto pokročilé analytické techniky?**
Jedná se o statistické metody či techniky sběru dat, takzvané dolování dat, které dokáží identifikovat skryté vzory v chování dat. Vzor chování každého dodavatele nebo uživatele je následně porovnán se standardním chováním v daném souboru dat. Neobvyklý či odchylný vzor chování indikující podvod je následně vyšetřen. Díky použití kombinace techniky vizualizace dat a detailní znalosti společnosti se vyšetřování může ihned zaměřit na neobvyklé chování. Výsledky detailního vyšetřování by se měly aplikovat také zpětně, a zvýšit tak přesnost vyhledávacího algoritmu

**Jaká data jsou zapotřebí pro takový typ testování?**
V úvodní fázi projektu se snažíme porozumět specifikům dané společnosti, jejímu podnikání a existujícímu kontrolnímu prostředí, abychom určili oblasti, u nichž hrozí vysoké riziko výskytu podvodu. Na základě identifikace rizik určíme oblasti, na které zaměřit naše vyšetřování. Hlavním zdrojem jsou obvykle data z podnikových informačních systémů, účetních systémů či aktuální peněžní toky získané přímo z bankovních výpisů. Pro datovou analýzu mohou být použity i další, méně obvyklé zdroje jako například data z navigací v automobilech (GPS), záznamy o vstupech do budov nebo o provozu sítě.

# Hospodářská kriminalita v České republice

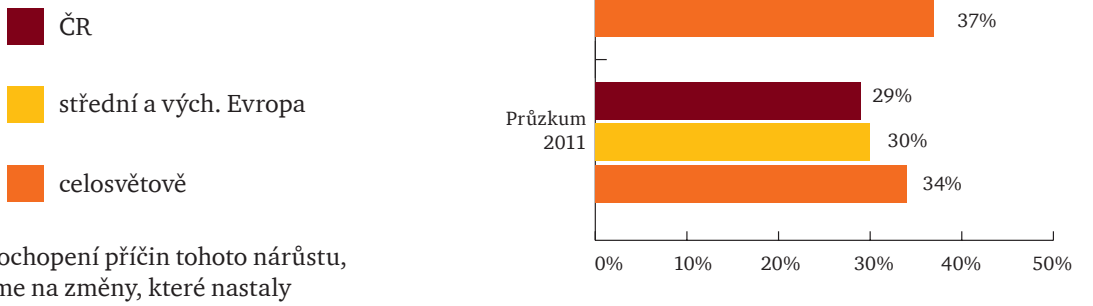
## Ústřední témata

### Zhoršení situace?

Od posledního průzkumu jsme zaznamenali prudký nárůst počtu společností, které se setkaly s hospodářskou kriminalitou. V roce 2011 se podíl českých společností, které identifikovaly podvod (29 %), nacházel pod regionálním a celosvětovým průměrem (30 %, respektive 34 %).

Oproti minulému průzkumu letos 48 % respondentů uvedlo, že v posledních 24 měsících jejich společnost čelila hospodářské kriminalitě. Tato hodnota je výrazně vyšší, než kolik uvádí regionální a celosvětový průměr (38 %, respektive 37 %)

Kolik společností se stalo obětí hospodářské kriminality?




Pro lepší pochopení příčin tohoto nárůstu, se podívejme na změny, které nastaly v jednotlivých kategoriích hospodářské kriminality.

### Rostoucí rozmanitost hospodářské kriminality

Útoky na firemní majetek jsou stále nápaditější. Podíl majetkové zpronevěry, tradičně nejběžnějšího a nejjednoduššího typu podvodu, se snižuje ve prospěch jiných neotřelých typů podvodů.

Typy hospodářské kriminality v České republice

Od dob našeho prvního celosvětového hospodářského průzkumu provedeného v roce 2001 respondenti pravidelně vybírali tři kategorie podvodů, a to majetková zpronevěra (obecně s velkým náskokem), podplácení a korupce a účetní podvod. V roce 2011 jsme přidali do našeho průzkumu počítačovou kriminalitu jako samostatnou kategorii, která ihned dosáhla 13 %. Dle našich očekávání a varování, se počet českých společností, které zaznamenaly případ počítačové kriminality (31 %), významně zvýšil. A to dokonce nad celosvětový průměr (24 %).

Letos jsme do našeho průzkumu přidali nové kategorie – hypoteční podvod, podvod v oblasti lidských zdrojů a podvod v nákupním procesu. Díky současnému trendu outsourcingu a organizační propojenosti společností uvedlo podvod v nákupním procesu řada respondentů (29 %), a ten se tak stal třetím nejčastěji uváděným typem podvodu v České republice.

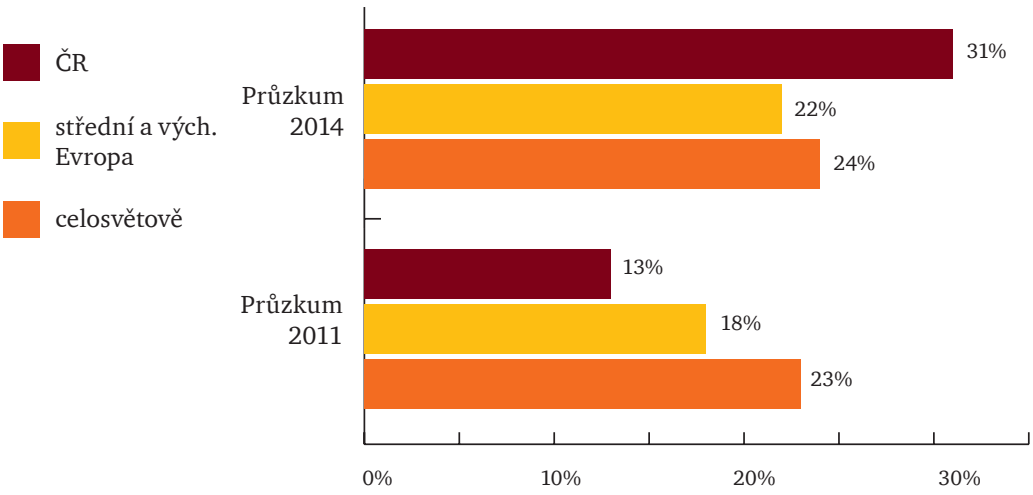
V porovnání s minulým průzkumem došlo k nárůstu v téměř všech kategoriích podvodů. Není tedy divu, že se tak významně zvýšil celkový počet společností, které se staly obětí hospodářské kriminality v České republice.

Je rovněž pravděpodobné, že výskyt podvodů, jako je podplácení, počítačová kriminalita či podvod v nákupním procesu, je ve skutečnosti ještě vyšší. Tyto druhy podvodů je složité odhalit. Během našich forenzních zakázek jsme se setkali s řadou případů dlouhodobě fungujících podvodných schémat, které poškozené společnosti odhalily zcela náhodou.

Proto by měly společnosti věnovat patřičnou pozornost všem druhům podvodů, jímž mohou teoreticky čelit. Pouhá kontrola hotovosti a dalších fyzických aktiv již nemusí být dostačující.

## *Počítačová kriminalita*

Podíl počítačové kriminality na spáchaných podvodech



Počítačové podvody můžeme považovat za nejnebezpečnější druh kriminality tohoto století. Potvrzují to:

- výsledky průzkumu skutečného výskytu
- výsledky průzkumu vnímání budoucí hrozby
- rostoucí závislost firem na počítačových aplikacích a podstata moderních obchodních transkcí

Moderní společnosti se snaží využívat plného potenciálu technologií a dávat svým zaměstnancům více svobody. Lidé pracují z domova s využitím svých vlastních chytrých zařízení připojených ke cloudu, během dovolené odpovídají na emaily z internetových kaváren nebo kontrolují dokumenty během čekání na letištích. Podstatně se tak rozšiřuje oblast, kterou je třeba chránit, a je nutné se vypořádat s prostředím, jež není plně pod kontrolou společnosti.

I to je důvod, proč se zásadním způsobem mění přístup k počítačové bezpečnosti:

- pojetí 90. let – reaguj až po prolomení bezpečnosti
- postoj na přelomu století – připrav se na prolomení bezpečnosti
- a nyní – předpokládej, že k prolomení již došlo, nebo se tak právě děje.

Není otázkou, zda se firma stane cílem počítačové hrozby, ale kdy a jak k tomu dojde. Úspěšné společnosti si stanovují priority ochrany svých klíčových dat před organizovanými útočníky podle jejich významu. V globálním prostředí jde přitom jak o data proudící uvnitř společnosti, tak i o informace od obchodních partnerů a dalších zúčastněných stran.

Více než polovina respondentů uvedla, že za posledních 24 měsíců začala počítačovou kriminalitu více vnímat. Nejčastějším důvodem ke znepokojení v oblasti počítačové kriminality jsou krádeže v oblasti duševního vlastnictví, osobních údajů nebo poškození dobrého jména a obchodní značky společnosti.

Pro dokreslení můžeme uvést případ, na kterém jsme v minulosti pracovali. Zaměstnanci oddělení IT jedné velké společnosti působící v energetickém průmyslu objevili v serverovně počítač, který nebyl v majetku společnosti a do něhož neměli přístup. Zároveň začalo docházet k výpadkům internetového připojení. Ty byly kvůli nutnosti přístupu do internetového bankovnictví pro společnost velkým problémem. Vyšetřováním jsme zjistili, jakou funkci měl neznámý počítač – jeden z administrátorů IT provozoval soukromě internetový obchod, a zneužíval k tomu zdroje společnosti.

Jeho činnost ohrozila provoz celé společnosti, jelikož z důvodu nefunkčního internetového bankovnictví společnost nebyla schopna zkontrolovat příchozí platby od klientů.

**Tomáš Kuča**, partner v oddělení Řízení rizik, specializující se na oblast počítačové ochrany

**Není počítačová kriminalita jenom dalším módním výrazem?**
Jedná se o současný fenomén ve světě informačních technologií. Nárůst počítačové kriminality je zřejmý a je doložen tisíci případů, které se neustále odehrávají všude kolem nás. Počítačová ochrana je preventivní opatření, které reaguje na tuto situaci.

**Co se v této oblasti změnilo za posledních pár let?**
V minulosti společnosti reagovaly až poté, co incident nastal. V lepších případech budovaly svoji ochranu v podobě očekávání budoucích incidentů. Zdá se, že v současnosti je nejlepším přístupem k oblasti rozvoje počítačové ochrany předpoklad, že k porušení ochrany již došlo. Útočníci se změnili. Používají důmyslnější metody a jsou stále vytrvalejší. Zaměřují se na specifické informace, aby dosáhli strategických cílů. Pracují napříč zeměkoulí, jsou organizovaní a někteří z nich jednají na popud států.

**Co můžeme udělat pro zlepšení naší situace?**
- zaměstnat vedoucího oddělení informační ochrany a zapojit ho do vedení společnosti
- stanovit role a zodpovědnosti v této oblasti
- sestavit tým, který dokáže reagovat na incidenty počítačové kriminality
- investovat do znalostí svých zaměstnanců v oblasti počítačové kriminality
- navázat spolupráci s experty v oblasti počítačové kriminality

***Moderní komunikační metody a nové technologie rozšiřují oblast, kterou je třeba chránit. Společnosti se musí vypořádat s prostředím, jež není plně pod jejich kontrolou.***

## *Podvod v nákupním procesu*

Letos poprvé byl podvod v nákupním procesu zařazen do průzkumu hospodářské kriminality jako samostatná kategorie hospodářského podvodu. Tento typ podvodu uvedlo v průzkumu 29 % českých společností, které byly obětí hospodářské kriminality. To ho řadí na třetí místo mezi nejčastěji uváděnými typy podvodů v České republice. Vysoká míra jeho výskytu předčila i naše očekávání.

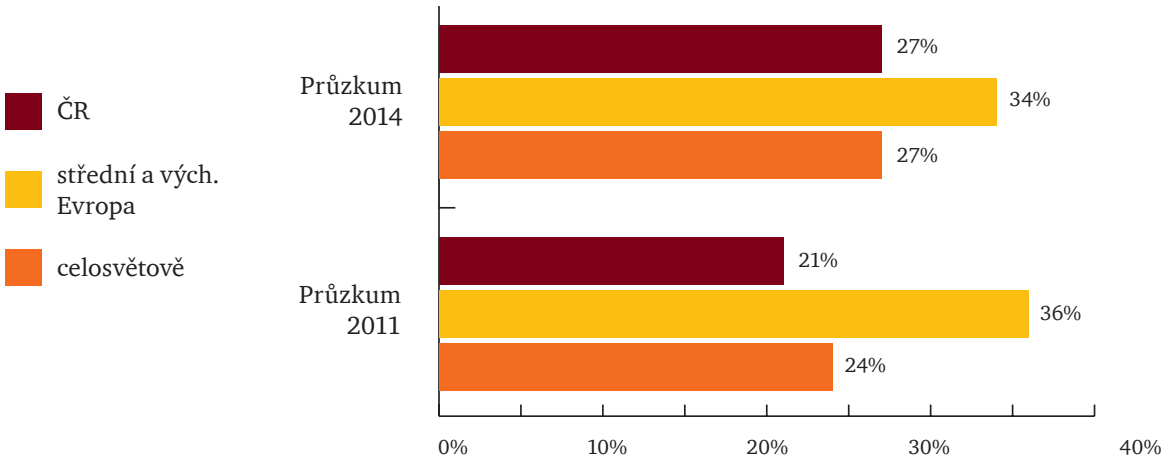
Nejcitlivějším bodem v nákupním procesu, jak v České republice tak i celosvětově, je proces výběru dodavatele. To ještě více podtrhuje nutnost dobře znát své obchodní partnery, kterou jsme zdůrazňovali v minulém průzkumu.

Pokud společnost poptává zboží, majetek nebo služby u obchodních partnerů, vzniká zde prostor pro případný podvod v nákupním procesu. Kvůli rostoucí provázanosti podnikatelských subjektů a stále běžnějšímu outsourcingu jsou společnosti těmito podvody více ohroženy. Existuje řada způsobů, jimiž může být podvod v nákupním procesu spáchán. Je proto velmi složité ho odhalit a vyšetřit.

## *Podplácení a korupce*

V posledních letech se korupce v České republice stala tématem veřejných diskusí. Oprávněně. Korupce se řadí mezi nejzávažnější typy hospodářské kriminality a je celosvětově vnímána jako největší riziko pro podnikání, a to jak z hlediska ztráty dobrého jména organizace, tak i z pohledu finanční ztráty. Z hlediska četnosti výskytu se jedná o čtvrtý nejčastější typ hospodářské kriminality v České republice (27 %) a třetí v celosvětovém měřítku (27 %). Střední a východní Evropa společně s Afrikou jsou regiony s nejvyšší mírou korupce.

Podíl podplácení a korupce na spáchaných podvodech




Celosvětový průzkum názorů generálních ředitelů 2014, který byl proveden PwC, ukázal, že povědomí o korupci roste. Podle tohoto průzkumu považuje 69 % generálních ředitelů v regionu střední a východní Evropy korupci a uplácení za hrozbu pro svou společnost. Letošní průzkum hospodářské kriminality odhalil, že 16 % společností bylo v posledních 24 měsících požádáno o úplatek. Celkem 35 % dotázaných se dále domnívá, že jejich společnost ztratila podnikatelskou příležitost ve prospěch konkurenta, u něhož mají podezření, že úplatek zaplatil.

## *Dopady hospodářské kriminality*

Žádná diskuze týkající se hospodářské kriminality nebude kompletní bez vyčíslení dopadů podvodů. Koneckonců aktivity prováděné firmami na omezení podvodů musejí přinášet výsledky, aby obhájily svoji existenci.

Celkem 44 % respondentů, kteří čelili hospodářské kriminalitě, uvedlo, že utrpěli ztrátu ve výši minimálně 100 tisíc dolarů. Ve srovnání s výsledky průzkumu z roku 2011 došlo k nárůstu obětí tohoto typu podvodu o šest procentních bodů. Jedná se o ztrátu těch společností, které se obvykle snaží podvodům předcházet a odhalovat je. O kolik větší by byla ztráta, kdyby společnosti nevynakládaly úsilí a nepodnikaly kroky k prevenci a detekci podvodů?

Kromě čistě finančních ztrát trpí společnosti i v dalších oblastech. Jako největší nefinanční újmu hodnotí podle celosvětových výsledků negativní dopad na dobré jméno organizace či značky. Nezanedbatelný je i vliv na morálku zaměstnanců.

V tomto ohledu bychom rádi upozornili na fakt, že negativní dopad na morálku zaměstnanců může být příčinou dalších následných podvodů, kterých se frustrovaní či demotivovaní zaměstnanci dopouštějí. Slovy „dělají to všichni“ nebo „patří jim to“ si podvodníci již mnohokrát zdůvodnili své první podvodné jednání!

## Řízení podvodů

### *Kdo páchá podvody*

Pokusili jsme se sestavit profil pachatele nejzávažnějších případů hospodářské kriminality, kterým dotazované společnosti čelily.

Podíl interních a externích pachatelů je téměř vyrovnaný (49 % : 51 %). Není překvapením, že u zaměstnanců středního a vyššího vedení společnosti je větší pravděpodobnost, že dojde ke spáchání závažného podvodu, než v případě řadových zaměstnanců. Typickým podvodníkem je muž ve věku mezi 31 a 40 lety, který strávil ve společnosti od tří do pěti let. V případě externích pachatelů je podíl zástupců či zprostředkovatelů (22 %) vyšší než zákazníků (17 %) či dodavatelů (9 %).

Zástupci a zprostředkovatelé mají důvěru poškozené společnosti. Mohou také detailně znát její postupy. Pracují více méně samostatně, takže je složitější mapovat jejich činnost.

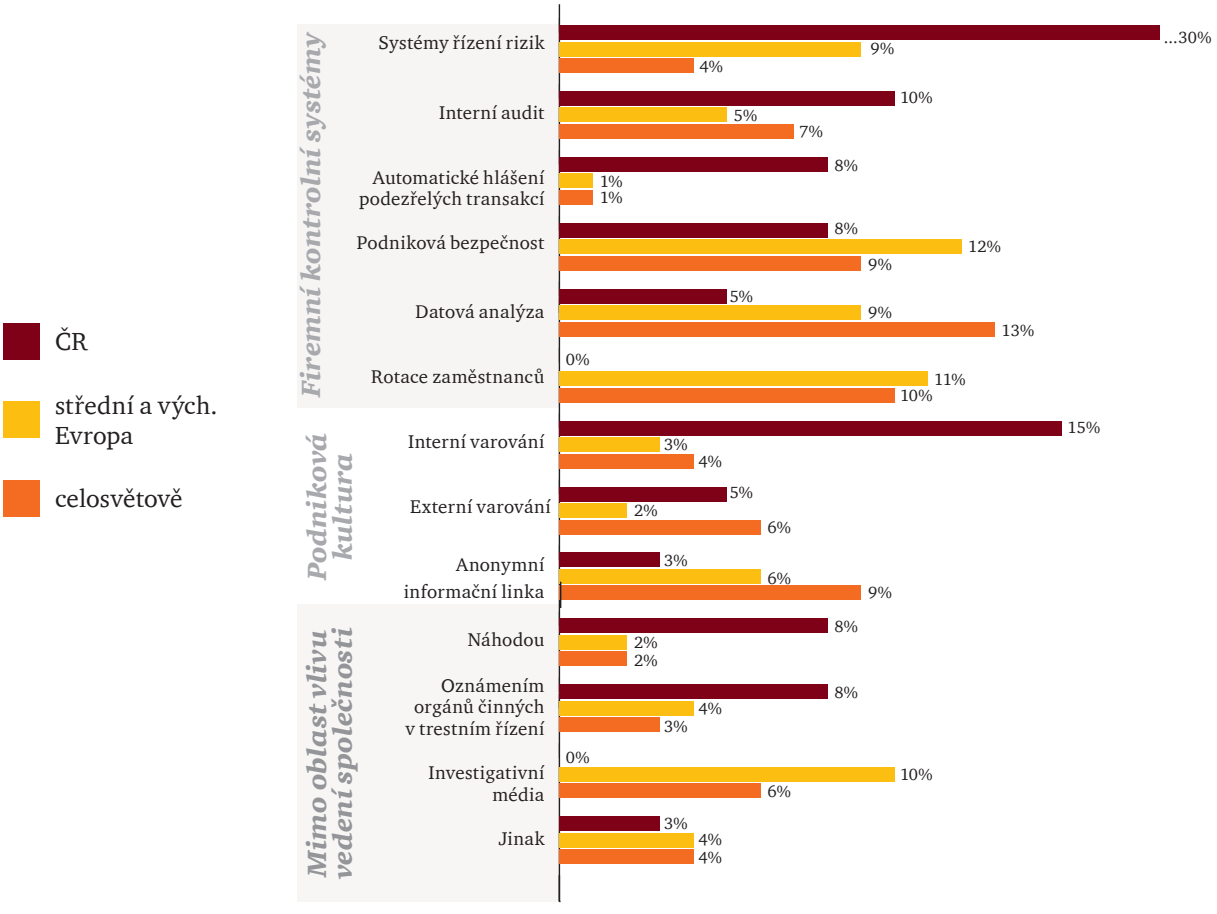
Z tohoto důvodu doporučujeme společnostem přemýšlet o způsobu, jak předejít podvodům, které spáchali zástupci a zprostředkovatelé, nebo jak takové podvody identifikovat v co nejkratším čase. Jako notoricky známý příklad lze uvést podvod organizovaný zástupci pojišťovny nebo úvěrové společnosti. Někdy jsou tyto podvody připravovány organizovanou skupinou podvodníků, která pronikla do řad zprostředkovatelů společnosti. V odůvodněných případech se prověřování obchodních partnerů a jejich vztahů s třetími stranami (takzvaný background check) jeví jako nezbytnost.

## *Prevence podvodů*

Proč se někdo rozhodne spáchat podvod? Náš průzkum ukazuje, že u interních pachatelů je nejvýznamnější podmínkou jednoznačně příležitost (86 %).

Zároveň příležitost představuje ze všech předpokladů pro realizaci podvodu faktor, který je pod kontrolou společnosti nejvíce. Proto je kontrola procesů v oblastech, které jsou k podvodům nejnáchylnější, efektivním způsobem, jak snížit riziko podvodu.

### Odhalení podvodů




Hodnoty jsou zaokrouhleny na nejbližší celá čísla

Výsledky průzkumu ukazují, že společnosti neberou hospodářskou kriminalitu na lehkou váhu. Je povzbuzující, že 40 % českých společností odhalilo hospodářský podvod díky systému řízení rizik podvodů či interními auditními procesy. Obdobně jako ve výsledcích z roku 2011 jsou tyto hodnoty výrazně nad celosvětovým průměrem (11 %).

Na druhou stranu je zde stále prostor pro přímočařejší kroky. Využití analytických metod (5 %) je pod celosvětovým průměrem (13 %). Tyto výsledky naznačují zdrženlivý přístup českých společností k využití IT detekčních systémů, přestože se při správném použití mohou stát nákladově velmi efektivním doplňkem k tradičním metodám.

První reakcí většiny společností v České republice, když odhalí potenciální podvod, je vydat se cestou interního vyšetřování (80 %). V mnoha případech také vyhledají pomoc externích právních poradců (22 %). Podle průzkumu se většina společností v České republice spoléhá spíše jen na tyto možnosti a nevyužívá ve vyšetřování znalostí forenzních specialistů (jen 11 % v porovnání s 20 % celosvětově) ani konzultací se svými auditory (9 % v České republice, 21 % ve střední a východní Evropě a 28 % celosvětově).

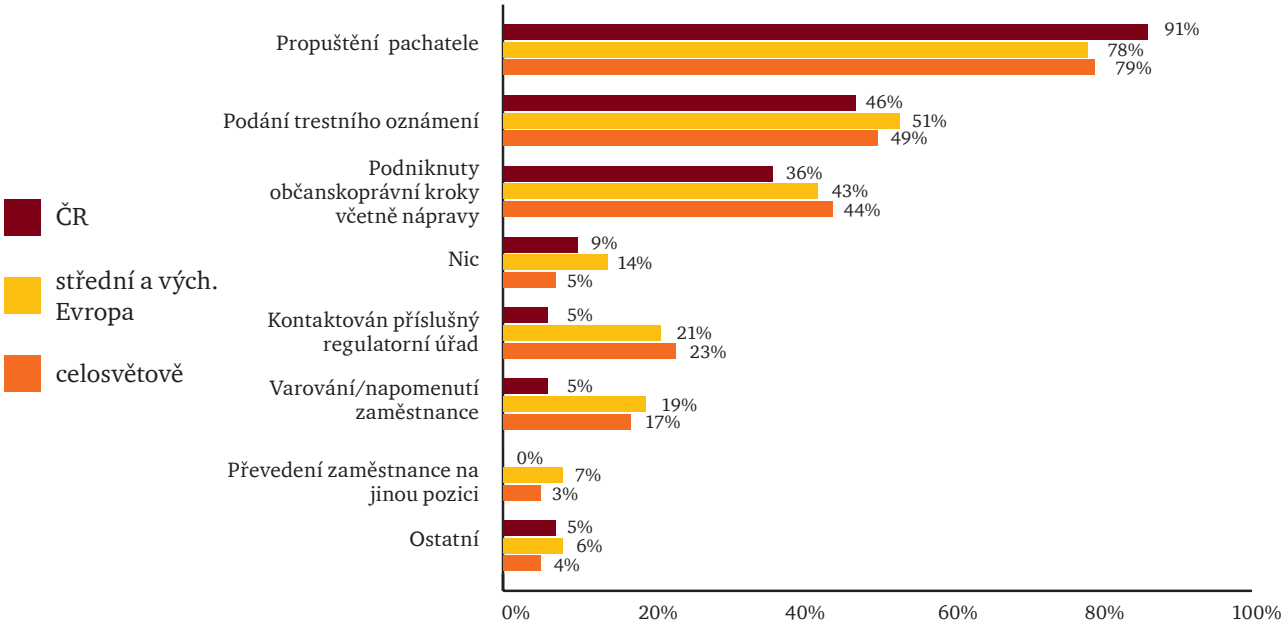
## Reakce společností po odhalení podvodu


## *Nápravná opatření*

Průzkum ukázal jednoznačný postoj většiny společností jak k interním, tak i k externím pachatelům podvodů. Propuštění interních pachatelů (91 %) je dokonce ještě častější než v předchozím průzkumu (81 %) a průzkumu z roku 2009 (65 %). To naznačuje zlepšující se povědomí společností o nákladnosti podvodů. Obzvláště v dobách ekonomické nestability, kdy je jen málo důvodů brát podvody na lehkou váhu.

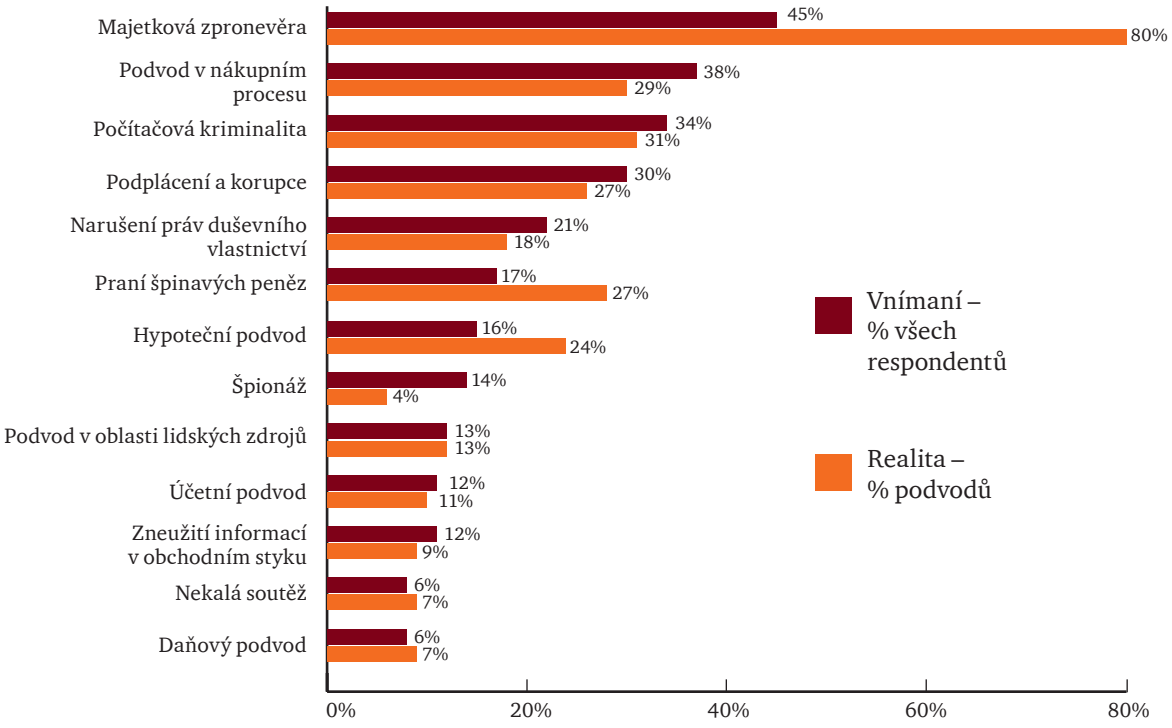
V případě externích podvodníků propuštění samozřejmě není možné. Nicméně 70 % českých společností v reakci na podvody externích pachatelů přerušilo obchodní vztahy. Je rovněž povzbuzující, že poměrně často dojde k podání trestního oznámení (83 %). Ve srovnání s celosvětovým průměrem (61 %) je to jednoznačně častěji.

### Nápravná opatření vůči interním pachatelům podvodů



## Očekávání

V rámci průzkumu jsme se také zaměřili na to, jaká jsou očekávání společností v oblasti vývoje hospodářské kriminality v následujících 24 měsících a jakým typům podvodů budou, podle svého názoru, v tomto časovém horizontu čelit. Tyto odpovědi silně závisí na vnímání možných rizik jednotlivými dotazovanými společnostmi. Nejde tedy o skutečnou míru rizika. I přesto je užitečné porovnat rizika očekávaná v budoucnu se současnou skutečnou mírou výskytu. Zajímavým zjištěním je, že navzdory uváděnému výskytu majetkové zpronevěry se zdá, že společnosti tento typ podvodů podceňují.



# *Kontakt*


***Sirshar Qureshi***
partner zodpovědný za Forenzní služby v CEE regionu
+420 251 151 235
sirshar.qureshi@cz.pwc.com

***Michal Kohoutek***
vedoucí oddělení Forenzních služeb
+420 251 151 231
michal.kohoutek@cz.pwc.com

***Pavel Jankech***
senior manažer
oddělení Forenzních technologií
+420 251 151 336
pavel.jankech@cz.pwc.com

***Kateřina Halásek Dosedělová***
senior manažerka, Forenzní služby
+420 251 151 293
katerina.halasek-dosedelova@cz.pwc.com

***Jiří Urban***
senior manažer, Forenzní služby
+420 251 151 627
jiri.urban@cz.pwc.com

***Filip Volavka***
senior manažer
oddělení Forenzních technologií
+420 251 151 269
filip.volavka@cz.pwc.com



© 2014 PricewaterhouseCoopers Česká republika, s.r.o. Všechna práva vyhrazena. V tomto dokumentu, název „PwC“ označuje společnost PricewaterhouseCoopers Česká republika, s.r.o., která je členem sítě společností PricewaterhouseCoopers International Limited, z nichž každá je samostatným a nezávislým právním subjektem.

# La fraude continue à être une vraie menace pour les entreprises

**55 %**
des entreprises françaises ont été victimes d'une fraude au cours des 24 derniers mois

**43 %**
des fraudes reportées par les entreprises françaises ont été détectées grâce à l'analyse informatique des données

**44 %**
des entreprises françaises craignent à l'avenir un acte de cybercriminalité

pwc

# Sommaire

# *Édito*

Nous avons le plaisir de vous présenter l'édition 2014 de notre étude mondiale sur la fraude en entreprise. Notre enquête repose sur des questionnaires collectés auprès de plus de 5 000 entreprises réparties à travers le monde.

Notre étude apporte une analyse unique sur tous les aspects quantitatifs et qualitatifs relatifs à l'évolution de la fraude et aux pratiques des entreprises pour y faire face, que ce soit dans le monde ou plus particulièrement en France.

Le premier enseignement de l'édition 2014 est la poursuite de la progression de la fraude en France grâce à l'efficacité croissante des dispositifs de détection : 55 % des entreprises déclarent avoir subi des fraudes (contre 46 % en 2011) avec 43 % des fraudes détectées à travers l'identification des transactions inhabituelles (36 % en 2011). Cette pratique, combinée à l'application de lourdes sanctions pour les fraudeurs, doit à terme conduire à la régression de la fraude en France.

Ces mesures sont d'autant plus importantes que notre étude montre également que la fraude se transforme : si le détournement d'actifs reste toujours et de loin la catégorie la plus fréquente, on relève l'émergence de nouvelles typologies de fraude plus complexes : la cybercriminalité, avec 28 % des entreprises touchées en France, et la « fraude au Président », particularité française, avec un taux de 10 % et un coût dépassant parfois la dizaine de millions d'euros.

Enfin, ce sont la cybercriminalité et la fraude aux achats qui sont parmi les fraudes les plus redoutées à l'avenir par les entreprises françaises (44 % et 35 % respectivement) mais celles-ci ne doivent pas non plus négliger les risques liés à la corruption lorsqu'elles s'implantent dans des pays sensibles.

Depuis notre première étude, menée en 2001, nous cherchons à faire progresser la lutte contre la fraude à travers l'analyse des témoignages des entreprises. Nous espérons que l'édition 2014 apportera une contribution utile aux entreprises.

Dominique Perrier

Jean-Louis Di Giovanni

*Le nombre de fraudes reportées par les entreprises françaises a presque doublé depuis 2009*

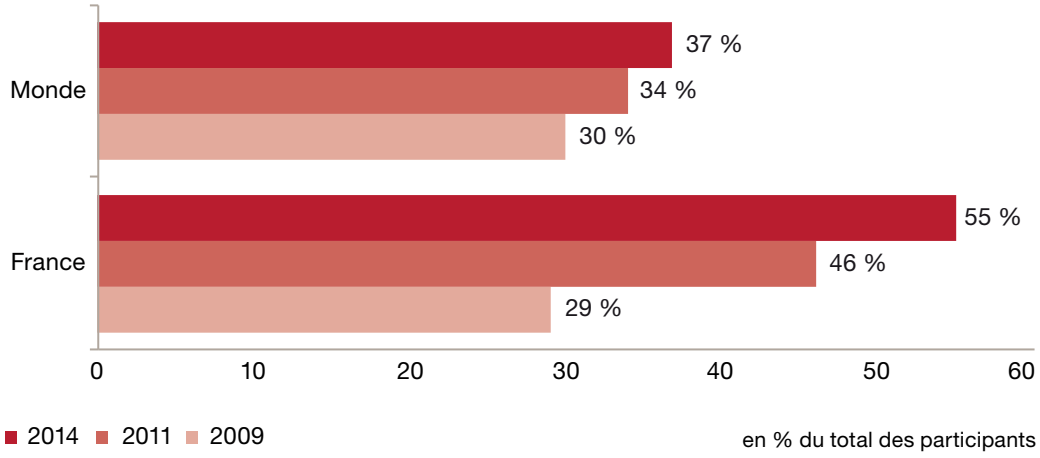
# La fraude en constante augmentation depuis 2009

La fraude demeure une préoccupation majeure des entreprises dans le monde et plus particulièrement en France puisque plus d'une entreprise sur trois ayant participé à notre étude dans le monde (37 %) et plus de la moitié des entreprises en France (55 %) ont été victimes d'une fraude au cours des 24 derniers mois.

Ces chiffres sont en constante augmentation par rapport aux deux précédentes éditions de notre étude comme le montre le graphique ci-dessous.

En effet, le nombre de fraudes reportées par les entreprises françaises a presque doublé depuis 2009 (+26 points) !

**Fraudes reportées par les entreprises**




Néanmoins, ces résultats ne doivent pas être mal interprétés car, à notre avis, l'augmentation des fraudes reportées n'indique pas nécessairement que les entreprises sont plus affectées par ce phénomène mais ils démontrent surtout que les entreprises sont mieux armées pour les détecter.

En effet, depuis la crise de 2008, les entreprises ont pris conscience que lutter contre la fraude peut leur permettre d'éviter non seulement des coûts financiers importants mais aussi de nuire à leur image, leur réputation et par conséquent, à leur activité.

Cette prise de conscience s'est généralement traduite par la mise en place de systèmes de détection efficaces reposant sur des analyses de données. Ces systèmes permettent de mieux identifier les cas de fraude ce qui explique, en partie, la forte augmentation des fraudes reportées par les entreprises tant au niveau mondial qu'au niveau français.

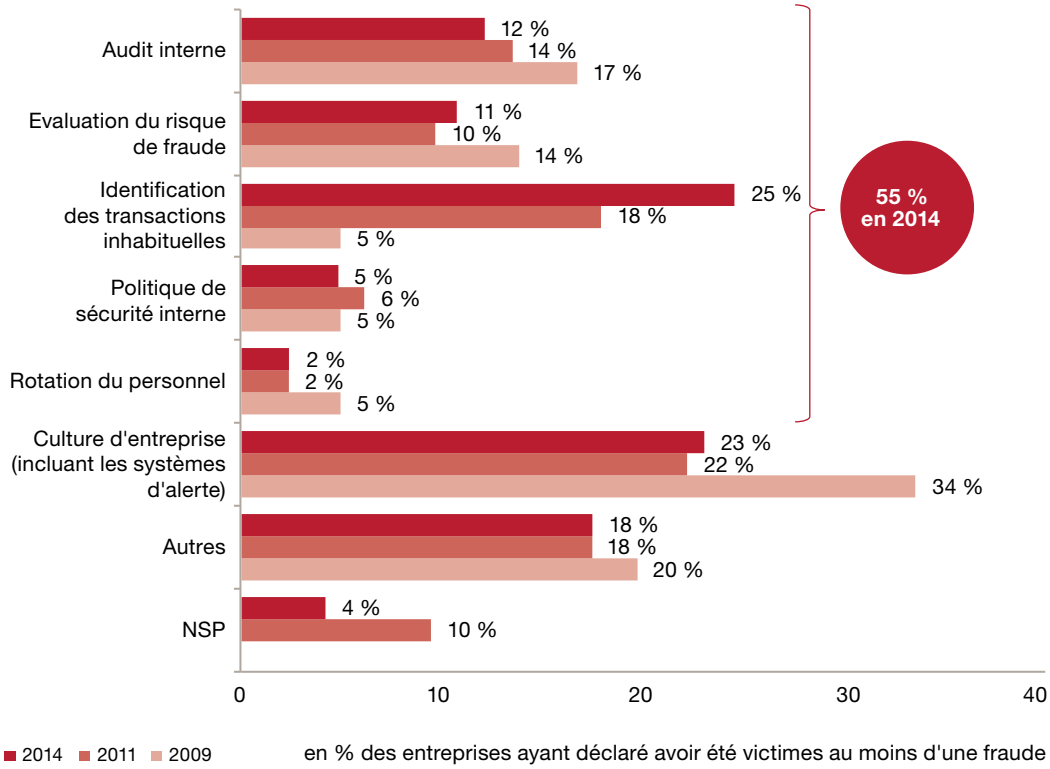
Un autre facteur contribue, à notre avis, aussi à ce phénomène. C'est l'avènement de la cybercriminalité ou criminalité informatique comme le second risque de fraude le plus reporté en France et Europe de l'Ouest après le détournement d'actifs, devant la fraude comptable et la corruption.

# *La fraude de mieux en mieux détectée grâce à l'analyse informatique des données*

Les modes de prévention et de détection des fraudes s'articulent généralement autour de trois principales composantes : les dispositifs de contrôle au sein des entreprises, la culture d'entreprise et la détection par « accident » ou par « hasard ».

Le graphique ci-dessous donne un aperçu des modalités d'identification des fraudes qui nous ont été reportées au cours des trois dernières éditions de notre étude. Il apparaît notamment que les dispositifs de détection et de prévention, au sens large, constituent le mode opératoire le plus efficace, puisqu'ayant permis d'identifier plus de 55 % des fraudes reportées dans le monde, ce pourcentage étant même de 62 % en France.

**Modes de détection**




Cette année, les résultats de notre étude confirment que la découverte d'une fraude est de moins en moins le fruit du hasard, mais que celle-ci est clairement corrélée à la montée en puissance de nouveaux modes de détection que sont l'analyse de données (« Data Analytics ») et l'identification des transactions inhabituelles (« Suspicious Transaction Reporting »)[1].

1 Ces deux modes de détection sont regroupés au sein de la catégorie « Identification des transactions inhabituelles ».

## *La France est devenue l'un des pays leaders de la détection des fraudes via l'analyse informatique des données*

En effet, notre étude 2014 confirme, d'une part, la tendance historique selon laquelle près d'une fraude sur quatre est détectée au travers des systèmes de remontée des alertes, qu'ils soient formels ou informels, mais, elle montre surtout que plus d'un quart des fraudes reportées ont dorénavant été identifiées à l'aide d'un système de détection automatisé, soit une augmentation de sept points par rapport à notre précédente étude (2011) et de vingt points par rapport à 2009 !

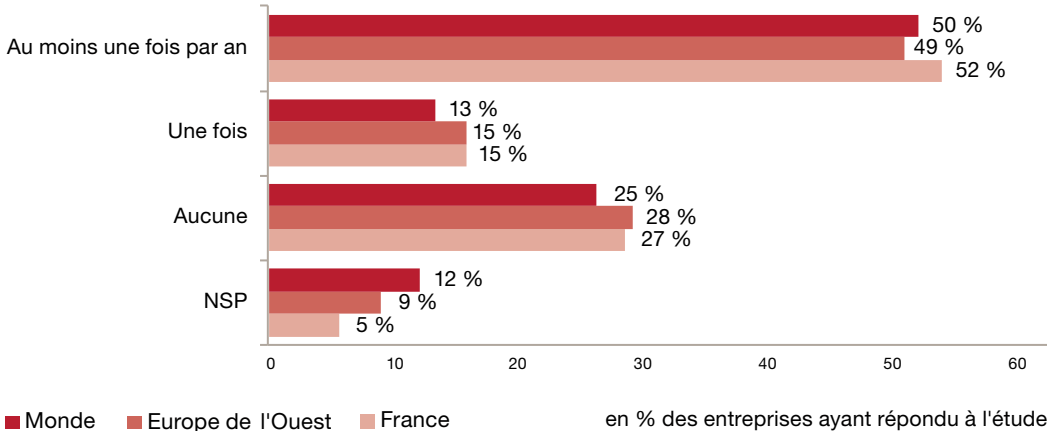
Une meilleure connaissance de ces modes de détection permet dorénavant aux entreprises de concevoir des procédures de contrôle « sur mesure » pour en accroître l'efficacité et la pertinence. Ceci est d'autant plus vrai si cette mise ne place s'est préalablement accompagnée d'un exercice d'évaluation du risque de fraude ou de cartographie du risque de fraude.

Sur les marchés plus matures que sont l'Europe de l'Ouest et la France, la corrélation entre le niveau de fraudes reportées et l'utilisation de ces systèmes de détection automatisés est plus forte qu'au niveau mondial. La proportion de fraudes détectées par ce biais est respectivement de 31 % et 43 % en Europe de l'Ouest et en France. En 2014, la France est devenue un des pays leaders de la détection via l'analyse informatique des données disponibles au sein des systèmes de l'entreprise [2] !

Notre étude 2014 révèle en outre la très forte corrélation entre la mise en œuvre d'une évaluation du risque de fraude et la découverte d'une fraude.

Notons à ce titre qu'une entreprise sur deux se livre au moins une fois par an à une évaluation du risque de fraude comme présenté dans le graphique ci-dessous.

**Pourcentage des entreprises ayant procédé ou pas à une évaluation du risque de fraude au cours des 24 derniers mois**

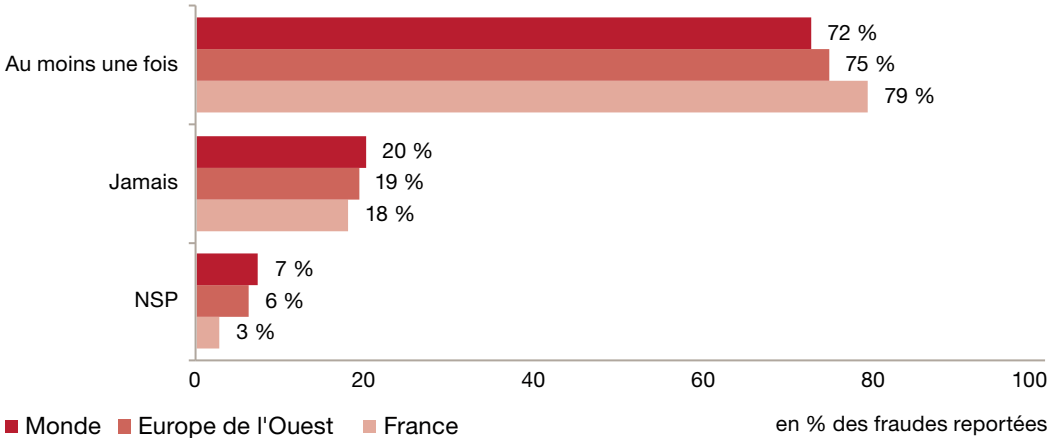



2 Pour les pays ayant obtenu plus de 50 réponses à notre étude.

Les résultats de notre étude pour la France illustrent bien ce constat puisque près de 80 % des entreprises françaises ayant reporté au moins une fraude avaient, au préalable, réalisé une évaluation de leur risque de fraude.

Au niveau mondial, la tendance est également cohérente avec 72 % des entreprises alors que ce pourcentage tombe à 20 % pour les entreprises qui ne se sont jamais livrées à ce type de travaux.

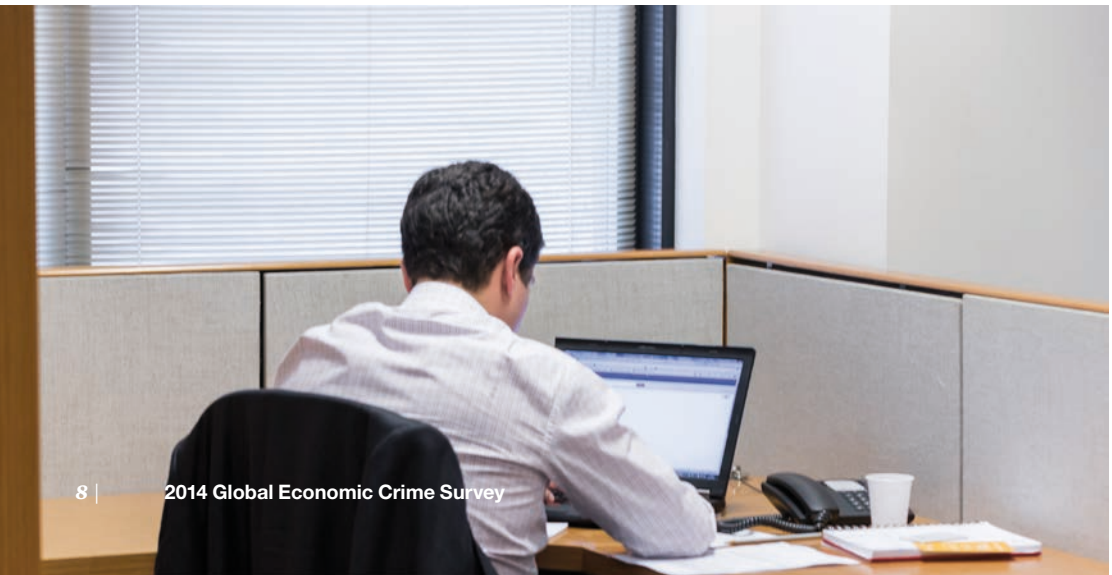
**Analyse de la corrélation entre les travaux d'évaluation du risque de fraude et la découverte de fraudes au sein des entreprises**




La forte corrélation observée confirme la pertinence de cette approche notamment si elle est combinée à la mise en œuvre de nouveaux modes de détection reposant sur l'analyse informatique des données disponibles au sein des systèmes de l'entreprise.

Par ailleurs, nous pouvons déduire de cette étude qu'il existe un vivier potentiel de fraudes non détectées au sein des entreprises qui ne se sont jamais prêtées à un exercice d'évaluation du risque de fraude.

Il est également intéressant de constater que pour les pays historiquement plus matures que la France en termes de lutte contre la fraude via l'analyse de données comme par exemple le Royaume-Uni, le pourcentage de fraudes reportées a baissé en passant de 51 % en 2011 à moins de 45 % en 2014, soit un recul de plus de six points. En effet, après une phase globalement ascendante entre 2009 et 2011 et une augmentation significative des fraudes reportées liée à la mise en place de ces systèmes détectifs automatisés, le Royaume-Uni récolte à présent les fruits de ses investissements. La baisse du nombre de fraudes reportées reflète l'effet dissuasif à moyen/long terme de ce type de dispositif. Ceci est d'autant plus vrai si l'entreprise communique sur l'existence de ces contrôles ce qui aura pour effet, in fine, de clairement faire savoir au fraudeur qu'il est dorénavant surveillé.



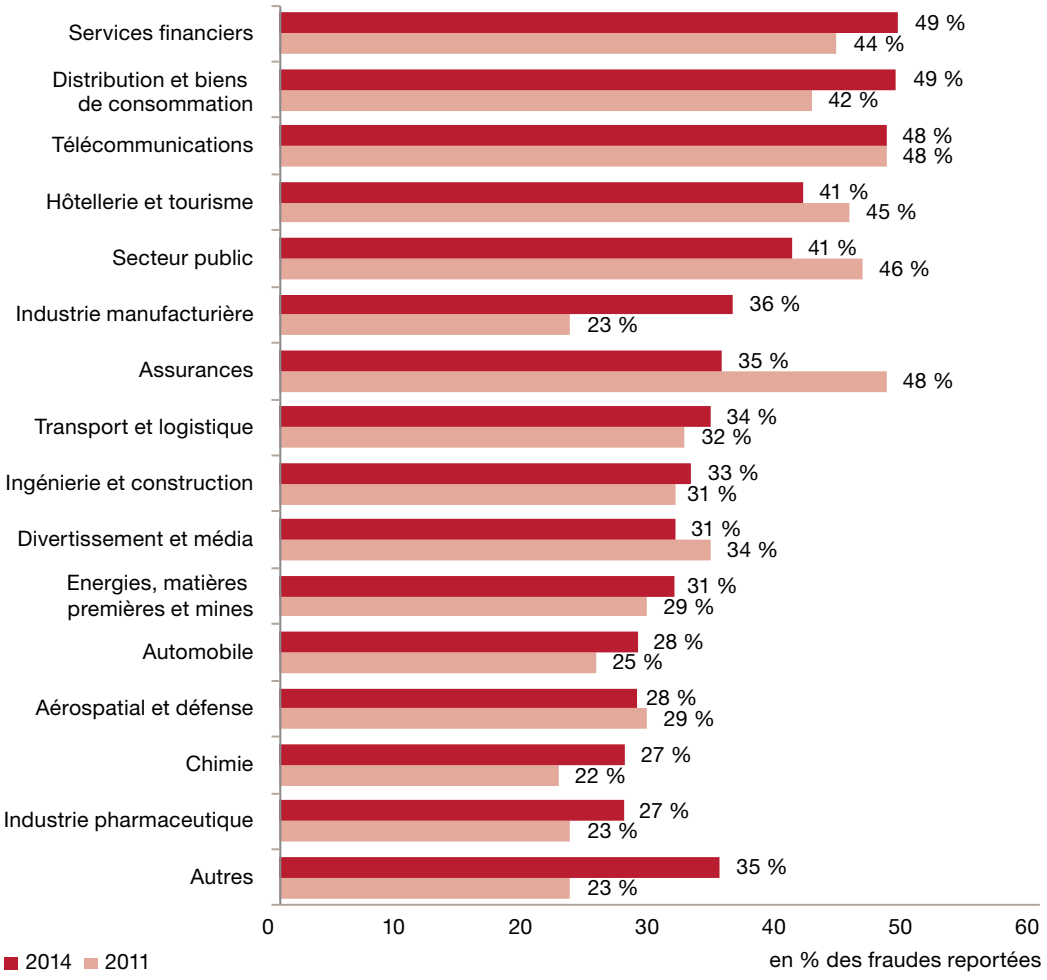
# *Les services financiers et la distribution sont les secteurs les plus touchés par la fraude*

Comme lors des précédentes études, l'étude 2014 montre que tous les secteurs d'activité sont victimes de fraudes. Cependant, certains secteurs sont plus touchés que d'autres.

Ainsi, il apparaît que les services financiers (49 %) et la distribution (49 %) sont les secteurs les plus touchés, mais à une différence près : la prédominance de la fraude externe pour les services financiers (59 %) et a contrario, de la fraude interne pour la distribution (67 %).

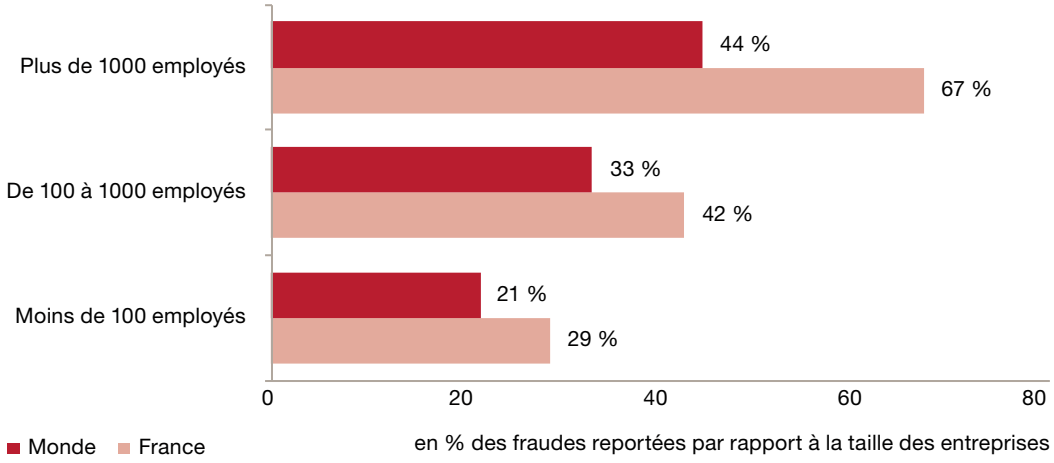
Il faut également noter la diminution historique des fraudes reportées par le secteur des assurances pour lequel on observe une baisse de plus de douze points par rapport à notre précédente étude : 35 % en 2014 contre 48 % en 2011 alors que ce secteur d'activité figurait toujours parmi les plus touchés. Cette baisse semble, pour partie, s'expliquer par la diminution du nombre de fraudes externes reportées.

**Fraudes reportées par secteur d'activité**



Notre étude 2014 met aussi en exergue la forte corrélation entre la taille des entreprises et le nombre de fraudes détectées et, par extension, reportées.

**Fraudes reportées selon la taille des entreprises**




Cependant, ce constat est à nuancer. En effet, bien que les entreprises de plus de 1 000 employés soient les plus touchées, il ressort de notre étude que le nombre de fraudes reportées par ces dernières au niveau mondial est en baisse après un pic observé lors de notre précédente enquête : le nombre de fraudes reportées est passé de 54 % en 2011 à 44 % en 2014, soit une baisse de dix points. Le retrait ainsi observé peut pour partie s'expliquer par la maturité atteinte par les plus grandes entreprises dans la lutte contre la fraude.

Pour les entreprises de plus petite taille, malgré la nette progression du nombre de fraudes reportées, il apparaît que celles-ci sont encore en retard par rapport aux entreprises de plus grande taille qui ont la capacité d'investir plus massivement dans des dispositifs de prévention et de détection.

Toutefois, l'écart entre les grandes et les plus petites entreprises se réduit. En effet, il ressort aujourd'hui qu'une grande entreprise détecte 2,1 fois plus de fraudes que les plus petites alors que ce ratio était de 3,2 en 2011.

La France se démarque dans ce paysage avec un nombre de fraudes reportées bien supérieur à la moyenne mondiale quelle que soit la taille de l'entreprise considérée.

*La fraude aux achats a directement été propulsée à la seconde place des fraudes les plus reportées dans le monde*

# Quels sont les principaux types de fraudes reportées ?

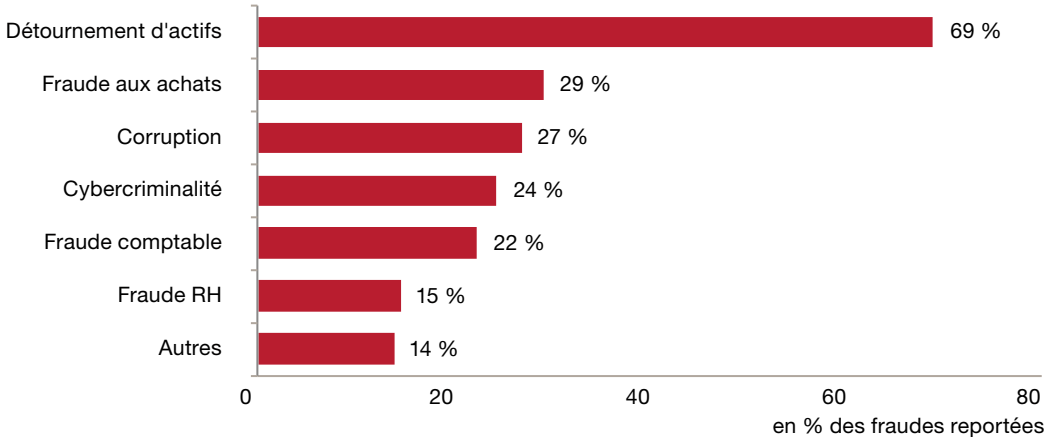
La fraude économique peut prendre de multiples formes. Traditionnellement, les types de fraudes les plus communément signalées par les entreprises depuis des années, dans le cadre de cette étude, reposaient sur le triptyque suivant : détournement d'actifs, fraude comptable et corruption.

Ainsi, comme à chacune des éditions de l'étude, le détournement d'actifs est la typologie de fraude la plus reportée, représentant près de 70 % des fraudes survenues dans le monde. Il convient de rappeler que ces fraudes portent généralement sur des montants en valeur moins importants mais que leur nombre peut parfois engendrer des coûts significatifs pour l'entreprise du fait de leur répétition.

Une nouveauté cette année : nous avons introduit une nouvelle catégorie de fraude qui peut être considérée comme à la croisée des chemins du détournement d'actifs et de la corruption, à savoir la fraude aux achats.

La fraude aux achats a, dès son introduction dans notre étude, directement été propulsée à la deuxième place des fraudes les plus reportées dans le monde avec 29 % !

**Types de fraudes reportées par les entreprises dans le monde**



## *Une spécificité bien française : la fraude au « Président »*

La corruption, quant à elle, gagne trois points par rapport à notre précédente étude et demeure la troisième catégorie de fraude la plus reportée au niveau mondial. Cette tendance peut pour partie s'expliquer par l'entrée en vigueur, depuis notre dernière étude, de nouvelles réglementations contraignantes dans certains pays (Royaume-Uni, Italie, etc.) qui en ont fait une problématique majeure à gérer par les entreprises dans le cadre de la définition de leurs dispositifs anti-fraude, notamment en raison du caractère extraterritorial de ces lois.

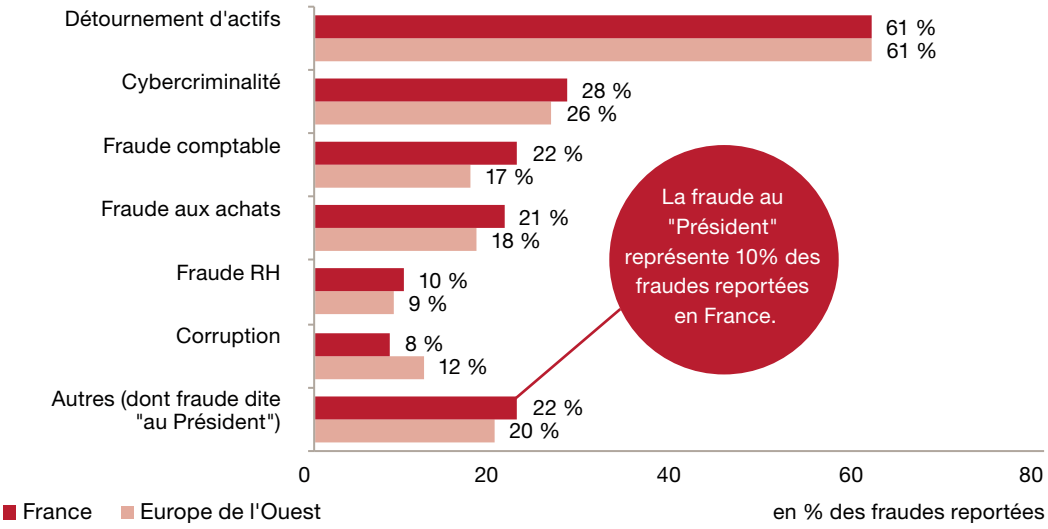
Pour ce qui concerne la fraude comptable, celle-ci recule à la cinquième place. Notre étude 2011 avait déjà entériné une baisse de ce type de fraude qui perdait près de 14 points entre 2009 et 2011 pour s'établir à 24 %. Cette tendance s'est dorénavant stabilisée puisque 22 % des entreprises ayant répondu à notre enquête cette année disent avoir été victimes de fraudes comptables.

Autre point mais non des moindres, la cybercriminalité ou criminalité informatique confirme sa quatrième place dans le classement établi pour les besoins de cette étude avec 24 % des fraudes détectées dans le monde.

Il est particulièrement intéressant de constater que, depuis notre dernière étude, la cybercriminalité est devenue le second type de fraude le plus reporté en Amérique du Nord, en France et au Royaume-Uni.

À titre d'exemple, 35 % des entreprises d'Amérique du Nord ayant été victimes de fraude ont reporté des cas de cybercriminalité. En France et en Europe de l'Ouest, la tendance est identique, ce chiffre étant de respectivement 28 % et 26 %. Dorénavant, la cybercriminalité représente en France le second type de fraude le plus reporté après le détournement d'actifs et devant la fraude comptable et la fraude aux achats !

**Types de fraudes reportées par les entreprises en France et en Europe de l'Ouest**




Notons en dernier lieu une spécificité bien française. Depuis quelques années, les entreprises de notre pays sont victimes d'une fraude externe communément appelée la fraude « au Président ».

En effet, des entreprises de toutes tailles ont subi de très nombreuses tentatives d'escroqueries, parfois couronnées de succès, fondées sur des modèles similaires ou proches consistant à ce qu'un fraudeur, se faisant passer pour le Président de la société, téléphone à un comptable habilité à effectuer des paiements pour lui demander d'effectuer un virement bancaire à l'étranger pour financer, par exemple, une acquisition confidentielle.

Il ressort des résultats obtenus lors de cette étude que près de 10 % des entreprises françaises interrogées ont été victimes de cette fraude. Les préjudices peuvent être très conséquents : de quelques centaines de milliers à plus de dix millions d'euros pour les fraudes les plus importantes !

Ces fraudes sont généralement réalisées par des bandes très organisées. En effet, avant de mettre en œuvre leur stratagème, les fraudeurs se sont particulièrement bien renseignés sur l'entreprise, ses dirigeants, ses circuits de décision et son mode de fonctionnement et ce, à partir des informations publiques disponibles mais aussi à l'aide des informations postées sur les réseaux sociaux. En outre, les fraudeurs ont l'assurance, la capacité de conviction nécessaires et savent utiliser tous les ressorts psychologiques (pression, persuasion et menaces) pour convaincre leur victime du bien-fondé de leur demande.

Nous allons maintenant revenir en détail sur trois types de fraude, à savoir la fraude aux achats, la cybercriminalité et la corruption.

# La fraude aux achats : une réelle menace pour les entreprises

Comme évoqué précédemment, nous avons fait figurer pour la première fois dans l'étude 2014 la fraude aux achats.

Rappelons qu'au niveau mondial, 29 % des entreprises ayant répondu à notre enquête ont déclaré en avoir été victimes sachant qu'en France ce pourcentage est de 21 %.

Typiquement, toutes les entreprises sont confrontées à ce type de risque dès lors qu'elles doivent acquérir des biens et services et ce plus particulièrement en amont, au moment de la sélection du fournisseur (détermination des fournisseurs consultés, définition du cahier des charges et appel d'offres à proprement dit).

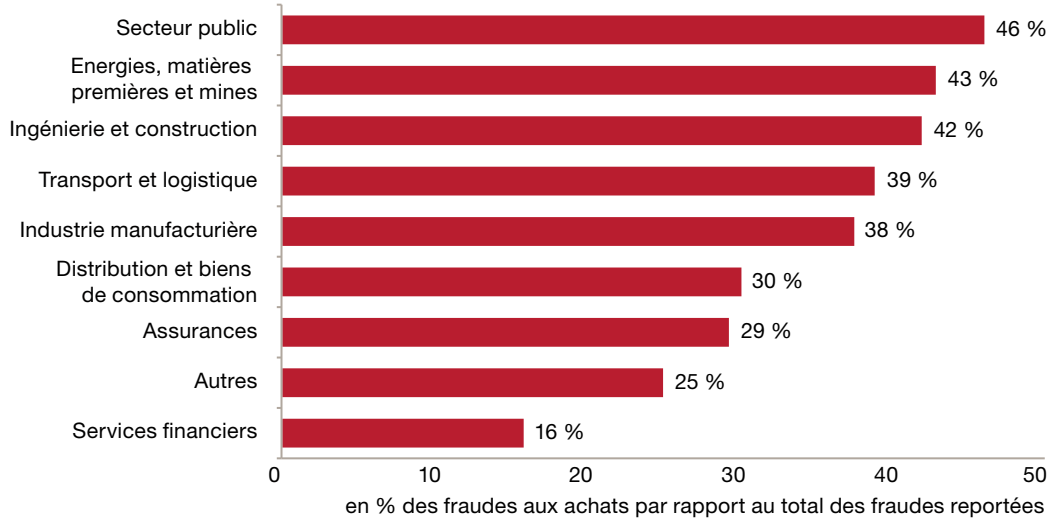
Il ressort de notre étude que ce type de fraude trouve principalement son origine dans les facteurs décrits ci-après :

- comme souligné par notre récente étude auprès de 1 344 chefs d'entreprise (« 2014 Global CEO Survey »), la recherche d'économies d'échelle par les entreprises conduit à la globalisation de la fonction achats ce qui concentre les pouvoirs de décision et, par là même, accroît le risque de fraude ;

- le recentrage de l'activité des entreprises depuis la crise de 2008 vers leur cœur de métier en externalisant une partie de leurs fonctions support, dont la fonction achats, peut également accroître le risque de fraude.

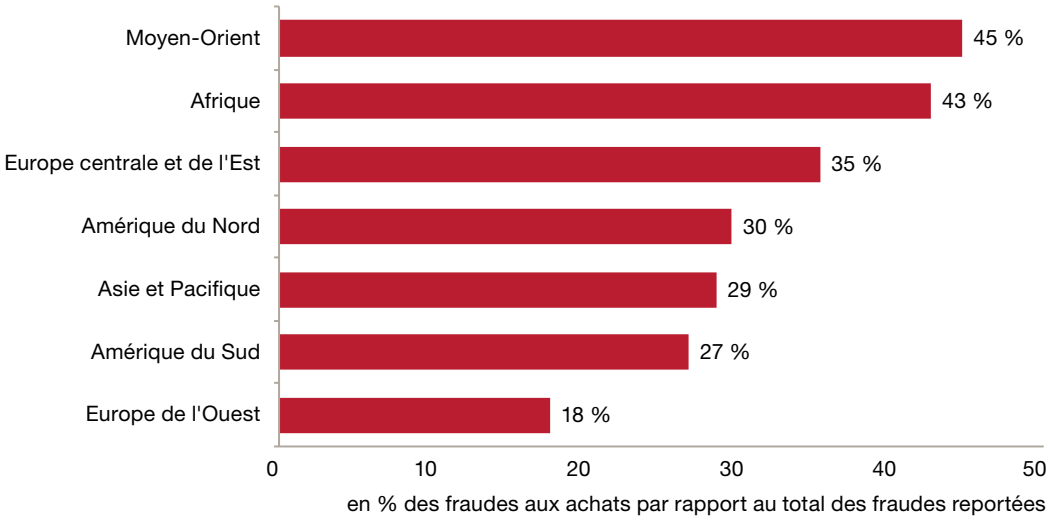
C'est le secteur public et les secteurs qui y sont fortement liés qui sont les plus touchés par ce phénomène : 46 % du total des fraudes reportées par le secteur public sont des fraudes aux achats, 43 % pour le secteur de l'énergie et 42 % pour le secteur de l'ingénierie & la construction[3].

**Part de la fraude aux achats dans le total des fraudes reportées par secteur d'activité**




De plus, ce sont les zones géographiques avec un secteur public fort, un important secteur de l'énergie et de grands projets d'infrastructures en cours qui sont les plus touchées par la fraude aux achats comme le révèle le graphique ci-dessous.

**Part de la fraude aux achats dans le total des fraudes reportées par zone géographique**




En réalité, la fraude aux achats a toujours été un risque majeur pour les entreprises notamment via des schémas conduisant, in fine, à une surfacturation. Lors de nos précédentes études, ces typologies de fraude étaient incluses dans les détournements d'actifs.

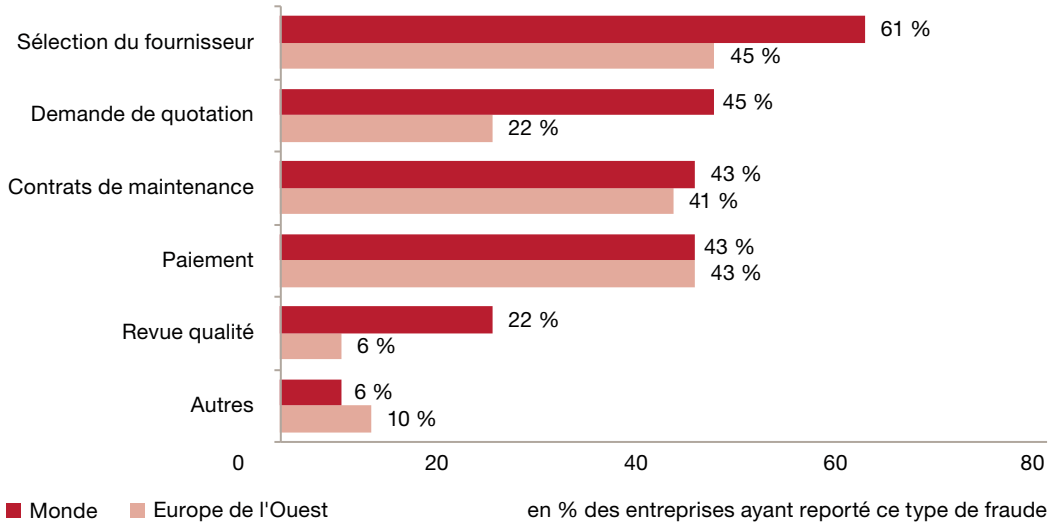
Cependant, notre expérience sur le terrain démontre que les mécanismes sont généralement plus élaborés et que les fraudeurs au sein des services achats agissent rarement seuls.

3 Seuls les secteurs ayant reporté plus de 70 cas de fraudes sont représentés dans le graphe ci-dessus.

## *Près de deux tiers des fraudes aux achats reportées interviennent lors de la phase de sélection du prestataire*

En effet, la difficulté majeure à gérer, pour ce type de fraude, réside principalement dans la collusion entre fournisseurs et acheteurs en amont du processus.

**A quel moment du processus "achat" survient la fraude ?**




Les résultats de notre étude corroborent effectivement notre propre expérience sur le terrain puisque près de deux tiers des fraudes aux achats reportées interviennent lors de la phase de sélection du prestataire.

La difficulté d'identifier ce type de malversations pour les entreprises rend indispensable la mise en place de procédures contraignantes incluant une forte séparation des tâches et des mécanismes de validation robustes lors de la sélection des fournisseurs.

# La cybercriminalité : un enjeu majeur pour des entreprises de plus en plus connectées

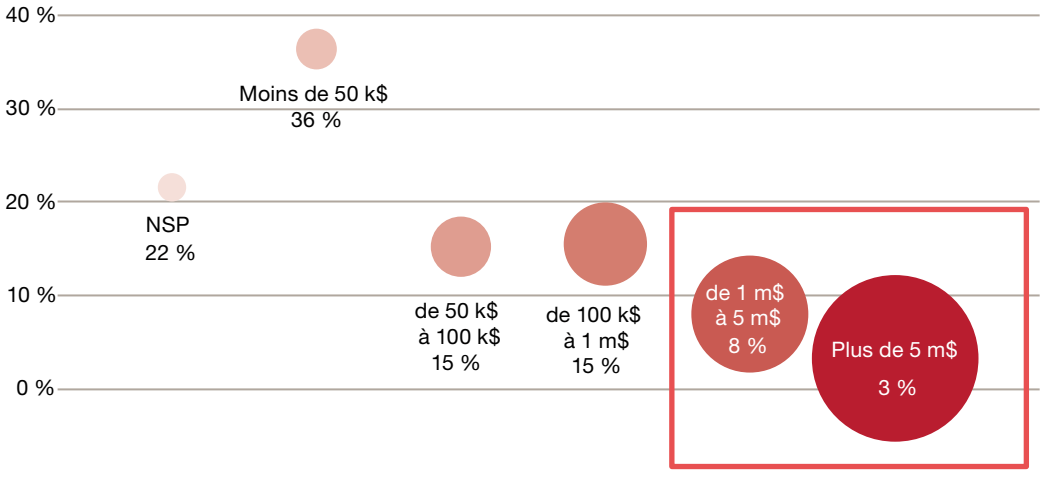
Les avancées technologiques au sein des entreprises et notamment la mobilité des équipements, l'augmentation de la quantité de données à protéger (80 % des données n'existaient pas il y a deux ans) ainsi que la recrudescence de l'utilisation des réseaux sociaux rendent les entreprises de plus en plus vulnérables à la cybercriminalité.

De plus, les progrès continuels de la technologie permettent aux fraudeurs d'avancer dans l'ombre et rendent leur détection et leur identification toujours très difficiles.

En 2011, lors de l'introduction de cette catégorie de fraude dans notre précédente étude, celle-ci est immédiatement ressortie comme une préoccupation majeure pour les entreprises.

Notre étude 2014 confirme cette tendance croissante puisque près d'un quart des entreprises ayant subi une fraude déclare qu'il s'agissait d'un acte de cybercriminalité. En outre, environ 11 % des entreprises victimes de cybercriminalité déclarent que l'incidence financière de ces attaques dépasse un million de dollars.

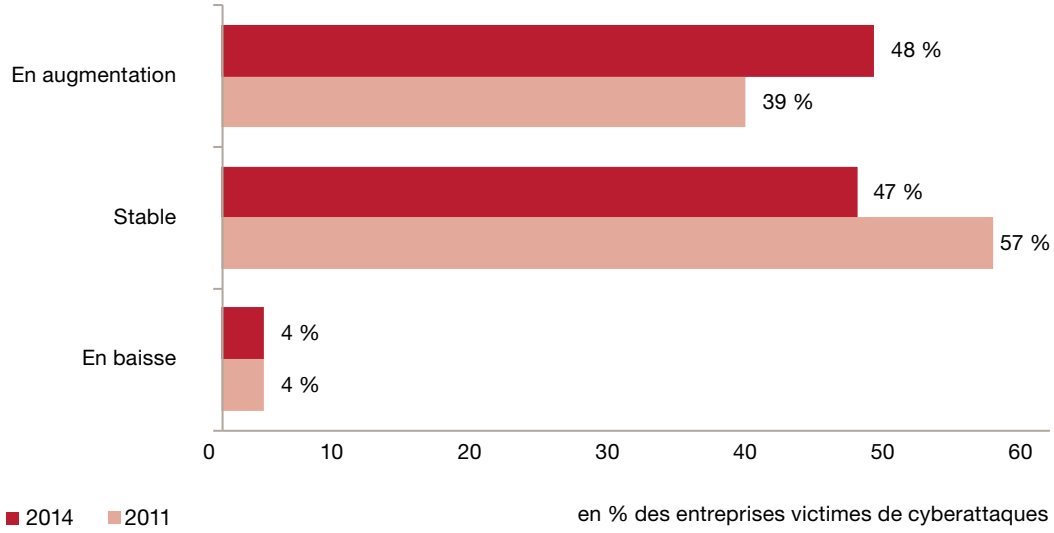
**Incidences financières pour les entreprises victimes de cybercriminalité**




en % d'entreprises victimes de cybercriminalité

De surcroît, nous constatons une évolution notable de la perception future de ce risque qui croît à un rythme plus élevé que les actes de cybercriminalité effectivement reportés. En 2011, 39 % des entreprises sondées se disaient inquiètes des risques inhérents à la cybercriminalité dans le futur contre 48 % cette année comme indiqué dans le graphique ci-après.

**Evolution de la perception du risque de cybercriminalité**




Cette tendance est également confirmée par les résultats de notre récente étude réalisée auprès de 1 344 chefs d'entreprise (« 2014 Global CEO Survey »), dans laquelle les présidents de sociétés indiquent à 48 % être inquiets des risques attachés à la cybercriminalité notamment concernant la sécurité des données.

En outre, il faut également prendre en compte le fait que certaines entreprises n'ayant pas reporté de fraude relative à la cybercriminalité ont pu néanmoins en être victimes. D'ailleurs, il apparaît ainsi que 22 % des entreprises ayant déclaré cette typologie de fraude ne connaissaient pas les dommages financiers en résultant.

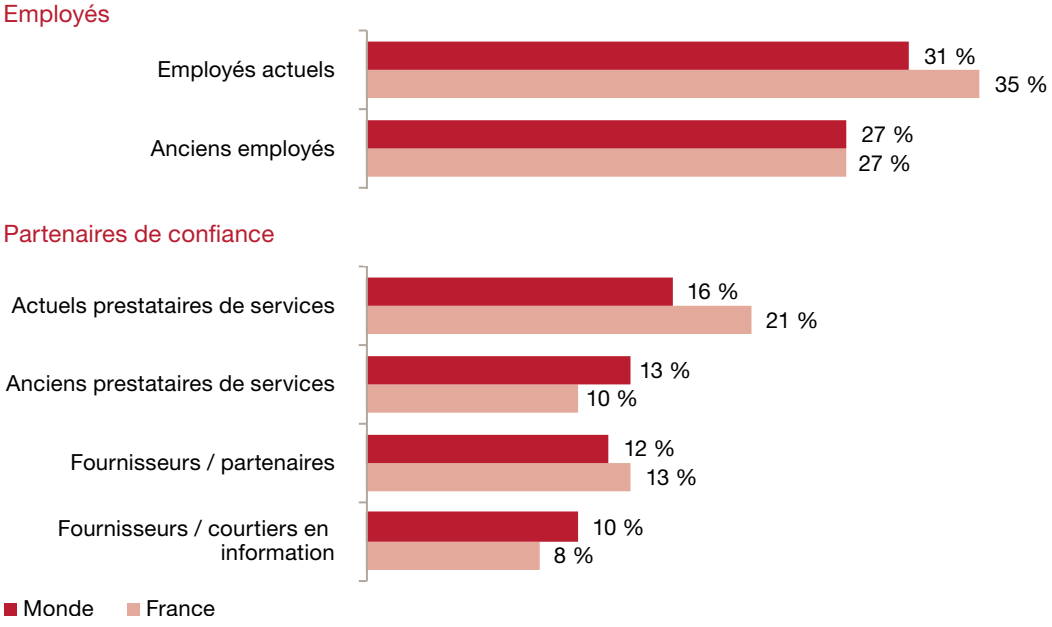
Il ressort de notre expérience que le nombre de fraudes de ce type est souvent sous-évalué par les entreprises qui ne désirent pas communiquer sur ce genre de dysfonctionnement car cela pourrait avoir des incidences significatives sur leur activité courante. À titre d'exemple, si des documents confidentiels d'un appel d'offres tombent entre les mains d'un hacker et sont utilisés par une entreprise malveillante, est-ce que l'entreprise qui a subi cette fraude la reportera ? Rien n'est moins sûr !

# *Cybercriminalité : la plupart des menaces proviennent de sources internes à l'entreprise*

En réalité, les dommages causés par la cybercriminalité ne sont pas systématiquement déclarés, bien au contraire, soit parce que les organisations n'ont pas pu les détecter, soit parce que les dommages sont trop difficiles à quantifier, soit en raison des faiblesses sous-jacentes que les entreprises risquent de mettre à jour.

En outre et malgré les idées reçues, il ressort également de notre étude 2014 sur la sécurité de l'information (« Global State of Information Security Survey ») que la plupart des menaces proviennent de sources internes à l'entreprise, en particulier des collaborateurs actuels ou anciens. La même tendance est observée en France et dans le monde.

**Qui est le cybercriminel ?** (hors menaces extérieures)




En revanche, la France est à rebours de ce qui est observé en Europe de l'Ouest et dans le monde pour ce qui concerne la perception de l'origine des cyber-attaques futures. Alors que près de la moitié des entreprises sondées pensent que les attaques viendront de l'interne, 61 % des entreprises françaises pensent que ces attaques viendront de l'extérieur.

Il ressort aussi de cette même étude que, dans les faits, malgré les risques considérables encourus par les entreprises, ces dernières ne protègent pas assez leurs informations sensibles et ne savent pas prioriser le degré d'importance de la masse de données gérées.

En effet, depuis l'explosion de la quantité des données et de la multiplicité des supports sur lesquels elles sont stockées, il est de plus en plus difficile pour les entreprises d'avoir des dispositifs de sécurité de l'information efficaces et robustes, notamment pour les données ayant trait à la propriété intellectuelle ou industrielle.

Enfin, la mobilité des employés et les nouveaux moyens de communication utilisés accroissent encore le risque de déperdition de données ou d'attaques de données sensibles. En effet, les smartphones, les tablettes et plus généralement l'utilisation de terminaux mobiles personnels par les employés a augmenté la quantité de données à protéger ainsi que le nombre de supports à sécuriser.

Il s'agit d'un défi majeur pour les entreprises à l'avenir qui doivent d'ores et déjà mettre en place ou renforcer leurs politiques de sécurité dans ce domaine. Pourtant, les résultats de notre étude sur la sécurité de l'information n'indiquent pas d'amélioration en ce sens et, au contraire, montrent une certaine dégradation, notamment en France.

Ces deux facteurs, augmentation des données et des supports à protéger ainsi que mobilité des données, ont considérablement fait évoluer les risques et les enjeux en matière de cyber-sécurité pour les entreprises.

Enfin, il ne faut pas oublier que le rapport gain espéré par rapport aux risques encourus est très élevé pour les cyber-fraudeurs en raison d'une part, de la difficulté à détecter ces attaques et leurs auteurs, et d'autre part, du fait d'un cadre juridique et réglementaire international inadapté à des poursuites efficaces.

# La corruption : une préoccupation croissante pour les entreprises

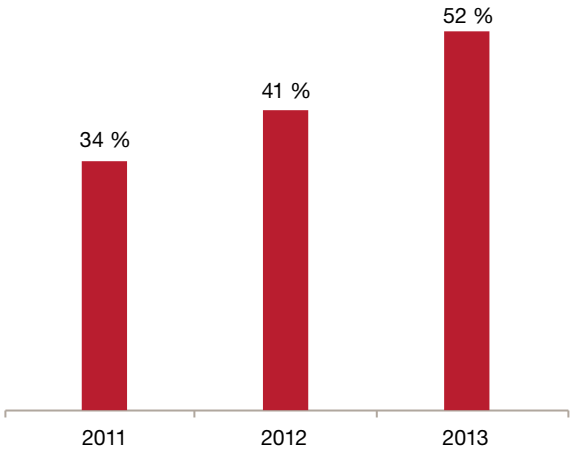
La corruption n'est pas, comme nous l'avons vu, la typologie de fraude la plus reportée par les entreprises mais il s'agit sûrement d'une réelle menace en termes de coût notamment en raison des lois très contraignantes en vigueur sur ce sujet telles que le « Foreign Corrupt Pratices Act - FCPA » américain ou le « Bribery Act » britannique (UKBA).

Il est important de souligner que tous les processus des entreprises sont exposés à ce risque : ventes, marketing, distribution, implantation internationale, fiscalité, …

Au niveau mondial, 27 % des fraudes reportées en 2014 concernent des actes de corruption soit une augmentation de trois points par rapport à notre précédente étude. En France et en Europe de l'Ouest, la tendance est moindre avec respectivement 8 % et 12 % d'actes de corruption déclarés.

En outre, l'étude mondiale 2014 de PwC menée auprès de 1 344 chefs d'entreprise (« Global CEO Survey ») révèle que la corruption est un enjeu croissant pour ces derniers. Leur taux de préoccupation sur ce sujet a crû de près de 20 points entre 2011 et 2013. En 2013, 52 % des chefs d'entreprises interrogés se disaient préoccupés par cette menace.

**Une préocupation croissante pour les chefs d'entreprise dans le monde**

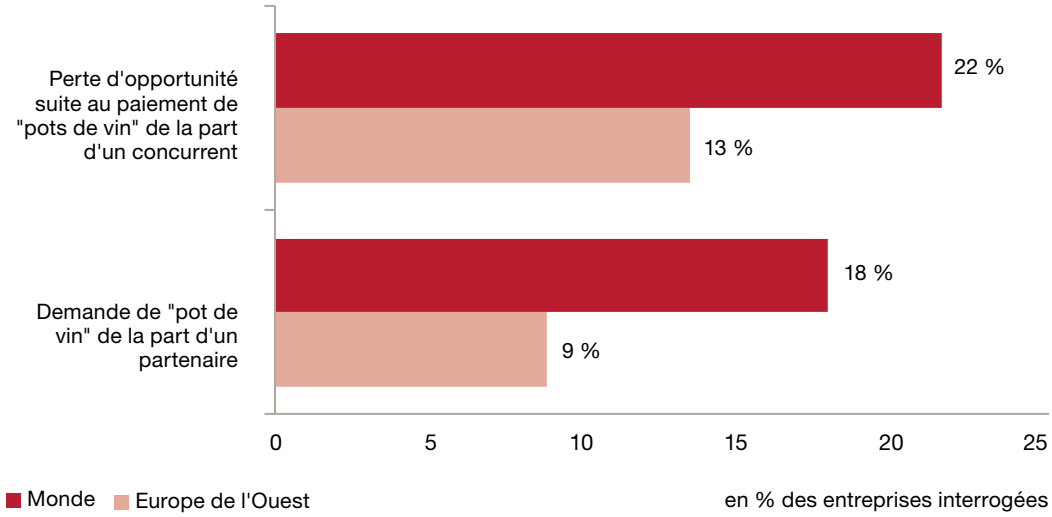



D'ailleurs, la corruption est une menace sérieusement prise en compte par les entreprises puisque deux entreprises sur cinq en France, en Europe de l'Ouest et dans le monde disent avoir remis en question leur stratégie d'implantation dans les pays à fort risque de corruption.

*12 % des entreprises dans le monde déclarent que le coût de la corruption pour leur organisation est supérieur à 5 millions de dollars*

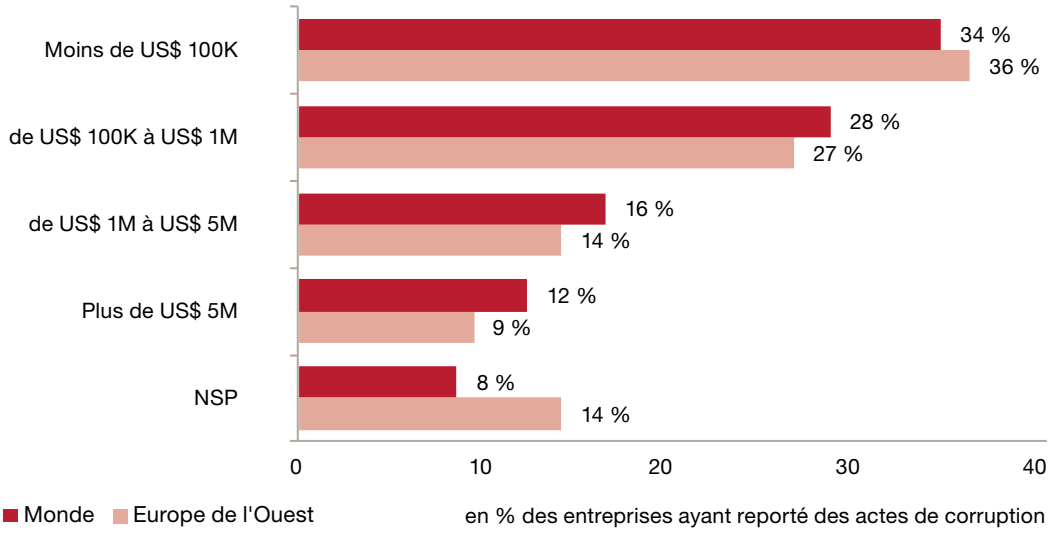
En termes d'incidence sur la conduite des affaires, 18 % des entreprises dans le monde et 9 % des entreprises en Europe de l'Ouest déclarent avoir été sollicitées pour le paiement d'un « dessous-de-table ». De plus, 22 % des entreprises dans le monde et 13 % des entreprises en Europe de l'Ouest disent avoir perdu une opportunité d'affaires en raison des mauvaises pratiques de leurs concurrents.

**Incidences de la corruption sur les affaires**

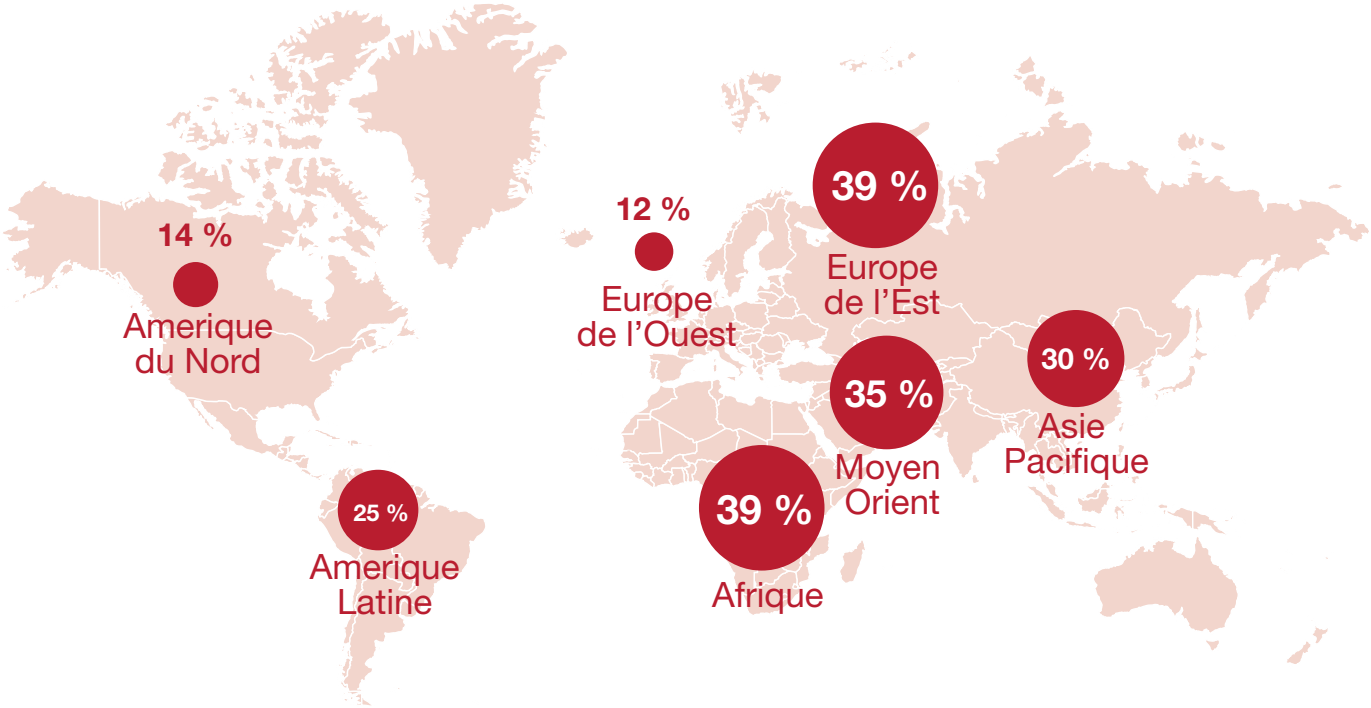



Le coût de la corruption est également considérable pour les entreprises, entre autres, en raison des fortes amendes infligées par les états ayant mis en place des régulations contraignantes. En effet, comme illustré dans le graphique ci-contre, 12 % des entreprises dans le monde déclarent que le coût de la corruption pour leur organisation dépasse les cinq millions de dollars !

## Le coût de la corruption

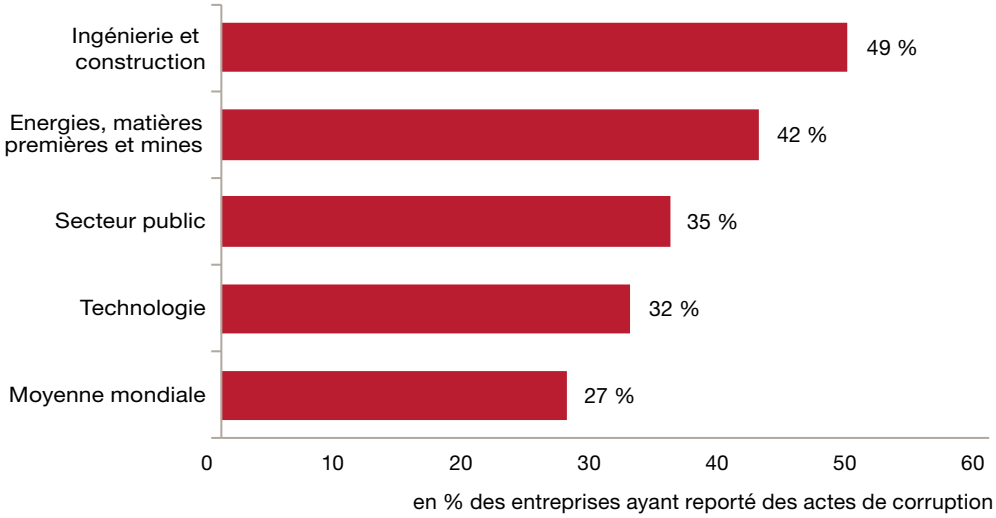



En termes de zones géographiques impactées par la corruption, ce sont l'Afrique, l'Europe de l'Est et le Moyen-Orient qui sont les zones les plus touchées.



Pour expliquer ce constat, nous pouvons mettre en avant les mêmes raisons que pour la fraude aux achats, à savoir l'importance des secteurs de la construction et de l'énergie, voire du secteur public.

### La corruption par secteur d'activité




Pour ce qui concerne les perspectives, les risques de corruption restent significatifs pour toutes les zones géographiques avec un taux de corruption anticipé de 29 % dans le monde, soit deux points de plus que le taux constaté dans le cadre de la présente étude.

Pour les entreprises françaises, le défi majeur à relever sera celui de l'international, que ce soit lors d'opérations d'acquisition ou simplement dans le cadre de la poursuite de leurs activités. Ce défi ne pourra être relevé que par la mise en place de procédures efficaces et d'une sélection précise des partenaires et des projets sur lesquels les entreprises françaises désireront s'engager.

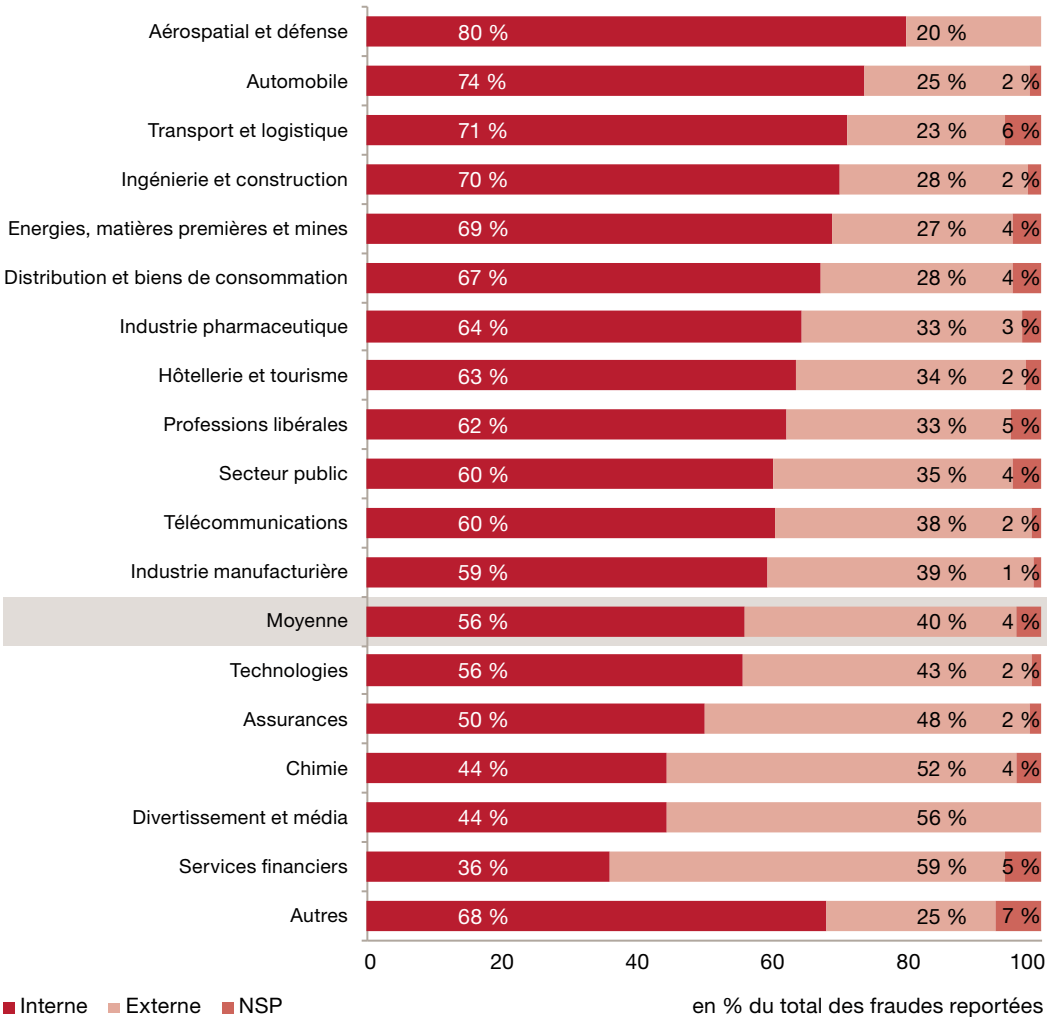
# *Le fraudeur : apprenez à le reconnaître !*

La lutte contre la fraude nécessite pour les entreprises de connaître d'où viennent les menaces afin de mieux cibler les actions correctrices à apporter à leur environnement de contrôle en général et à leur dispositif anti-fraude en particulier.

Les entreprises ayant déclaré au moins une fraude dans le cadre de notre étude sont plus touchées par la fraude interne (56 %) que par la fraude externe (40 %). Cette répartition est en ligne avec les statistiques de notre précédente étude qui faisait ressortir exactement la même répartition.

Comme lors de nos précédentes études, le niveau élevé de fraudes externes s'explique, pour partie, par la forte représentation du secteur des services financiers au sein de la population d'entreprises ayant déclaré au moins une fraude dans le cadre de cette étude. En effet, de par la nature même de ses activités, ce secteur fait état d'un niveau de fraudes externes particulièrement élevé (59 %).

**Répartition des fraudes par type de fraudeur (interne/externe)**



## *En France, le fraudeur est une personne plus établie dans l'entreprise*

Il est également intéressant de constater que plus de 55 % des fraudes reportées par les entreprises françaises sont du fait de fraudeurs externes contre 39 % de fraudeurs internes !

Cette tendance est inverse à celle observée au niveau mondial où, comme nous l'avons déjà vu, 56 % des fraudeurs sont internes à l'entreprise et 40 % sont externes. Au niveau européen, la répartition entre fraude interne et externe est quasiment identique : 48 % des fraudeurs sont internes et 49 % sont externes.

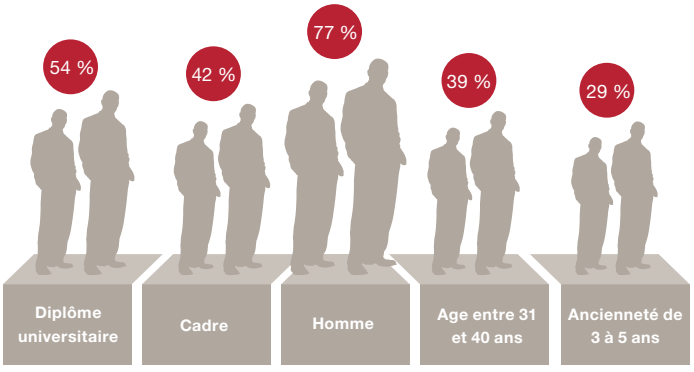
Cette situation s'explique, en grande partie, par le nombre élevé de « fraudes au Président » dont ont été victimes les sociétés françaises ce qui, in fine, a une incidence de dix points sur le calcul du pourcentage de fraudes externes.

La fraude interne reste néanmoins la typologie de fraude prépondérante pour plus de 70 % des secteurs d'activité.

Le profil du fraudeur interne au niveau mondial a peu évolué depuis notre dernière étude : il s'agit toujours d'un homme, cadre, trentenaire, diplômé et disposant de trois à cinq années d'ancienneté au sein de l'entreprise.

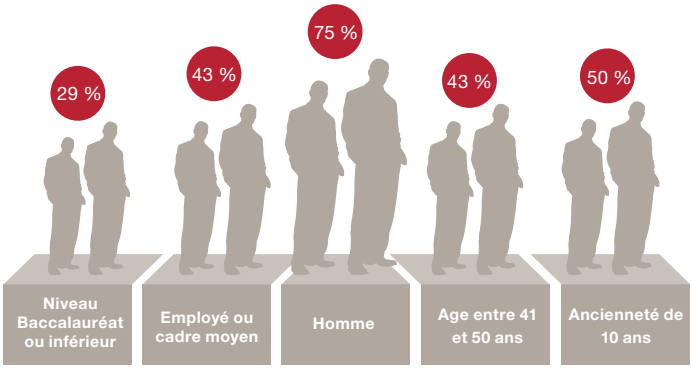
En France, le fraudeur est une personne plus établie dans l'entreprise ce qui paraît plus logique puisqu'il connaît mieux les systèmes et, dans ce cas, est plus à même de les contourner. Il a plutôt la quarantaine, dispose de plus de dix années d'ancienneté et, dans la majorité des cas, est un employé ou cadre moyen.

### Portrait robot du fraudeur dans le monde




en % des fraudes reportées

### Portrait robot du fraudeur en France




en % des fraudes reportées

Par ailleurs, il convient de souligner un point important qui ne découle pas directement de notre étude mais de notre expérience sur le terrain : le fraudeur est en général une personne appréciée par ses collègues et qui est perçue comme performante dans son travail par ses supérieurs. Ces deux points ajoutés au portrait-robot précédemment défini rendent le fraudeur très difficile à identifier.

# Que risque le fraudeur ?

Lorsqu'une fraude est détectée, l'entreprise doit immédiatement prendre des mesures pour sanctionner les coupables des actes frauduleux commis.

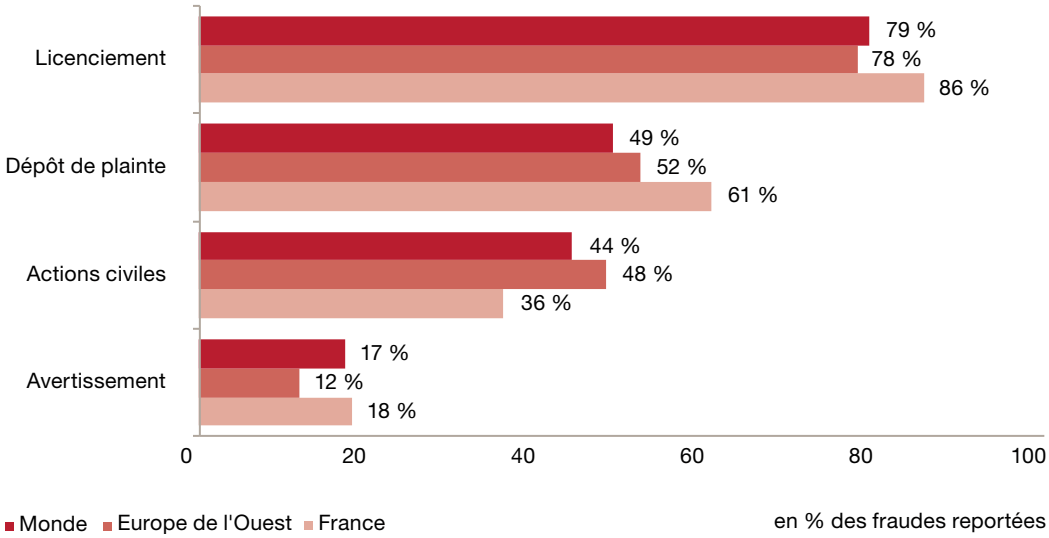
Notre étude 2014 confirme que les entreprises apportent des réponses fermes envers les fraudeurs internes avec près de 80 % des entreprises ayant répondu à notre enquête qui déclarent avoir licencié les fraudeurs identifiés. La France semble être encore moins tolérante avec plus de 86 % des fraudeurs identifiés licenciés.

Le licenciement du ou des fraudeurs s'accompagne généralement d'un dépôt de plainte ou d'une action civile afin de tenter de récupérer les sommes potentiellement détournées.

Dans peu de cas, les entreprises se contentent de donner uniquement un avertissement au fraudeur interne.

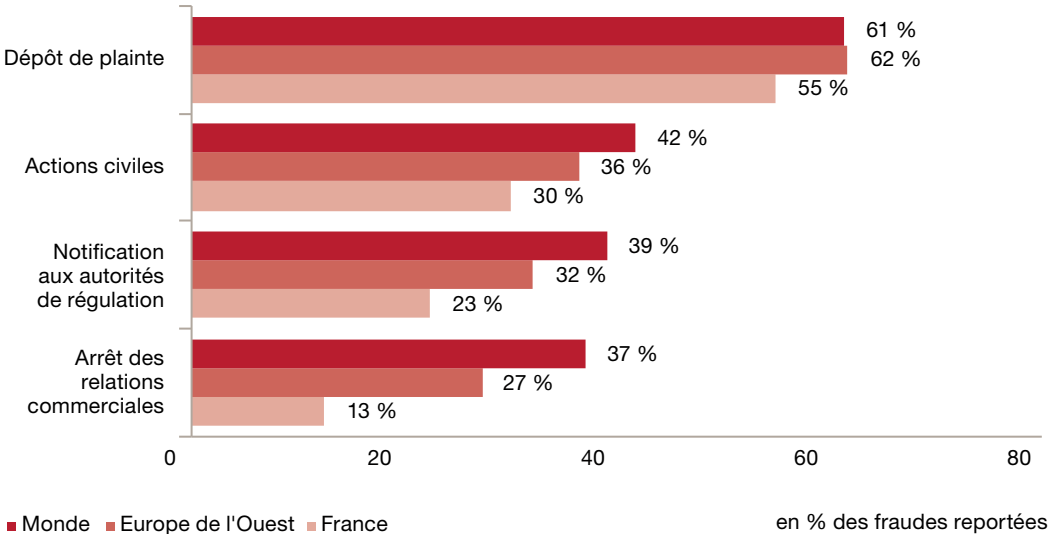
Cette situation nous semble concourir à l'optimisation de la gestion du risque de fraude au sein des entreprises. En effet, dès lors qu'un fraudeur se sait être « surveillé » par le biais d'un dispositif d'analyse des transactions inhabituelles, par exemple, et fermement sanctionné s'il venait à être découvert, cela se révèle dissuasif et conduit irrémédiablement à réduire le risque de fraude au sein de l'entreprise.

**Sanctions prises à l'égard des fraudeurs internes**



Pour ce qui concerne les fraudeurs externes, les entreprises, lorsqu'elles ont pu les identifier, prennent également le même type de décision que pour la fraude interne, à savoir le dépôt d'une plainte associée, le cas échéant, à une action civile.

## Sanctions prises à l'égard des fraudeurs externes




*Pour 20 % des cas de fraudes reportés, l'incidence financière est supérieure à un million de dollars*

# Quels sont les dommages causés par la fraude ?

La détermination de l'incidence financière d'une fraude pour une entreprise est toujours difficile à prévoir avant la survenance de cette dernière, mais elle est aussi délicate à estimer avec précision, une fois la fraude survenue.

Cependant, les enseignements de nos dernières études sont clairs. Le coût de la fraude, en termes financiers et non financiers, peut être extrêmement significatif pour l'entreprise.

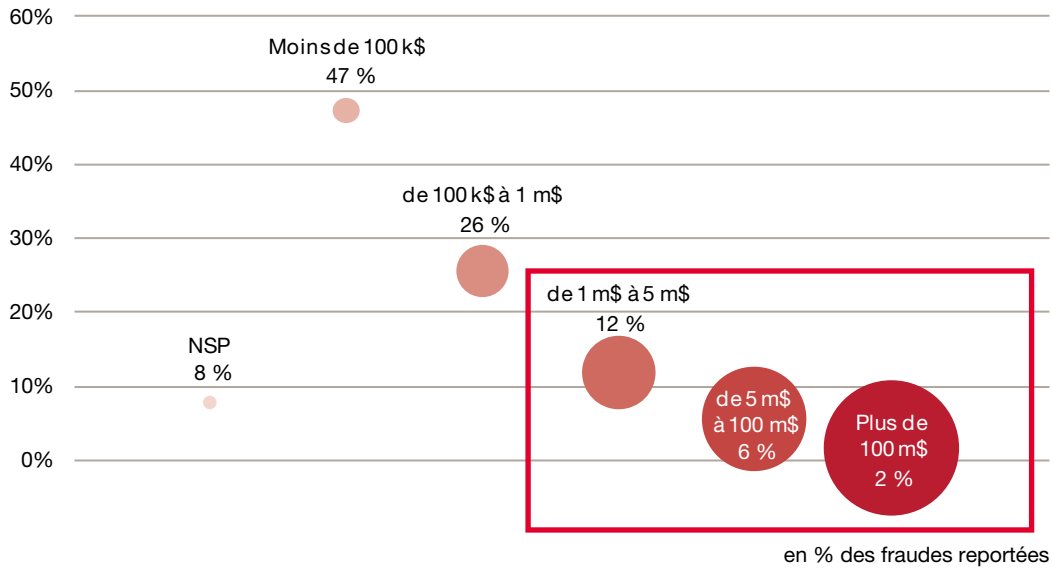
En effet, en plus du montant de la fraude à proprement parler, il faut prendre en compte le coût généré par la gestion de cette fraude, les éventuelles amendes des autorités de régulation et les dommages collatéraux potentiels en termes d'image ou d'environnement de travail pouvant aussi, parfois, se traduire par des pertes de revenus.

En termes strictement financiers, il ressort de notre étude que pour près d'une entreprise sur deux dans le monde, le montant cumulé des fraudes subies au cours des 24 derniers mois a une incidence supérieure à 100 000 dollars sachant que dans 20 % des cas reportés ce coût est supérieur à un million de dollars. Ce pourcentage est deux fois moins élevé pour ce qui concerne les entreprises françaises (10 %).

Pire encore, pour 2 % des entreprises ayant répondu à notre étude, l'incidence financière dépasse les cent millions de dollars. Ces fraudes de grande ampleur sont à mettre en parallèle avec l'augmentation du nombre de cas de corruption reportés et les importants coûts associés à ce type de fraude (amendes des autorités de régulation, frais de conseils juridiques et financiers, etc.).

Le graphique ci-dessous présente l'incidence financière des fraudes reportées par les entreprises au cours de la période de notre étude.

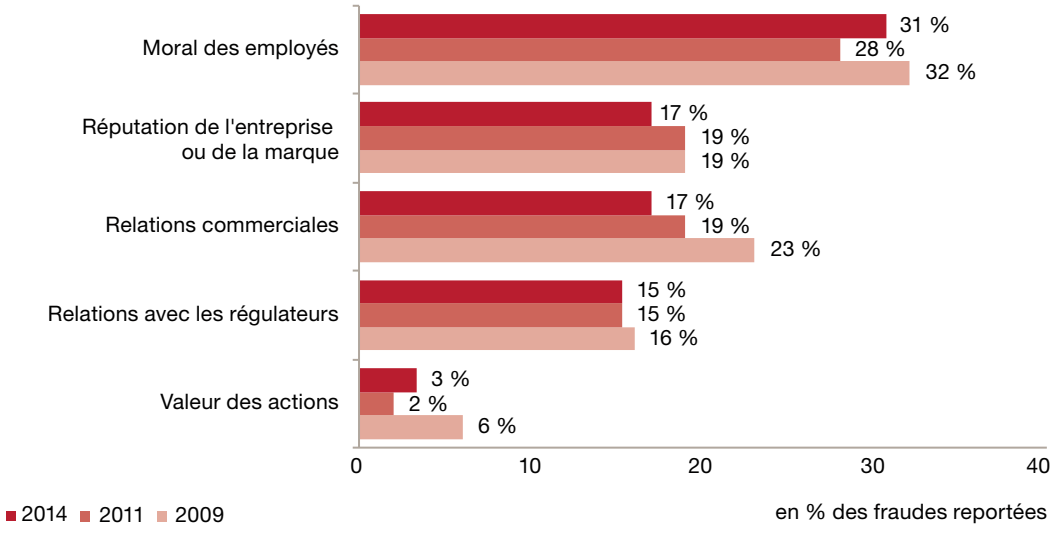
## Incidences financières de la fraude en entreprise




Il convient de rappeler qu'en plus des dommages strictement financiers, la fraude peut également avoir des incidences non financières considérables pour les entreprises qui en sont victimes : atteinte à la réputation de l'entreprise, baisse du moral des employés, dégradation de l'environnement de travail, incidence sur le cours de bourse…

En effet, pour près d'un tiers des entreprises interrogées, la baisse du moral des employés constitue le dommage collatéral majeur (31 %), suivi, à égalité, de l'atteinte à la réputation de l'entreprise (17 %) et de la dégradation des relations commerciales avec les partenaires (17 %).

## Dommages collatéraux de la fraude en entreprise

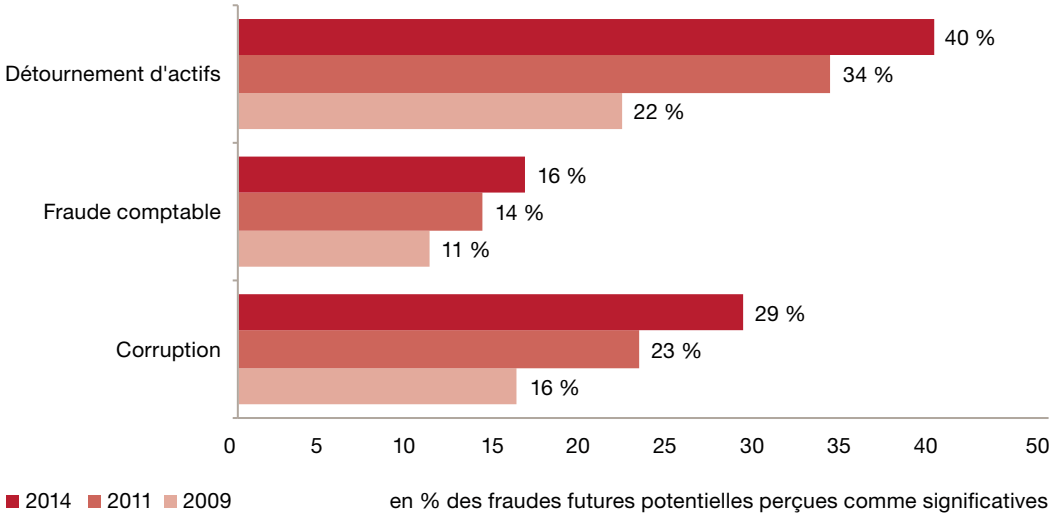


# *Une évolution dans la perception des risques futurs*

Dans le cadre de notre étude, nous avons interrogé les entreprises sur les fraudes effectivement subies mais également sur leur perception des risques de fraudes dans le futur.

Pour chacune des grandes typologies historiques de fraudes, le taux de réponses obtenues est systématiquement supérieur à celui de notre étude précédente comme le démontre le graphique ci-après.

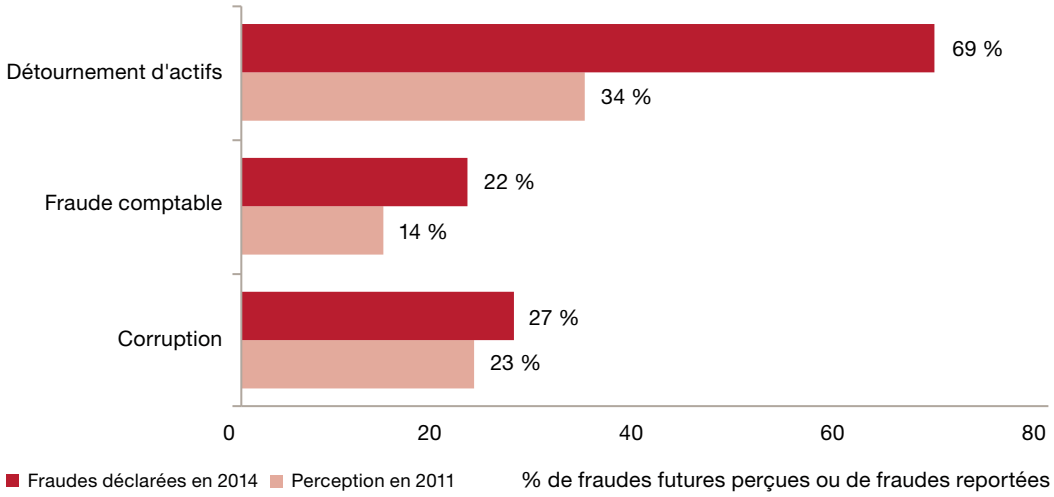
**Perception de l'évolution du risque de fraude**




Cependant, bien qu'il soit incontestable que d'étude en étude, les entreprises ont fortement progressé dans leur perception de l'évolution du risque de fraude, il n'en demeure pas moins que cette perception est toujours sous-estimée au regard de la réalité observée.

Le graphique ci-dessous illustre ce manque d'anticipation, inhérent notamment à l'imprévisibilité de la survenance d'une fraude.

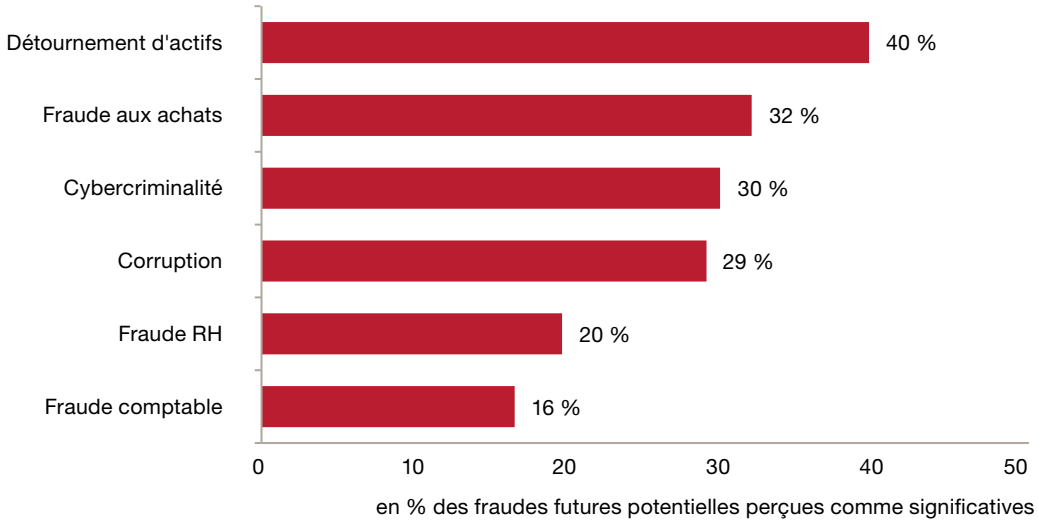
**Perception de l'évolution du risque de fraude en 2011 comparée au niveau de fraudes reportées en 2014 dans le monde**




Il ressort de notre étude 2014 que la préoccupation principale des entreprises interrogées dans le futur concerne le détournement d'actifs, suivi de la fraude aux achats.

En outre, 30 % des entreprises interrogées estiment qu'elles seront victimes d'un acte de cybercriminalité dans les 24 prochains mois, soit une augmentation de six points par rapport à notre précédente étude.

**Perception de l'évolution du risque de fraude dans le monde**

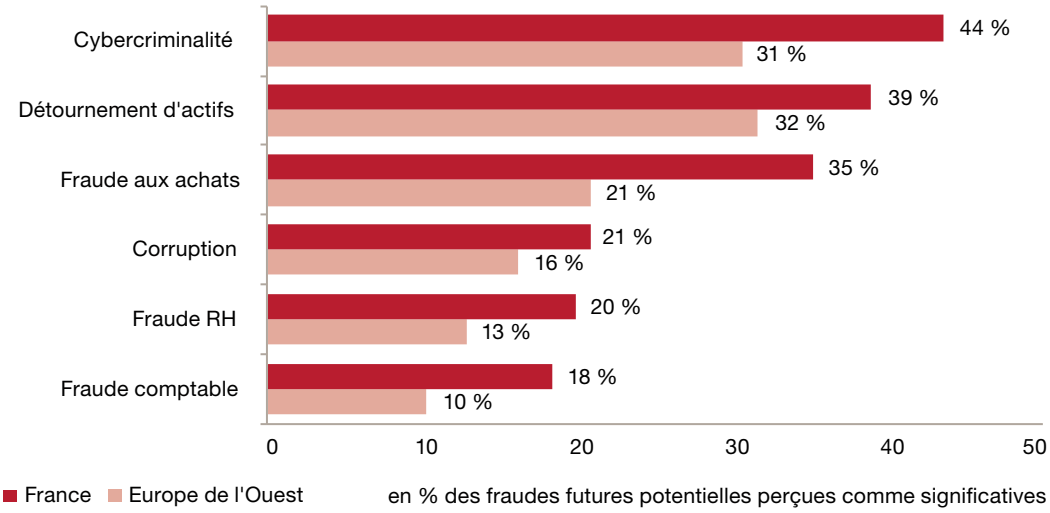



Cette tendance est particulièrement marquée au niveau français où 44 % des entreprises sondées estiment qu'elles subiront d'un acte de cybercriminalité dans les 24 mois à venir.

Par ailleurs, il est intéressant de constater que les entreprises françaises semblent être réellement conscientes du risque de fraude. En effet, pour chacune des typologies, leur perception est supérieure ou égale à la moyenne européenne ou mondiale, exceptée pour la corruption.

Il n'en demeure pas moins que pour ce qui concerne le détournement d'actifs, il est fort à craindre que le pourcentage de 39 % soit sous-évalué au regard du niveau actuel de ce type de fraude (61 %).

**Perception de l'évolution du risque de fraude en France et en Europe de l'Ouest**




*44 % des entreprises françaises sondées craignent d'être victimes d'un acte de cybercriminalité dans les 24 prochains mois*

# *Annexes*

# Description de la population ayant répondu à notre enquête

Notre septième étude mondiale sur la fraude en entreprise a été menée dans 95 pays à travers le monde. 5 128 réponses ont été récoltées sur la base d'un questionnaire complété sur un site internet dédié au cours des mois de septembre et octobre 2013. Nous avons demandé aux personnes ayant répondu à cette étude si elles avaient été victimes d'une fraude au cours des 24 derniers mois et si oui de nous décrire les circonstances et caractéristiques attachées à cette fraude.

| Zone/Pays en nombre de participants | 2014 |
|---|---|
| **Asie & Pacifique** | **1 162** |
| Australie | 79 |
| Chine (hors Hong Kong) | 85 |
| Hong Kong (et Macao) | 116 |
| Inde | 115 |
| Indonésie | 4 |
| Japon | 75 |
| Malaisie | 110 |
| Nouvelle Guinée | 81 |
| Nouvelle-Zélande | 82 |
| Singapour | 82 |
| Thaïlande | 76 |
| Vietnam | 1 |
| **Afrique** | **612** |
| Afrique du Sud | 134 |
| Algérie | 2 |
| Angola | 22 |
| Botswana | 5 |
| Cameroun | 6 |
| Congo | 1 |
| Côte d'Ivoire | 3 |
| Ghana | 3 |
| Guinée | 2 |
| Kenya | 124 |
| Lesotho | 1 |
| Malawi | 1 |
| Maroc | 17 |
| Mozambique | 4 |
| Namibie | 26 |
| Nigéria | 82 |
| Sierra Leone | 1 |
| Swaziland | 4 |
| Tanzanie | 12 |
| Tunisie | 17 |

| Zone/Pays en nombre de participants | 2014 |
|---|---|
| Ouganda | 12 |
| Zambie | 83 |
| Zimbabwe | 42 |
| **Amérique du Sud et Centrale** | **711** |
| Argentine | 82 |
| Bahamas | 2 |
| Barbade | 1 |
| Brésil | 132 |
| Chili | 75 |
| Colombie | 1 |
| Cuba | 2 |
| Équateur | 22 |
| Mexique | 211 |
| Pérou | 82 |
| République Dominicaine | 1 |
| Vénézuela | 100 |
| **Amérique du Nord** | **215** |
| Canada | 100 |
| États-Unis | 115 |
| **Europe de l'Ouest** | **1 555** |
| Allemagne | 10 |
| Autriche | 6 |
| Belgique | 68 |
| Chypre | 88 |
| Danemark | 118 |
| Espagne | 79 |
| Finlande | 34 |
| France | 131 |
| Grèce | 11 |
| Hollande | 75 |
| Irlande | 78 |
| Israël | 31 |
| Italie | 101 |
| Luxembourg | 12 |

| Zone/Pays en nombre de participants | 2014 |
|---|---|
| Norvège | 92 |
| Portugal | 75 |
| Royaume-Uni | 372 |
| Suède | 91 |
| Suisse | 83 |
| **Europe Centrale et de l'Est** | **877** |
| Bulgarie | 79 |
| Hongrie | 91 |
| Kazakhstan | 1 |
| Lituanie | 1 |
| Pologne | 94 |
| République Tchèque | 94 |
| Roumanie | 77 |
| Russie | 111 |
| Serbie | 52 |
| Slovaquie | 76 |
| Slovénie | 33 |
| Turquie | 78 |
| Ukraine | 90 |
| **Moyen-Orient** | **232** |
| Arabie Saoudite | 74 |
| Bahrein | 2 |
| Égypte | 7 |
| Émirats Arabes Unis | 117 |
| Jordanie | 9 |
| Liban | 8 |
| Oman | 1 |
| Qatar | 12 |
| Soudan | 1 |
| Syrie | 1 |
| **Pas de pays spécifié** | **28** |
| **TOTAL** | **5 128** |

| Secteur des entreprises participantes | 2014 |
|---|---|
| Services financiers | 19 % |
| Industrie manufacturière | 9 % |
| Énergies, matières premières et mines | 8 % |
| Distribution et biens de consommation | 8 % |
| Assurances | 7 % |
| Professions libérales | 6 % |
| Ingénierie et construction | 6 % |
| Secteur public | 5 % |
| Transport et logistique | 5 % |
| Industrie pharmaceutique | 5 % |
| Technologies | 5 % |
| Automobile | 4 % |
| Télécommunications | 3 % |
| Divertissement et média | 2 % |
| Hôtellerie et tourisme | 2 % |
| Chimie | 2 % |
| Aérospatial et défense | 1 % |
| Autres secteurs | 5 % |

| Types d'entreprises participantes | 2014 |
|---|---|
| Secteur privé | 50 % |
| Cotées en bourse | 35 % |
| Gouvernement et secteur public | 9 % |
| Autres | 6 % |

| Taille des entreprises participantes | 2014 |
|---|---|
| Moins de 100 employés | 8 % |
| De 101 à 1 000 employés | 20 % |
| De 1 001 à 10 000 employés | 32 % |
| Plus de 10 000 employés | 39 % |
| Ne sait pas | 2 % |

| Fonction occupée par les participants à notre enquête | 2014 |
|---|---|
| Direction financière | 28 % |
| Direction générale | 18 % |
| Audit interne | 14 % |
| Gestion des risques | 6 % |
| Conformité et contrôle | 6 % |
| Département sécurité | 3 % |
| Département juridique | 4 % |
| Systèmes d'information | 3 % |
| Conseiller/consultant | 4 % |
| Opérations et production | 2 % |
| Marketing et ventes | 3 % |
| Ressources humaines | 1 % |
| Fiscalité | 1 % |
| Service clients | 1 % |
| Recherche et développement | 1 % |
| Achats | 1 % |
| Autres | 6 % |

# Quelques définitions

***Fraude :***
acte intentionnel réalisé par un salarié (fraude interne) ou un tiers (fraude externe) de manière à retirer un avantage généralement financier selon un procédé illicite.

***Détournement d'actifs :***
transfert illégal d'un bien du patrimoine de l'entreprise à celui d'un salarié, d'un tiers ou d'une autre entreprise.

***Fraude comptable :***
manipulation intentionnelle des comptes dans le but d'en donner une image plus flatteuse sans nécessairement procurer au fraudeur un gain financier personnel.

***Corruption :***
acte d'offrir, donner, recevoir ou solliciter quelque chose de valeur pour influencer une décision ou obtenir un avantage généralement financier.

***Cybercriminalité :***
fraude commise en utilisant des systèmes informatiques connectés à un réseau et notamment Internet. Parmi les cas classiques de cybercriminalité, on peut citer le vol d'informations personnelles telles que les coordonnées bancaires.

***Fraude aux achats :***
fraude consistant à biaiser le choix d'un fournisseur dans le cadre, entre autres, d'une procédure d'appel d'offres, ce qui, in fine, conduit généralement à une surfacturation des prestations rendues.

***Fraude RH :***
fraude impactant les cycles « ressources humaines » ou « paie » incluant par exemple la création d'un salarié fictif, le paiement d'heures non justifiées, l'embauche d'un proche ou d'une personne n'ayant pas les qualifications requises.

**Autres sources :**

- PwC - 2014 Global CEO Survey [http://www.pwc.fr/17th-annual-global-ceo-survey1.html]
- PwC - 2014 Global State of Information Security Survey [http://www.pwc.fr/global-state-of-information-security-survey-2013.html]

# Contacts

## Forensic Services


***Dominique Perrier***
Associée
+33(0)1 56 57 80 17
dominique.perrier@fr.pwc.com

***Jean-Louis Di Giovanni***
Associé
+33(0)1 56 57 12 57
jean-louis.di.giovanni@fr.pwc.com


**Forensic Services**, une offre de services complète de PwC

Le département « Forensic » de PwC France, créé en 1999, fait partie d'un réseau mondial comprenant 2 200 experts dont 500 experts en sécurité informatique.
Les interventions de nos experts consistent à évaluer les impacts financiers de situations de crise et à accompagner nos clients pour mettre en œuvre des solutions leur permettant de limiter leurs risques.


Les informations contenues dans cette publication ne peuvent en aucun cas être assimilées à des prestations de services ou de conseil rendues par leurs auteurs ou éditeurs. Aussi, elles ne peuvent être utilisées comme un substitut à une consultation rendue par une personne professionnellement compétente. Cette publication est la propriété de PricewaterhouseCoopers Advisory. Toute reproduction et /ou diffusion, en tout ou partie, par quelque moyen que ce soit est interdite sans autorisation préalable.
© 2014 PricewaterhouseCoopers Advisory. Tous droits réservés.

www.pwc.com/crimesurvey

# Economic Crime:

## A Threat to Business Globally

*Hungarian country report*
*February 2014*

pwc

www.pwc.com/hu/crimesurvey

# Contents

*Global Economic Crime Survey 2014 was carried out by PricewaterhouseCoopers. It is the largest survey of its kind with over 5,000 survey participants from over 100 countries.*

*The survey is intended not only to describe the current state of economic crime but also to identify trends and perception of future risks.*



# *Preface*

We are pleased to present to you the Hungarian results of the 2014 PwC Global Economic Crime Survey.

This is the seventh time we have prepared the global survey and the sixth time we have published a Hungarian country edition. This survey describes the current state of economic crime and also identifies trends and perception of future risks. To provide a more comprehensive overview of these topics, we also included global and regional data.

With over 5,000 responses from senior executives from around the world, including 91 Hungarian companies, this is the most comprehensive global survey of economic crime available to businesses.

Economic crime is constantly evolving and seeking new ways to thrive. Companies need to find new and more efficient ways to defend their assets or else they will be outpaced by the evolution of fraud.

Our survey supports this observation: economic crime is common in Hungary and is taking more diverse forms.

Procurement fraud and cybercrime have gradually emerged as standalone major categories of fraud. We strongly advise companies to adjust their risk assessments accordingly.

The results have also shown that the costs of economic crime and asset misappropriation are rising, and bribery and corruption remain the two most widely experienced types of economic crime in Hungary.

We invite all entrepreneurs and managers to read through the report and to draw conclusions relevant to their undertaking. A global report and local variants for different countries are available to help organisations do business globally.

Last but not least, we would like to thank the survey participants who were kind enough to share their observations of fraud and provide their insights. We are especially thankful to 91 respondents from Hungary. All respondents share our belief: economic crime is too costly to ignore.

***Miklós Fekete,***
Partner,
PwC Hungary

***George Surguladze,***
Senior Manager,
PwC Hungary

# Main Findings

## The Dangers of Crime

### *Crime around us*

Economic crime continues to be a serious issue affecting organizations in Hungary, and no industry is immune.
Our survey indicates that approximately 1 in 4 Hungarian organisations (26%) reported having experienced one or more instances of economic crime in the last two years.

In our experience, many cases remain undetected, and it would be extremely difficult for organisations to uncover all instances of fraud, especially if the organization does not make available anonymous ways to report economic crime and/or does not perform fraud risk assessments regularly.
Fifty-eight percent of respondents reporting fraud estimated the total financial loss of their company due to economic crime as being between USD 100,000 and USD 5 million.

### *Crime evolves*

Traditionally, asset misappropriation is the most frequently observed type of crime (63% of companies). However, fraudsters are seeking out new avenues for defrauding victim companies. The distribution of various types of economic crime is becoming more diverse, companies are seeing an increase in the share of other types of crimes: cybercrime (17% of companies), procurement fraud (25%), money laundering (25%), bribery and corruption (38%).

## Cybercrime

### *Occurrence*

Companies are more likely to suffer from cybercrime now than at any time in the past. In the previous survey, there were approximately 12 companies reporting asset misappropriation (the most common economic crime) for each company reporting cybercrime. This year the ratio is four to one.

### *Risks of cybercrime*

Business operations are relying more and more on network applications. This increases the potential impact of cybercrime.

### *High latency*

Moreover, cybercrime is dangerous as the victims may not be aware it is happening. The latency (share of undetected occurrences) of, for example, IP theft must clearly be many times higher than the latency of cash theft.

Therefore, the real occurrence is most probably significantly higher than reported.

## Procurement fraud

### *Occurrence*

Procurement fraud emerged as a standalone category of fraud, having been reported by 25% of respondents. The top reported risk factor is the process of inviting and selecting vendors.

### *Risks of procurement fraud*

Procurement fraud usually includes collusion between parties. Therefore, the detection of this type of fraud is often difficult. However, there are ways to mitigate the risks.

## Corruption and bribery

### *Risks of corruption*

Corruption is seen as the greatest risk in doing business globally, both in terms of reputation loss and monetary loss. This finding is also in line with PwC 's Global CEO Survey, according to which corruption and bribery is the highest scoring threat to business growth.

# What Hungarian companies do and do not do

### *Remedial actions*

The picture is somewhat ambiguous with respect to measures taken against fraudsters. In the case of internal perpetrators, quite often, the law enforcement authorities are notified (70%); civil action is also often taken (60%) – these results exceed both CEE and global averages. But at the same time, internal perpetrators were dismissed in only half of the cases (50%) reported in Hungary which is below regional (78%) and global averages (79%).

When fraud by an external subject is discovered, the law enforcement authorities are notified only in the half of the cases (50%); civil action is also sought (57%). But business relations are discontinued in only approximately a third of all instances.

### *Prevention and detection*

There does not seem to be a clear pattern in terms of how fraud is detected in Hungary. Methods such as data analytics and suspicious transaction reporting do not play a dominant role in fraud detection.

It is also evident that there is room for improvement in terms of crime detection methods.
Hungarian companies should definitely start thinking of increasing the efficiency of detection methods based on computer analysis.

Tens of thousands or more of records, hundreds of disconnected worksheets, many different systems... Where should a company begin? All the information one could possibly want is available, but how to analyse it?

Although companies store and analyse more data than ever before, it is often difficult to gain insights within the data using traditional analytical methods. While spreadsheets are easy to prepare and understand, the ability to draw conclusions from the data diminishes as the volume and complexity of data grows.

Visualisation, or visual analytics, is the concept of using pictures, charts, diagrams and maps to reveal key relationships, communications, trends and patterns within large amounts of data.
Many companies are now using the power of visualisation to detect fraud and abuse; from detecting fictitious employees and conflicts of interest, to detecting inappropriate travel expense expenditure.



# Digital footprints

***We asked Pavel Jankech, Senior Manager in Forensic Technology Services, for his thoughts on prevention and detection techniques***

***- Do you think that the measures that companies use against fraud are sufficient?***

Currently, companies use primarily preventative measures to combat fraud. This, however, increases the risk of fraud remaining undetected for longer. The impact of such fraud can be really serious, and it's not just a pure financial loss. Also at risk is reputation, employee morale, or business relationships with suppliers.

***- What would you recommend to companies?***

Robust control environment is an absolute necessity. Nevertheless, it is never 100% bullet proof, so we recommend that companies also implement detection mechanisms, such as regular data analytical tests or implementation of a continuous fraud detection system. Using detection measures will help identify fraud earlier and thus reduce losses.

***- What data test do you have in mind?***

Traditional methods seek to identify suspicious transactions (red-flags) through rules-based testing. Classic examples include round-sum invoices and late-night postings. The challenge is that red-flags are typically not unusual events, and therefore the outputs from the tests are long lists of exceptions with many false-positives, leading to a high cost of manual investigation. Moreover, these rules are already well known, so the fraudster can easily avoid them.

***- How can a company avoid those limitations?***

In our experience, each of the different types of fraud leaves a "footprint" in the data. Using advanced analytical techniques and visualization can identify different patterns of behavior that correspond to these tracks.
This approach can be used proactively to identify potential weak areas of control in the company, or reactively in the investigation of a specific incident.

***- What kind of advanced analytical techniques are available?***

These are advanced statistical methods or data mining techniques. These can help identify hidden patterns in the data behavior. Each of the patterns indicates the behavior of the supplier or user, and is compared with standard behavior in the dataset. Unusual or anomalous patterns indicating fraud are subsequently investigated. Using a combination of techniques for the visualization of data and detailed knowledge of the company, the investigation should focus just on unusual or anomalous behavior. The results of detailed investigations shall apply retroactively to increase the accuracy of the search algorithm.

***- What data is required for this type of testing?***

During the initial phase of the project we would seek to understand specifics of the company and its business and its existing control environment to identify key risk areas for fraud.
Based on those we would define where to start looking for fraud. The main sources are typically data from ERP and accounting systems, or actual cash flows gathered directly from bank statements.

# *Economic Crime in Hungary*

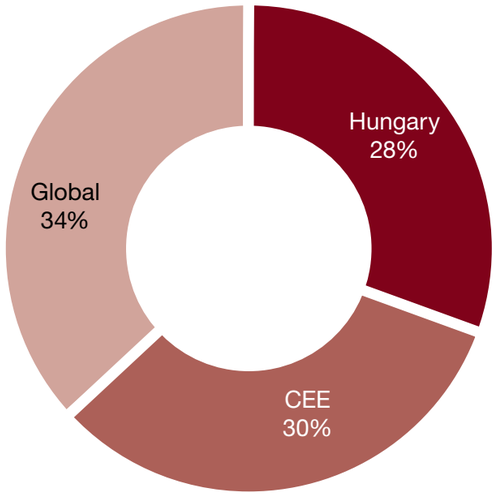
## Central themes

### Safer than CEE?

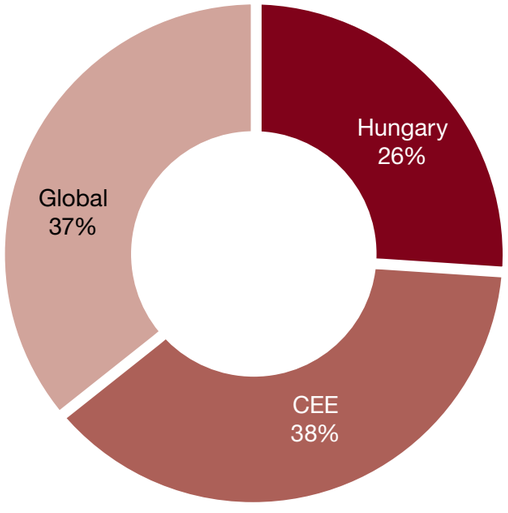
We have not seen a material change in the reported economic crimes since the previous survey. In 2011, the number of Hungarian companies detecting fraud was somewhat below the regional and global average.

This year, similar to 2011, approximately a quarter of respondents indicated their companies detected economic crime in the past 24 months, more than 10 percentage points below the global and regional average (37% and 38% respectively).

**Shares of companies experiencing economic crime: GECS 2011**




**Shares of companies experiencing economic crime: GECS 2014**




Note:

GECS 2014 asked participants to describe their experience with economic crime in the previous 24 months whereas GECS 2011 asked about the 12-month experience of the survey participants.

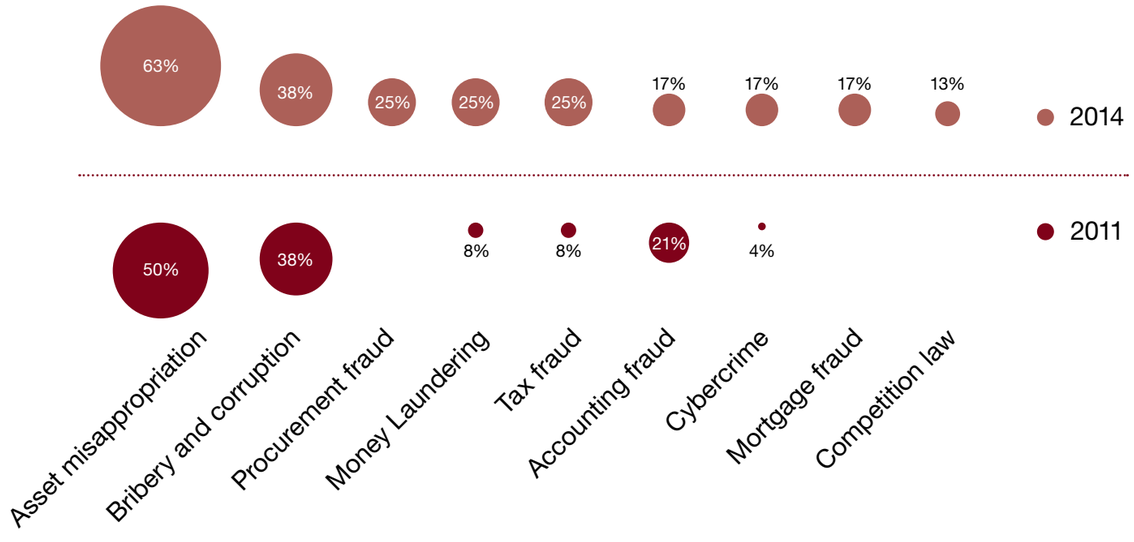
## High diversity in economic crimes

Asset misappropriation remains the traditionally most common and most simple type of crime. Yet it is clear that attacks against corporate assets can take diverse forms.

It is quite likely that the relative occurrence of crimes such as bribery, cybercrime or procurement fraud is even higher. These types of crimes are difficult to detect. During our own forensic engagements, we encountered numerous instances of long-going schemes which were detected by the victim company by accident.

Therefore, companies should consider different fraud schemes they may be facing. Control over cash and other physical assets might not be enough.

**Economic crimes as reported by companies**




Note:

procurement fraud, mortgage fraud and competition law abuses were not included in GECS 2011 as separate categories. Less frequent types of crime omitted for clarity.

# Cybercrime

Compared to the previous survey, the share of respondents experiencing cybercrime increased to 17% from about 4%.

Cybercrime can be described as one of the most dangerous crimes of this century. This is supported by:

- survey results on actual occurrence
- survey results on perception of future threats;
- the very nature of today's business transactions and the increasing dependence on computer applications.

Cybercrime might take completely new forms, previously unheard of, or find room for old types of fraud in the network environment, e.g. theft of working time and bandwidth (malware used for distributed denials of service; there was no equivalent in pre-computer times) and now Bitcoin scams using fake marketplaces (an old fraud in a new environment, where the users may not always recognize the hazards). This increases the general risks of cybercrime.

About a third of respondents indicated that their perception of cybercrime risks has increased over the last 24 months. This is a significant increase compared to our 2011 survey, according to which only 14% of Hungarian respondents commented that their perception of cybercrime risk had increased.

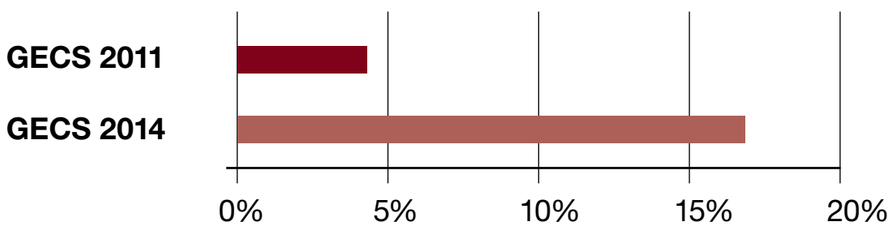
Our survey suggests that theft of intellectual property, personal data, reputational damage and service disruption are of the greatest concern when it comes to cybercrime.

While globally 30%, and in the CEE 26% of respondents believe that their organisations will likely face cybercrime in the following 12 months, in Hungary only 16% of respondents believe so.

Modern companies are following trends in utilizing technology to its full potential, and are giving their employees more freedom. People work from home using their own smart devices connected to the cloud, respond to emails from vacation in internet cafes, and review reports at airports. This is basically enlarging the perimeter that needs to be protected, making it necessary to deal with environments that are not fully under company control.

This is also a reason for a shift in the security paradigm: 90s - respond after the breach, 00s - get ready for the breach, 10s - assume the breach has happened or is underway. It is not a question whether the company will be subject to cyber-threat, but when and how it will happen.
Successful companies are prioritizing in what matters most - guarding their crucial data against organized attackers who target intelligently in a global business ecosystem consisting of fluid data moving around internally as well as to/from business partners and other stakeholders.

## Hungarian companies experiencing cybercrime




# Procurement fraud

For the first time, GECS 2014 included procurement fraud as a separate category of economic crime. 25% of respondents indicated that their companies experienced at least one instance of procurement fraud. This was globally the second most frequently indicated economic crime. The most vulnerable point, both in Hungary and globally, is the vendor selection process.

The reported high occurrence of procurement fraud exceeded even our expectations. There are numerous ways how procurement fraud can be committed. As a result, procurement fraud is one of the more complex fraud to be detected and investigated. As the detection of procurement fraud is difficult, it is possible that the actual occurrence is even higher. The impact of such fraud can be severe, and financial loss is often not the most damaging aspect. Employee morale, relationships with business partners or company's reputation are all at risk.

With only preventative measures in place, there is a higher risk that a determined fraudster can operate undetected for longer. Employing additional detective measures can help identify fraud earlier, resulting in reduced loss.

# Corruption and bribery

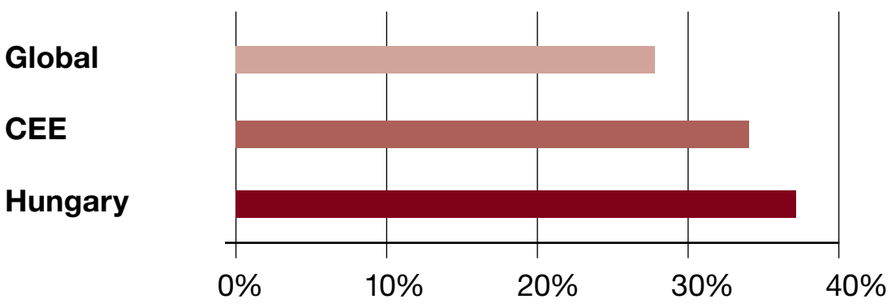
Corruption is seen as the greatest risk in doing business globally, both in terms of reputation loss and monetary loss.

According to this survey, in terms of occurrence, corruption and bribery is the second and third most frequently indicated type of economic crime in Hungary and globally respectively. Central and Eastern Europe is, along with Africa, the region with the largest prevalence of corruption.

This is also in line with the findings of PwC's CEO Survey, which indicated that corruption awareness is on the rise; more than half of the CEO's surveyed say they are concerned or very concerned about corruption as a threat to their organisations.

Almost one in five Hungarian respondents indicated that their company was asked to pay a bribe in the last two years. One in three Hungarian respondents believe that their company lost an opportunity to a competitor which they believe had paid a bribe during the same period.

## Share of corruption and bribery in total fraud reported



## Impact of economic crimes

No discussion of economic crimes would be complete without trying to place a value on the impact of fraud. After all, the anti-fraud effort is another function of the company which should pay off to justify its existence.

It is very difficult to accurately estimate the financial impact of economic crime. However, we asked our respondents to estimate, to the best extent possible, the cost of fraud and economic crime, they have suffered. 58% of respondents reporting fraud estimated the total financial loss of their company due to economic crime as being between USD 100,000 and USD 5 million.

This is an increase compared to 42% per our 2011 survey and exceeds both the regional and global results (43% and 38%, respectively).

There are also other negative impacts on the company besides purely financial losses. Consistent with both the previous Hungary results and the global results, the companies report an impact on employee morale as the greatest non-financial impact.

In this respect, we would like to point out that negative impact on employee morale might serve as a trigger of secondary, induced fraud being perpetrated by frustrated or demotivated employees. “Everybody does it” or “they deserved it” has been many times observed as a handy rationalization of first-time fraudsters.



# Managing fraud

## Who commits fraud

We tried to make a profile of the perpetrator of the most serious economic crime the respondents’ companies had experienced.

The responses indicate that in the majority of Hungarian cases, parties external to the organisation are the main perpetrators of economic crime (58%). Vendors and customers represent the bulk of external perpetrators. Fraud committed by vendors (21%) is nearly double the regional (11%) and global (10%) average. This is also consistent with the fact that procurement fraud was the third (together with money laundering and tax fraud) most frequently experienced type of economic crime in Hungary.

Our view has not changed since our last survey. Namely, based on our experience, due to a lack of resources, some organisations tend to neglect the importance of background checks on their business partners. This can lead to, in many cases, organisations not having a clear picture of the past business history and reputation of their business partners. If corporate intelligence/background checks of external parties (vendors, agents, intermediaries, etc.) are not performed, questionable business ethics cannot be identified in time, and the organisation can become a victim of economic crime.

We recommend that organisations step-up their efforts in this area. As a key prevention measure, knowing your business partners prior to engaging with them is less costly than dealing with the unpleasant consequences.

According to the surveyed companies, the share of fraud performed by internal perpetrators is 42% which is in line with 46% for CEE. The responses indicate that middle and senior managers are more likely to commit fraud than junior staff members, which is also in line with the findings for the CEE and globally. The most typical internal fraudster is a male, 31-40 years old, who has spent three to five years in the company.

## Prevention of fraud

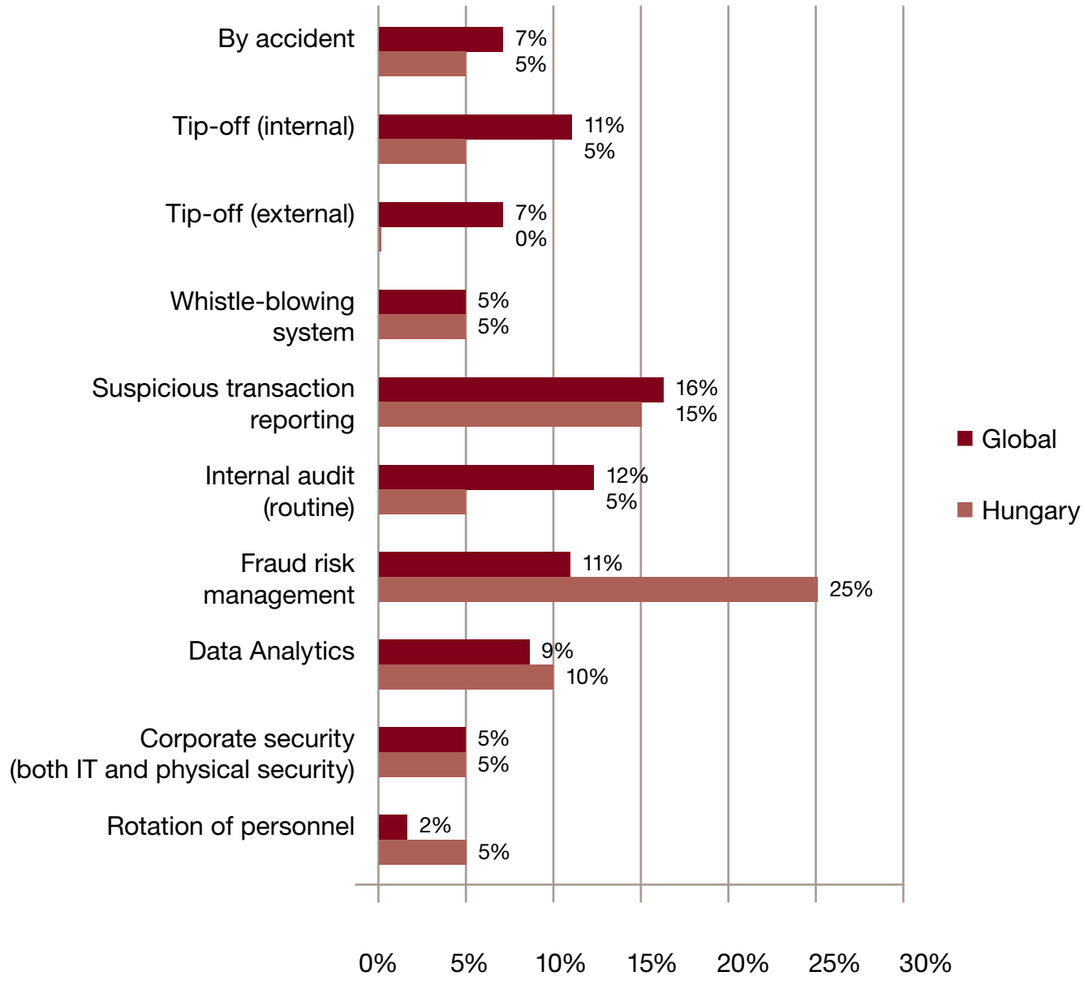
Why would someone decide to commit fraud? Our survey indicates that, by far, the most significant contributing factor for internal fraudsters is simply opportunity.

At the same time, out of possible contributing factors, opportunity is the one most within a company’s control. Therefore, a review of procedures in the areas most vulnerable to fraud may be an effective way to reduce the risk of falling victim to fraud.

# Detection of fraud

Companies do not take economic crime lightly. It is encouraging to see that there are responsible corporate executives who are not leaving the detection of economic crime to chance. They use proactive methods such as fraud risk management (25%) and suspicious transactions reporting (15%). Proactive identification and detection of economic crime are the most powerful tools in the fight against fraud.

## Method of detection of the most serious economic crime




On the other hand, there is still room for proactive actions. Data analytical methods could be used more often as these techniques can be a very cost-effective supplement of traditional methods, when employed correctly.

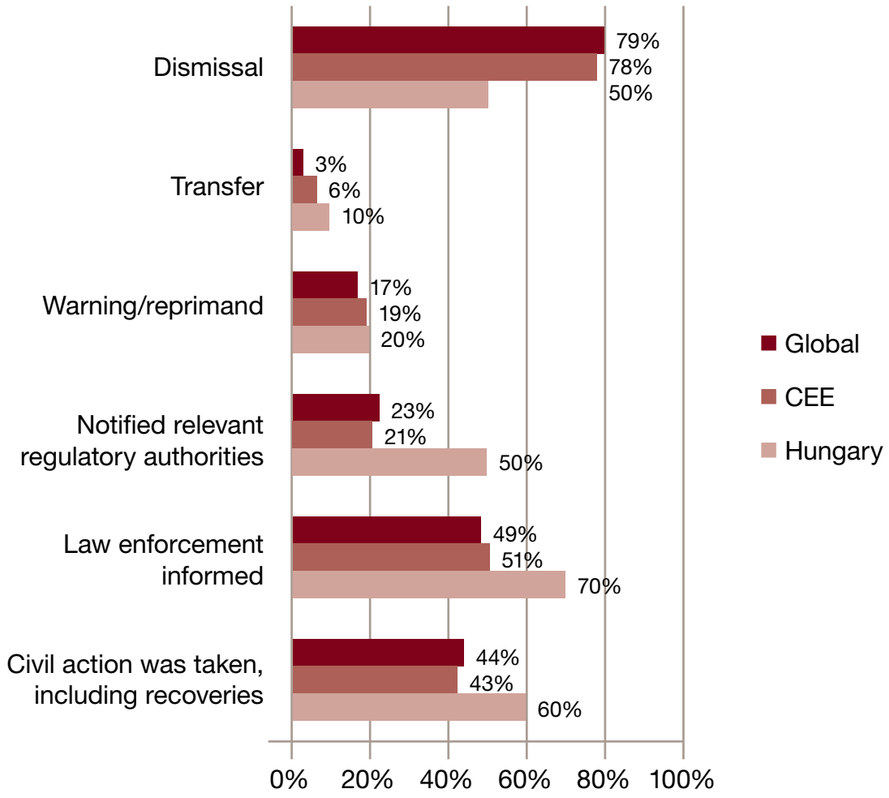
And what's the first reaction of a company when potential fraud is detected? Most companies resort to internal investigation.

## Initial measures taken

# Remedial actions

Compared to our 2011 survey, we see that companies are taking a tougher stance against fraudsters. Namely, this time we did not have any companies indicating that no action was taken against internal perpetrators of fraud, whereas in 2011 almost a quarter of companies reported that no action was taken. Also, it appears that Hungarian companies are more prone to start civil action and turn to law enforcement agencies or regulatory authorities than their peers in the region or globally. This would suggest a better awareness of companies that fraud is costly. Especially in times of economic turmoil, there are few reasons to take fraud lightly.

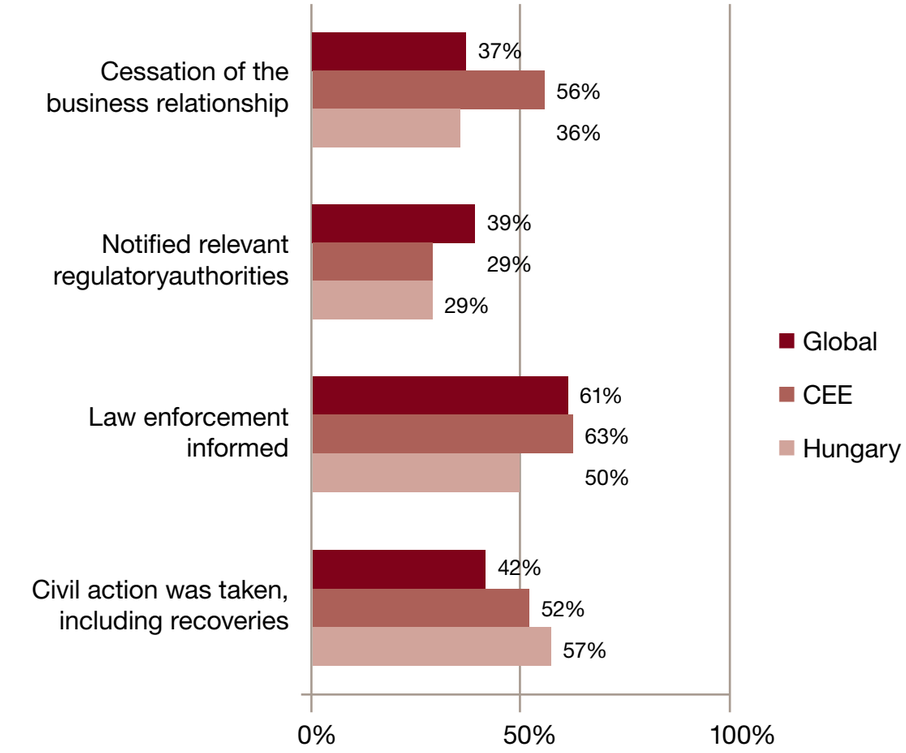
## Actions against main internal perpetrator




But at the same time (in line with our 2011 survey results) only about half of the companies reported that internal perpetrators were dismissed; this is lower compared to almost 80% reported regionally and globally.

With an external perpetrator, dismissal is obviously not an option. It appears that Hungarian companies prefer to take civil action including claiming damage compensation more than their regional or global peers. Terminating business relationships or involving law enforcement agencies is not as popular among Hungarian companies as in the case of regional companies.

## Actions against main external perpetrator




# Who responded

Our survey was conducted in fall 2013, with the participation of 91 companies from Hungary.

The study was not focused on a specific type of organization. The respondents were from all sizes and types of companies, ranging from purely local companies (38%) to truly global ones (26%).

Among the respondents there were CEO's (34%), CFO's (21%), heads of departments (20%) and general managers (13%). Their principal functions included mainly executive management (34%), finance (31%) and compliance (10%).

We would like to once again thank our respondents for all the information they volunteered and all the thoughts they shared.

# Contacts


***Miklós Fekete***
Partner
E-mail: miklos.fekete@hu.pwc.com
Tel.: +36 1 461 9242

***George Surguladze***
Senior Manager
E-mail: george.surguladze@hu.pwc.com
Tel.: +36 1 461 9127


pwc

*www.pwc.com/hu/crimesurvey*


© 2014 PricewaterhouseCoopers Hungary Ltd. All rights reserved. In this document, "PwC" may refer either to PricewaterhouseCoopers Hungary Ltd. or to the PwC network of member firms, each of which is a separate and independent legal entity. For more information, please visit the http://www.pwc.com/structure website.

*PwC Middle East Economic Crime Survey*
*February 2014*

# *Economic Crime in the Arab World*

**21%**
One in five Middle East organisations report being the victim of economic crime

**5%**
Only 5% of frauds were detected by routine Internal Audit

**37%**
More than one in three victims of economic crime reported incidents of cybercrime

**38%**
More than one third of Middle East respondents believe they will suffer procurement fraud in the next 2 years

pwc

*www.pwc.com/me*

*According to 70% of CEOs surveyed, economic crime continues to be a major concern for organisations of all sizes, across all regions and in virtually every sector.*

# *Table of contents*

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with close to 184,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

Established in the Middle East for 40 years, PwC has firms in Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Oman, the Palestinian territories, Qatar, Saudi Arabia and the United Arab Emirates, with around 2,700 people. (www.pwc.com/middle-east)

# *Foreword*

We are pleased to present to you our second edition of the PwC Global Economic Crime Survey – Middle East Report. This survey provides the views of respondents from more than 230 organisations in nine Arab Countries making it one of the most comprehensive studies in the Middle East.

This report provides important insights into the trends of economic crime in the region. Economic crime is a risk that threatens economic development and impacts the welfare of peoples. Economic crime in the public sector impacts every aspect of daily life and hinders investment. It also threatens businesses by compromising their internal processes, eroding the integrity of employees, and tarnishing reputations that take long years to build.

In the past few years we have seen an increased focus by both the public and private sectors on fighting economic crime. Many governments have set up anti-corruption bodies tasked with reducing corruption in their countries by implementing proactive measures, reacting to incidents, or both. Although we have seen several good initiatives much more is still needed to build the capacity to fight economic crime and reduce it to much lower levels. On the other hand countries that have witnessed changes in ruling regimes have suffered from a deficit of controls which correspondingly increased the risk of economic crime.

A determined focus is needed by the incoming governments to combat economic crime, and to reinstate supervisory and control bodies at a national level.

In the private sector, we have been seeing an increased focus, particularly within large businesses, on building their fraud risk frameworks. Over 70% of the CEOs of some of the leading organisations in the Middle East who participated in PwC's Global CEO Survey [1] highlighted that they are concerned or extremely concerned about the risk of bribery and corruption. We have also noticed that businesses in the region are increasingly starting to realise that proper responses to incidents of economic crime, despite the short-term impact on employee morale, can act as an effective deterrence mechanism, helping in the longer term to set the proper tone in the organisation and preserve value.

This year we have made two particular themes the focus of our report. Our survey shows that cybercrime is now the second most reported type of economic crime in the region, hence we have devoted a section of our report to it. In addition, we focus on corruption which remains a pervasive risk to the region, both in terms of the level of incidents reported in our survey and the significance of the negative impact this creates inside and outside our borders.

We hope that you will find this report useful both as a reference point in the ongoing campaign against economic crime but also as a strategic tool to help you consider the economic crime risks which your organisations face, and to enhance your control mechanisms to prevent, detect and respond to economic crime.

We are very grateful to all the respondents and organisations that made this Middle East Report possible by taking the time to complete the survey.

John Wilkinson, Partner
Middle East Forensic Services Leader
Dubai – UAE

Tareq Haddad, Partner
Middle East Investigations Leader
Riyadh – KSA

[1] www.pwc.com/ceosurvey

# The highlights

**21%**

*Reported incidents of economic crime in the Middle East have declined. 21% of respondents in the 2014 survey suffered some form of economic crime, compared to 28% in 2011. This contrasts with the results of our global survey which saw an increase in reported incidents from 34% to 37% over the same period.*

*Asset misappropriation remains by far the most commonly reported type of economic crime followed by cybercrime and bribery and corruption.*

*Cybercrime is now the second most common form of economic crime reported, demonstrating the extent to which new technologies are creating opportunities for technologically sophisticated fraudsters.*

*More than half of the respondents believe that bribery and corruption is a significant risk to their organisation when doing business globally. 18% of respondents indicated that their organisation had been asked to pay a bribe, and 24% believed their organisation had lost out to a competitor who paid a bribe.*

**18%** of respondents indicated that their organisation had been asked to pay a bribe

**24%** believed their organisation had lost out to a competitor who paid a bribe

*This year's survey identified significant incidences of procurement and human resources fraud, each of which were reported by more than one third of those who reported suffering some form of economic crime.*

*Over 60% of respondents who reported fraud indicated that the perpetrators were internal staff, with nearly 90% of those indicating that 'opportunity' was the biggest factor contributing to this.*

*The profile of a fraudster has changed: whilst the majority of economic crime is still perpetrated by male, internal staff our 2014 survey shows the principle demographic is senior management staff aged 41-50, rather than middle management staff aged 31-40 as reported in 2011.*

*Respondents in the Financial Services sector reported that 60% of frauds suffered were perpetrated by external parties, significantly above the results for any other sector.*

**60%** External

*Regrettably 16% of economic crime in the Middle East is detected by chance, significantly above the global average of 7%, indicating a widespread lack of effective fraud detection methods in the Middle East.*

*The financial impact of economic crime remains high: 12% of respondents said that the direct financial impact on their business was greater than USD5 million in the last 24 months. Interestingly, the percentage of respondents who indicated that the financial impact was greater than USD 100 million increased to 6%, which is three times the global average.*

*The perceived non-financial impact of economic crime has changed. In our 2011 survey the greatest perceived impact was on the reputation or brand of the victim organisation. In our 2014 survey our respondents indicated that the greatest perceived impact was on employee morale.*

*More than 38% of respondents predicted that their organisation will suffer from some form of economic crime in the next 24 months.*

*Looking ahead, Middle East organisations are most concerned about procurement fraud, bribery and corruption and asset misappropriation. In our opinion all organisations must be concerned about cyber crime, which we expect to be a growing trend of criminality in the coming years.*

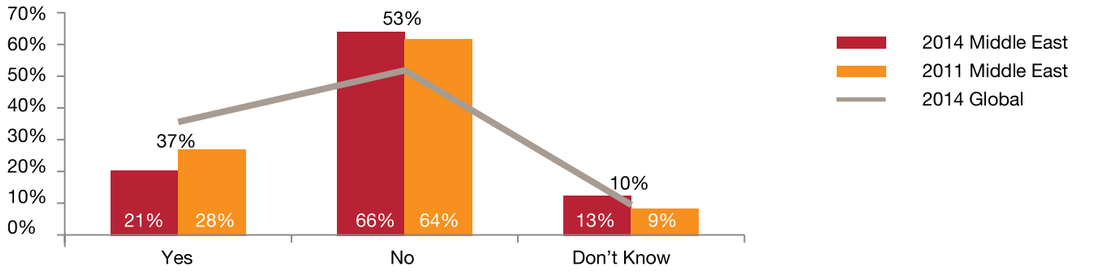
# *Economic crime in the Middle East*
## The big picture

The 2014 GECS confirms that economic crime remains a fundamental fact of life for organisations in all regions and in all industries. The worldwide incidence of reported economic crime is on the rise – 37% of respondents globally reported suffering some form of economic crime compared to 34% in the 2011 survey.

This global trend in reported frauds has always fluctuated, but in every survey in the 14 years since the PwC Global Economic Crime Survey was launched the figure has been at least 30%.

In the Middle East, however, the situation is different. Our 2011 Middle East report highlighted that 28% of respondents indicated that their organisations had reported incidents of economic crime – well below the global average. This year's report indicates that the rate of reported incidents of economic crime has dropped to 21%. Nonetheless, those organisations which reported economic crime experienced more types of economic crime than the global position. This could suggest that where economic crime is present it is more pervasive in Middle Eastern organisations than the global average.

**Figure 1: % of respondents who suffered some form of economic crime**

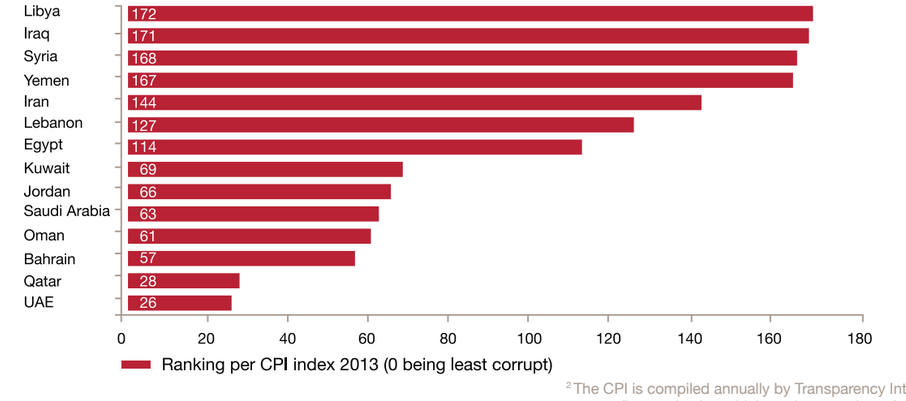



To put this into further context, the Middle East reported fewer incidents of economic crime in both the 2011 and 2014 surveys than any other region, with the nearest comparator being Asia Pacific, where the figure is 32%. This is despite the fact that several countries in the Middle East have scored poorly on Transparency International's Corruption Perceptions Index[2].

It is important to note that there is an element of undiscovered fraud that has to be taken into consideration when looking at these results. Alarmingly, 16% of cases of reported economic crime in the Middle East were discovered by accident. While the true level of undetected fraud is very difficult to measure, the strength and effectiveness of fraud detection mechanisms can assist in identifying more incidents of economic crime.

Furthermore, in performing our analysis a clear story has emerged. The extent to which organisations in the Middle East are actively taking steps to protect themselves from economic crime is also below the global average: fraud risk assessments are conducted less frequently than the global norm – 54% of our respondents indicated that they had performed some form of assessment in the past 24 months compared to a global average of 64%. In the absence of a robust fraud risk assessment adequate risk-based controls cannot be properly planned and implemented. This in turn leads to a lower than average rate of detection of economic crime from manageable internal controls such as internal audit (Middle East: 5%, Global: 12%), targeted fraud risk management controls (Middle East: 3%, Global: 11%) and structured data analysis (Middle East: 5%, Global: 9%).

**Figure 2: Middle East country rankings, CPI index 2013**




[2] The CPI is compiled annually by Transparency International, a non-profit organisation which tracks a number of corruption indices. Please refer to www.transparency.org

The big picture, therefore, is that while the level of reported economic crime has declined in the region, organisations throughout the Middle East should be doing more to implement tailored, fraud risk focused controls to identify and combat the current level of unreported economic crime.

In this report we analyse the types of economic crime suffered in our region and their impact in both financial and non-financial terms. We also highlight the profile of those reported to have perpetrated fraud and provide some practical guidance on what businesses can be doing to mitigate their risk.

# *Types of economic crime*
## Common themes, emerging threats

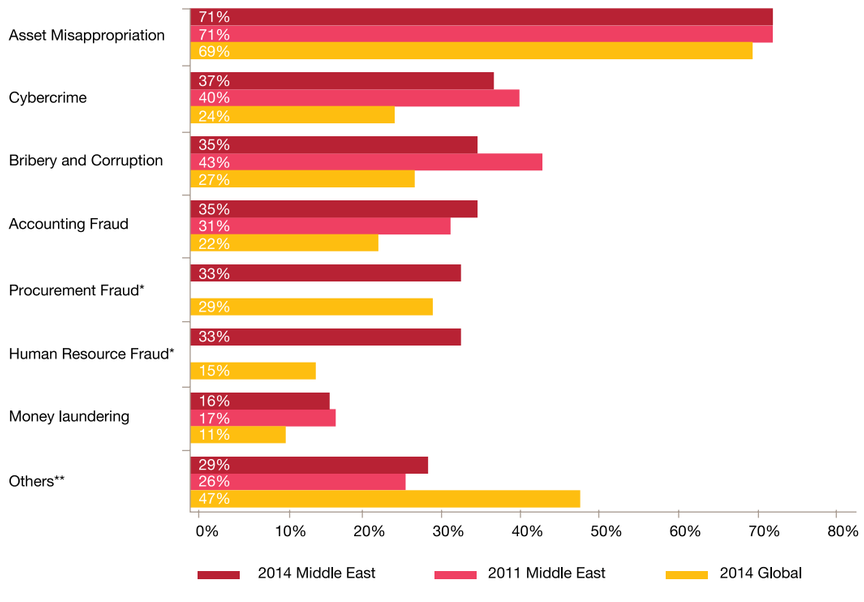
The results of the survey identified that 21% of respondents had suffered at least one instance of economic crime in their organisation. This rate of reported incidents is lower in the Middle East than anywhere else in the world, but the variety of crime suffered by those who did experience it in some form is consistently more varied than the global picture.

The survey showed that four types of economic crime remain most common: asset misappropriation (by a considerable margin), cybercrime, bribery and corruption and accounting fraud. In our 2014 survey accounting fraud, unlike any other type of reported economic crime, has increased compared to the results in 2011.

This year, to recognise our perception of their importance both globally and within the Middle East, we have separately identified two further categories in our survey: procurement fraud and human resource fraud. Our experience in the Middle East is that these two business processes are of particular concern to the C-suite, and it is interesting to observe the significant volume of respondents who experienced economic crime related to them.

The graph below provides further detail on the range of economic crime suffered.

**Figure 3: Types of economic crime suffered**




** represents category introduced in the current year's survey*
*** 'Others' includes IP infringement, tax fraud, insider dealing, mortgage fraud, anti-trust practices and espionage.*

***Asset misappropriation*** remains the most commonly encountered crime by organisations globally and in the Middle East. This is not surprising: theft of assets is the simplest form of economic crime, requiring minimal technology. It is perhaps the category where 'opportunity' plays the most significant role, as explored further below.

***Cybercrime*** ranks, for the first time, as the second most reported economic crime in the Middle East though globally it is in fourth position[3]. Recent sophisticated cyber attacks in the region, combined with an increase in concerns about cyber security at a governmental level, may have contributed to this increase. Unsurprisingly respondents perceive the greatest threat of cybercrime coming from outside their organisation.

***Bribery and corruption*** remains a significant threat in the Middle East and globally. Headline news has showed us that this type of economic crime can have some of the most devastating impacts on organisations.

***Accounting fraud*** has been more prevalent in the Middle East than globally over the last 24 months and, unlike the majority of other fraud types reported in our survey, has actually increased over that period. This could be a result of increasing pressure on management teams in the region to achieve ambitious financial and profitability targets.

As noted above, procurement fraud and human resource fraud are included in our survey as separate categories for the first time, and both are regularly suffered by Middle East respondents.

The high incidence of ***procurement fraud*** is interesting in the light of traditionally tight procurement tendering processes in this region. Our survey respondents who reported suffering from procurement fraud were asked to indicate which parts of the procurement cycle had experienced fraud in the past 24 months (see figure 4). The results indicate that current tender and vendor selection methods are not proving effective: a significant majority of respondents indicated that fraud is occurring in these stages of the procurement process, rather than at the payment stage.

**Figure 4: Procurement fraud in the Middle East vs. Global**

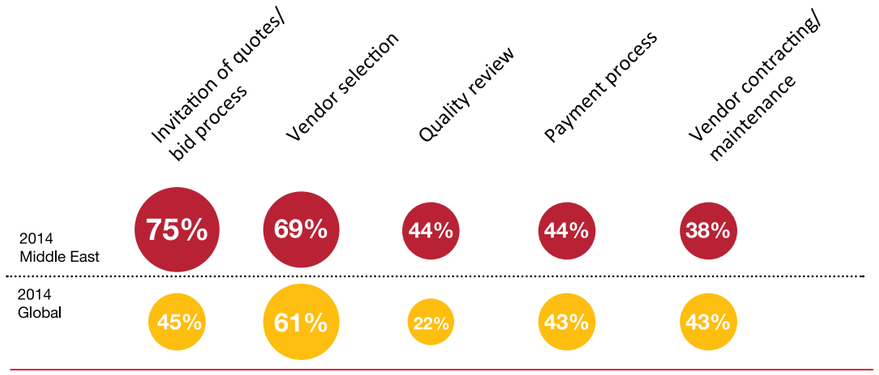
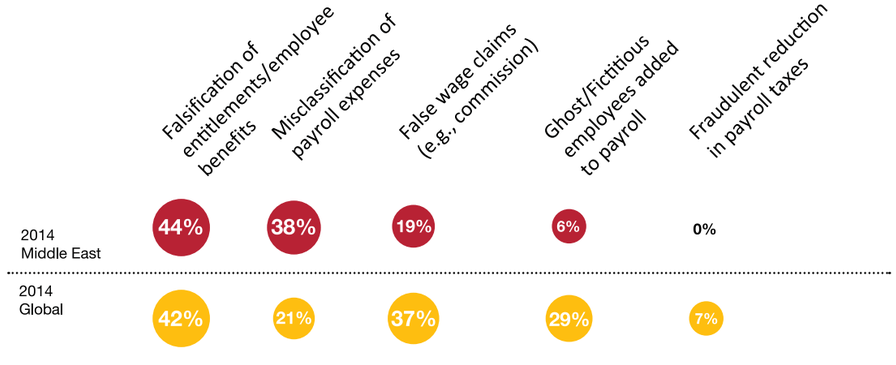



**Figure 5: HR fraud in the Middle East vs. Global**




[3] In the global survey asset misappropriation, procurement fraud and bribery and corruption are more commonly reported.

*Combating procurement fraud – take preventative action*

*Even with strong controls in place, the procurement process can be vulnerable to fraud both from within the organisation and from outside.*

*In our experience, enhanced background screening of personnel involved in the tender process, coupled with thorough due diligence on bidding parties reduces the risk of procurement fraud. This will assist in identifying conflicts of interest, the decision makers' vulnerabilities and exposures, and the bidding parties' track record regarding fraud and corruption. Few organisations of any size undertake detailed checks of their bidders, and yet the evidence of previous misconduct may be easy to find. Due diligence of all parties need not be time consuming or costly, but will give companies more confidence in the ability of their tender board to make objective decisions and will expose bidders to an enhanced level of scrutiny.*

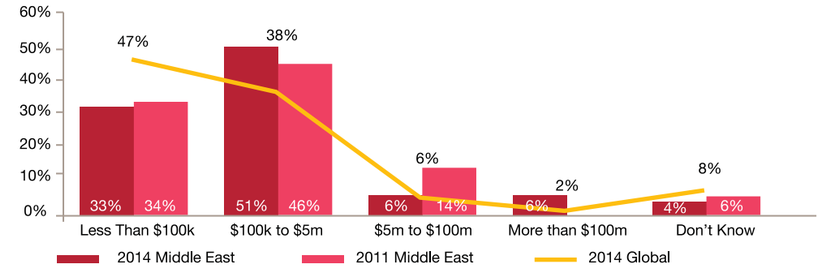
Courtenay Smith, Head of Corporate Intelligence, PwC

# *The damage caused by economic crime*
## A financial and non-financial cost

Of those who indicated that their organisations reported economic crime 51% said that the direct financial impact on their organisation of all frauds suffered in the last 24 months was between USD100,000 and 5,000,000, representing an increase from our last survey when the figure was 46%.

At the top end of the scale there are indications that incidents of economic crime of high financial impact increased where results show that 6% suffered total losses in excess of USD100 million. This indicates that the percentage of reported economic crimes in the Middle East where the financial losses are more than USD100 million is three times the global average.

**Figure 6: The financial impact of economic crime**




The case for more focus on prevention of fraud is therefore clearly proven from a financial perspective. But what about the non-financial impact that economic crime has on Middle East organisations?

### Collateral damage

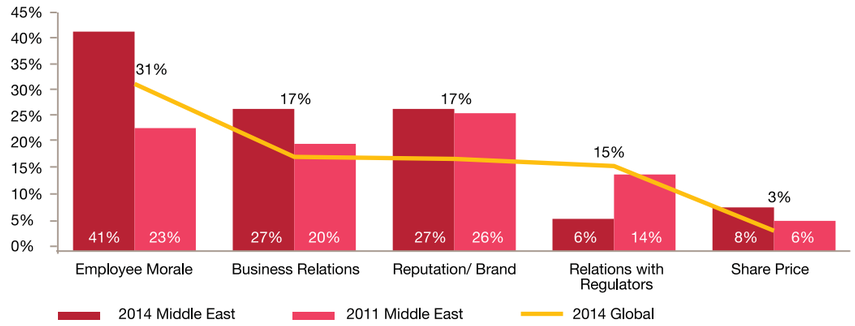
The fallout from fraud is not merely the direct cost. Our survey has highlighted the collateral damage suffered by Middle East organisations, taking into account a range of factors as shown at figure 7 below.

The change in these statistics since our last report is stark – Middle East organisations now consider damage to employee morale to be the number one collateral impact of suffering economic crime, ahead of more traditional 'commercial' indicators such as business relationships and brand reputation.

This is in line with the results from the global survey, but a significant shift from the Middle East results in 2011, when brand reputation was believed to be the most significant.

When evaluating the impact of economic crime it is important to consider the financial aspects in conjunction with the collateral damage which could have an impact on the organisation's productivity, ability to generate revenues, and ability to gain the trust of stakeholders including employees, business partners, shareholders and regulators.

**Figure 7: The collateral impact of economic crime**



# *Looking to the future*
## Is economic crime on the rise?

Our survey asked respondents to consider the likelihood that their business would be a victim of economic crime in the future.

In our 2011 survey we indicated that the trend in reported incidents of economic crime was likely to rise: 28% of respondents at that time reported having suffered some form of economic crime in the past 24 months, but a significantly larger percentage thought the future looked bleak: 39% believed they were likely to suffer from at least one type of economic crime.

There is therefore a significant variance between the future expectations of respondents in 2011, where at least 39% predicted that their organisations would suffer from economic crime, and the level of reported incidents indicated in our 2014 survey of 21%. The results of the survey do not directly explain this variation: however the inherent nature of economic crime suggests that there will always be a level of incidents that will go undetected. It is also interesting to note that this year respondents again predict a further increase over the next 24 months, with 38% expecting their organisations to suffer from at least one type of economic crime.

**Figure 8: Trends in Fraud Perception**


** represents categories included in the current year survey*

In many cases, as shown by figure 8 above, these perceptions are greater than the global average.

*37% of organisations who reported economic crime were victims of cybercrime in the last 24 months*

# *Spotlight:*
## Cybercrime in the Middle East

### The emerging threat

One of the key findings from this year's survey is that cybercrime is now the second most reported economic crime in the Middle East, rising from third in our 2011 survey.

Globally, 24% of respondents who suffered from some form of economic crime reported cybercrime, up one percentage point from 2011. In this region the burden is more significant, with 37% of victims of economic crime suffering from cybercrime.

According to a recent PwC survey[4], the most commonly occurring cyber threats in this region are to applications, systems and networks, but mobile devices, removable storage devices and data held by third parties are also at risk.

Recent high profile cases in the Middle East highlight the risks: in 2012 two of the region's largest oil and gas companies were reported to have been subject to cyber attacks which affected tens of thousands of individual computers, causing widespread disruption.

In 2012 and 2013 there were reported cybercrimes in the financial services sector across the region, in particular in the UAE, Oman and Lebanon.

One of the features of this developing threat is the speed with which attacks can be carried out – often subjecting the victims to significant financial, data or other losses before they even realise that an attack is in progress, diminishing the effectiveness of any response. Meanwhile the very technology on which the victim organisations rely becomes the tool used against them by the sophisticated criminal, whose identity can quickly be hidden, or changed.

The pace of technological change is also a factor. Sophisticated hacking groups are at the forefront of the development of new technology, and keeping pace with their methods is a significant challenge even at a governmental level.

Fundamentally in this region and globally businesses are struggling to understand, and keep pace with, cybercrime risks. Networks are not protected in a sophisticated manner designed to prevent access by sophisticated external parties.

Many local governments in the Middle East are now taking action, led by the UAE's Cyber Crimes Law 2012 and Saudi Arabia's 2012 Arab Cybercrime Agreement, in a bid to combat the growing threat.

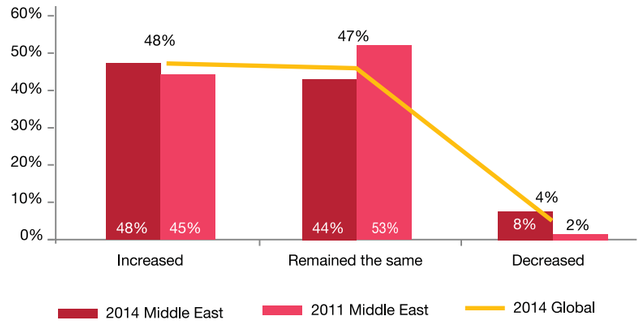
[4] www.pwc.com/security

## Perceptions

Our results show that cybercrime remains highly reported, both globally and in this region.

Perceptions are also changing. When asked whether their perception of the risks of cybercrime to their organisation had changed over the past 24 months 48% of our survey respondents indicated that the risk had increased, and 44% indicated that the risk has remained the same. Only 8% believed there had been a reduction in the risk from cybercrime.

**Figure 9: Perception of cybercrime**




## The cost of cybercrime

Quantifying the true cost of cybercrime is notoriously difficult for a variety of reasons. Factors such as the opportunity cost of implementing cyber security frameworks, interruption to operations, loss of business, impact on safety systems, damage to brand or reputation, lost opportunities through decisions to avoid certain markets or products as a result of the perceived risk of cybercrime or the value of intangible assets lost to cybercrime, such as data or industrial methodologies, are near impossible to calculate.

Despite this inherent difficulty, we asked our survey respondents to estimate the cost of cybercrime to their business in the past 24 months. 35% indicated that they did not know what the actual cost of cybercrime was, whilst 40% responded that they believed there had been no financial loss from cybercrime.

These results highlight the scale of the problem. In many cases, those organisations reporting that they had suffered no financial loss may simply be unaware that they have been the victims of cybercrime in the first place or have not properly quantified the true business cost of the cyber attack. This is not unusual: the results from our global survey are exactly in line with the Middle East findings, with 40% of organisations globally reporting that they suffered no financial loss.

Of the Middle East respondents who did indicate the value of their losses from cybercrime 6% indicated that the loss was greater than USD1 million, with 2% reporting losses between USD5 million and USD100 million.

Taken together our results indicate that the true cost of cybercrime may be far more significant than reported.



*Our experience has been that the level of sophistication employed by determined cyber criminals in the Middle East is as high as anywhere in the world. The persistency which hackers employ and the simple vulnerabilities they exploit present a real danger to Middle East organisations, whose staff may be the subject of cyber attacks and, knowingly or unknowingly, give away sensitive information or allow IT control breaches to occur. Combating this requires much broader planning than just IT security.*

Dean Gilbert, Head of Forensic Technology, PwC

## Where does the risk of cybercrime come from?

37% of respondents in the Middle East felt that the greatest cybercrime threat to their organisation came from outside their business, with only 9% believing the threat was internal.

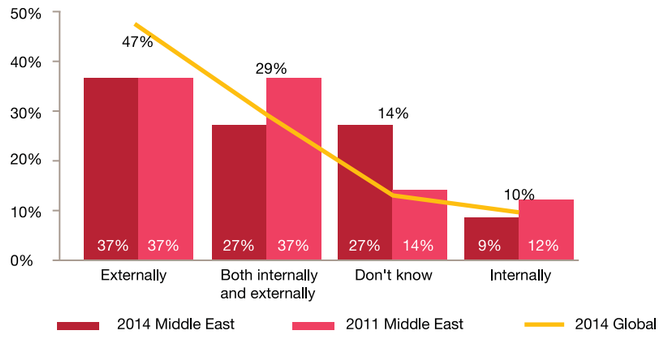
Whilst these results are not substantially different to the results from our 2011 survey, the increase in those who did not know where the greatest threat came from has increased dramatically from 14% in 2011 to 27% in 2014. In addition this figure is substantially higher than the global average of 14%. This suggests that more awareness about cybercrime and its impacts is needed in the Middle East.

## What are Middle East organisations really worried about?

We asked our respondents what aspects of cybercrime they were most worried about. The results demonstrate a high level of concern about a range of factors with reputational damage, financial loss, disruption to their services, theft of Intellectual Property and theft of personal information all being concerns for more than 80% of all survey respondents.

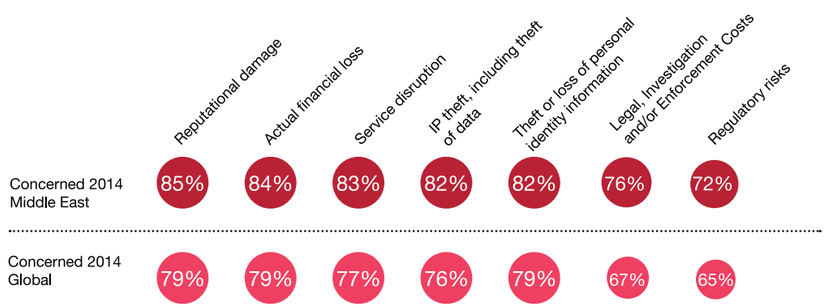
Our results also indicate that the level of concern is greater in the Middle East than globally, with respondents in this region expressing greater worry about every category of damage from cybercrime than the global average.

**Figure 10: Greatest threat of cybercrime**




Interestingly, respondents in the Middle East were least concerned with the regulatory risks and cost associated with legal support, investigation, and enforcement as a result of cybercrime.

**Figure 11 : What keeps organisations awake?**




### *Taking practical action – what can be done to combat the risk?*

- **Get the C-Suite involved** – the CEO and the Board need to be aware of the risks of cybercrime and how these can influence strategic business decisions.
- **Look at how prepared the organisation is for cybercrime** – unlike traditional economic crime, cybercrime is fast-paced and technologically advanced, which means the organisation needs to be prepared to continually adapt.
- **Set up a cyber incident response team that can act and adapt quickly** – the organisation can then track and assess risks and deal with an incident as soon as it is identified.
- **Fight fire with fire** – recruit people with the right skills and experience: expertise is key to understanding the threat and taking decisive action if an attack is detected.
- **Take a tougher and clearer stance on cybercrime** – the organisation should show it means business by taking legal action against cybercriminals where possible.
- **Consult with others** – sharing knowledge of current cyber threats with others in the industry can help to provide early warnings of new developments.



*35% of organisations who reported economic crime were victims of Bribery and corruption in the last 24 months*

# *Spotlight:* Bribery and corruption

35% of those respondents who indicated that their organisation had been the victim of economic crime had experienced corruption at some point in the survey period, making it the third most common crime suffered. This rate is significantly higher than the global rate of 27%.

When we asked about how the next 24 months look, **over one third of respondents in the Middle East predicted that their organisations would face bribery and corruption** issues in the next 24 months. It therefore remains a real risk.

While bribery and corruption was not the most common form of crime reported, of all the types of fraud covered in our survey it may pose the greatest threat to business both in the Middle East and globally. Cases of bribery and corruption reaching headline news indicate that the financial costs and collateral damage caused by incidences of bribery and corruption can be the most significant amongst the different types of economic crime. Governments, as well as commercial organisations in the Middle East are realising the increasing importance of fighting corruption.

At the public sector level several Governments in the Middle East region have established bodies mandated to lead the fight against corruption and bribery. Such organisations include the Abu Dhabi Accountability Authority in Abu Dhabi, the National Anti-Corruption Commission (Nazaha) in Saudi Arabia, the Jordan Anti-Corruption Commission in Jordan, the Anti-Corruption Authority in Kuwait and the Administrative Control and Transparency Authority in Qatar.

While many positive steps have already been taken by these bodies many are still in the early stages of development. Much work still remains to enable these organisations to effectively fight economic crime and reduce it to an acceptable level. Political will at the highest levels within Government is key to the success of these organisations.

On the other hand we have seen that businesses are starting to realise that more efforts are needed to fight corruption and to ensure that their business is driven by **innovation, competitiveness and efficiency.** This is particularly evident in larger organisations who are investing in enhancing and building their fraud risk management functions. We have seen several organisations and sovereign wealth funds conduct fraud risk assessments and design controls to specifically address corruption risks together with other types of fraud. We have also seen an increased awareness within boards of directors and audit committees about their responsibility to deal with the issues of corruption and bribery and launch objective and independent investigations where required.

Legislation and enforcement at a national and international level remain important factors in the fight against bribery and corruption. To date the US Foreign Corrupt Practices Act has already had an impact on businesses in the Middle East, though the UK Bribery Act has not yet had such a significant effect in the region.

At a national level, legislation and enforcement by Governments in the Middle East still require enhancement.

### *What action should organisations take to prevent bribery and corruption?*

The UK Bribery Act of 2010 sets out six principles that may serve as a guide for commercial organisations in the Middle East who wish to prevent bribery being committed on their behalf. These are helpful guidance to any organisation seeking to better control the risk of bribery, and not exclusive to those subject to the UK Bribery Act.

1. **Proportionate procedures** - A commercial organisation's procedures to prevent bribery by persons associated with it are proportionate to the bribery risks it faces and to the nature, scale and complexity of the commercial organisation's activities. They should be clear, practical, accessible, effectively implemented and enforced.
2. **Top level commitment** - The top-level management of a commercial organisation (be it a board of directors, the owners or any other equivalent body or person) are committed to preventing bribery by persons associated with it. They foster a culture within the organisation in which bribery is never acceptable.
3. **Risk assessment** - The commercial organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The assessment is periodic, informed and documented.
4. **Due diligence** - The commercial organisation applies due diligence procedures, taking a proportionate and risk based approach, in respect of persons who perform or will perform services for or on behalf of the organisation, in order to mitigate identified bribery risks.
5. **Communication (including training)** - The commercial organisation seeks to ensure that its bribery prevention policies and procedures are embedded and understood throughout the organisation through internal and external communication, including training, that is proportionate to the risks it faces.
6. **Monitoring and review** - The commercial organisation monitors and reviews procedures designed to prevent bribery by persons associated with it and makes improvements where necessary.

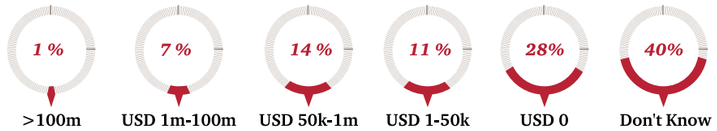
## Perception and impact of bribery and corruption

Consistent with the global average, more than half of the Middle East respondents said that they perceived corruption to be a significant risk to their organisation when doing business.

Two fifths of Middle East respondents said that the most severe impact that corruption had on their organisation was financial loss followed by damage to corporate reputation (27%). Globally however, 36% perceived damage to corporate reputation to have severe impact followed by financial losses (28%).

In the case of financial loss 7% of Middle East organisations and 4% of global organisations have lost between USD one million and USD100 million, with 1% in the Middle East losing over USD100 million. Surprisingly, 40% of organisations in the Middle East and 34% organisations globally are unaware of the amounts lost through corruption.

**Figure 12: Financial losses suffered through instances of bribery and corruption**




When asked if organisations had been asked to pay a bribe, nearly one fifth answered positively and nearly one quarter felt their organisation had lost an opportunity due to a competitor paying a bribe.

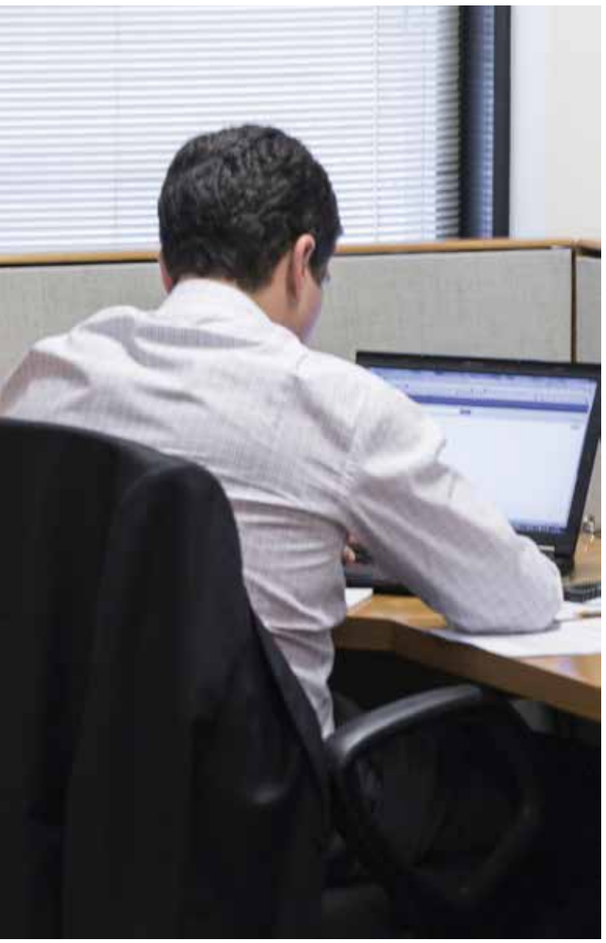


**Figure 13: Instances where organisation lost to a competitor**

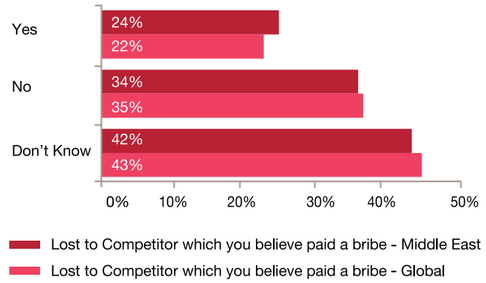
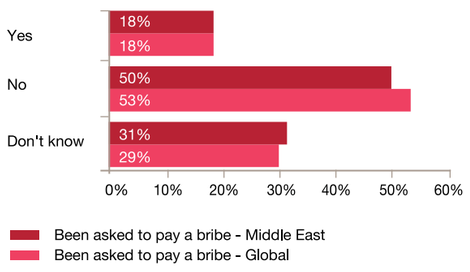



**Figure 14: Instances where organisations were asked to pay a bribe**




# *Know your enemy*
# Profile of a fraudster

As in our last survey we asked respondents who faced economic crime to profile the perpetrators of the most significant economic crimes impacting their organisation in the past 24 months.

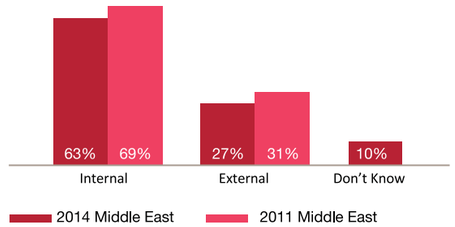
## The enemy in plain sight

A large proportion of the Middle East respondents (63%) said that the perpetrators of fraud were from among their own staff. This is higher than the global average of 56% but lower than the results of our 2011 survey, perhaps reflecting the emerging threat of cybercrime and money laundering, which are mainly associated with fraudsters from outside the business.

Interestingly, the profile of the perpetrator has changed from our last report in 2011. The typical fraudster in our last report was internal to the organisation, male, between the ages of 31-40 and in a middle management position with a tenure of 3 – 5 years in the organisation.

The most prevalent profile of a perpetrator in our current survey remains an internal staff member and male but is viewed as now most likely to be in a senior management position and aged between 41-50 with more than ten years in the organisation. They are typically educated to degree level or higher.

**Figure 15: Type of perpetrator**




## Profile of the internal fraudster

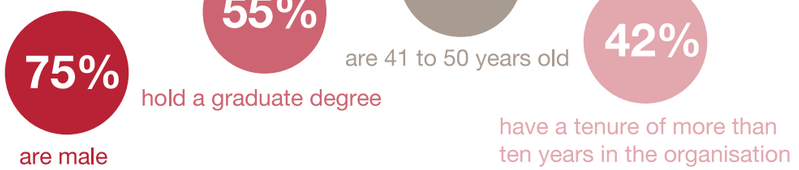



**Figure 16: Profile of the external fraudster**

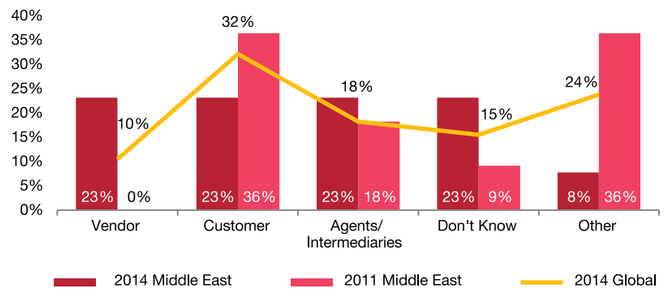
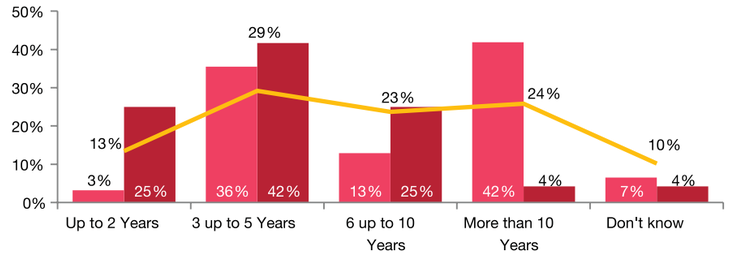
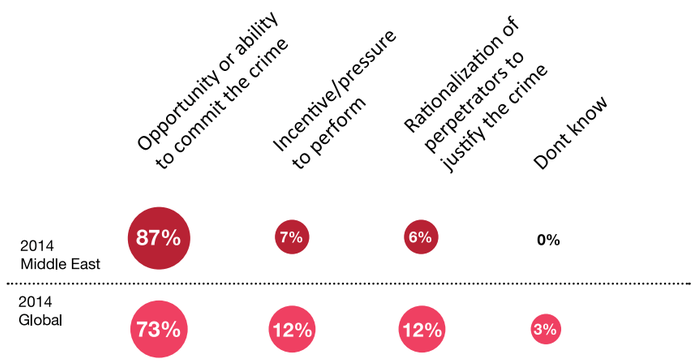


**Figure 17: Length of service**




We also asked our respondents to identify the factor that they believed had contributed most to economic crime within their orgnisation. Repondents overwhelmingly identified opportunity as the number one factor.

**Figure 18: Factors for economic crime by internal fraudsters**




Notwithstanding the individual demographic profile, the fact that perpetrators are mostly internal to the organisation is not surprising – given their greater level of knowledge over the organisations controls – but it should be considered an opportunity. Addressing the weaknesses in internal control which the internal perpetrator can exploit is one area over which management can have the most significant impact.

There are, however, exceptions to this rule. The financial services industry globally reports the inverse statistic – almost 60% of perpetrators are external.

In our Middle East survey 20% of respondents were from the financial services industry. One key driver is the risk faced by this industry from money laundering – almost universally a fraud perpetrated by external parties, in this case customers. Here, the results from the Middle East exceed the global average: 16% of respondents indicated they had experienced money laundering, compared to 11% globally.



# *Limiting the damage*

## Prevention and detection of economic crime

What can be done to detect an economic 'crime in progress'? Or better yet, how can it be prevented? Whilst there remains no sure way of eliminating fraud, the risk can be managed and reduced through effective controls.

### Prevention

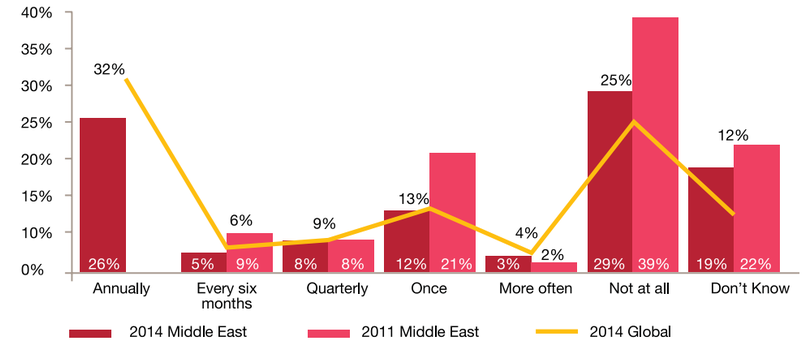
Preventing economic crime requires a clear understanding of what it is that needs to be prevented. A simple concept to grasp, but the only way to design effective anti-fraud controls is to conduct an assessment of the fraud threats that the business faces.

We asked our survey participants whether their businesses conducted fraud risk assessments in the past 24 months.

Only 42% of Middle East respondents indicated that their organisation conducted an assessment at least annually and 48% either did not conduct one at all or were not aware whether one had been conducted. As in our previous survey these results are substantially below the rest of the world, where reported incidents are noticeably higher – 51% of global respondents indicated that their organisation conducted a fraud risk assessment at least annually.

We also asked participants what the reasons were for not performing an assessment. One third of those who did not conduct one responded that there was a perceived lack of value from the process, highlighting the need for better education and awareness within organisations of the need for targeted fraud prevention.

**Figure 19: Frequency of fraud risk assessment**

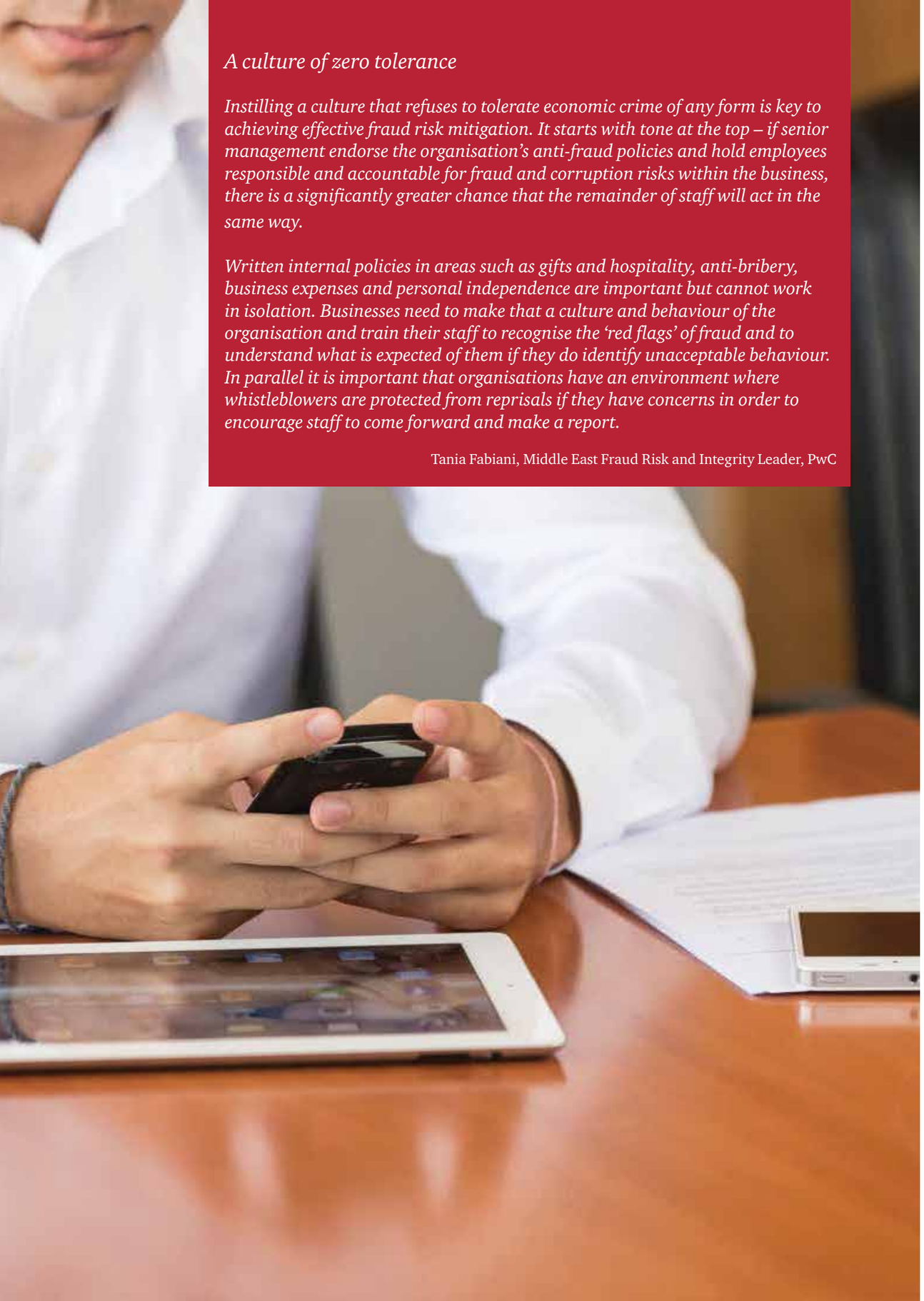



*Note: There is no comparative figure for 2011 for fraud risk assessment conducted "annually"*

In our view, the fact that the level of fraud risk assessments conducted in the Middle East lags behind the rest of the world, whilst reported incidents are significantly lower than the global average is an indication of the link between conducting fraud risk assessments on a regular basis and the detection of economic crime through focused controls when it occurs.

### *An effective fraud risk assessment considers factors from all angles:*

- **Internal**: What controls does the business already have in place, are they tested and robust? Does the assessment cover all areas of the business? What influence does organisational culture and tone at the top exert on the fraud environment? What policies and procedures exist, and what level of training do staff, including internal audit, have in preventing and detecting fraud?
- **External**: Does the business operate in any high risk jurisdictions? Which counterparties does the business trade with, and do they have any history of fraudulent or corrupt practices? What is the regulatory and law enforcement landscape like? What are the risks from cyber attacks? What are the common issues being faced by the industry in relation to fraud?
- **The past**: Has the business suffered fraud in the past, and were lessons properly learned and controls tightened? Has there been a history of fraud schemes in the relevant industry from which lessons can still be learned?
- **The future**: Is the business about to enter new markets? Are new staff, new products and new business processes forecast in the next 12 months?



*A culture of zero tolerance*

*Instilling a culture that refuses to tolerate economic crime of any form is key to achieving effective fraud risk mitigation. It starts with tone at the top – if senior management endorse the organisation's anti-fraud policies and hold employees responsible and accountable for fraud and corruption risks within the business, there is a significantly greater chance that the remainder of staff will act in the same way.*

*Written internal policies in areas such as gifts and hospitality, anti-bribery, business expenses and personal independence are important but cannot work in isolation. Businesses need to make that a culture and behaviour of the organisation and train their staff to recognise the 'red flags' of fraud and to understand what is expected of them if they do identify unacceptable behaviour. In parallel it is important that organisations have an environment where whistleblowers are protected from reprisals if they have concerns in order to encourage staff to come forward and make a report.*

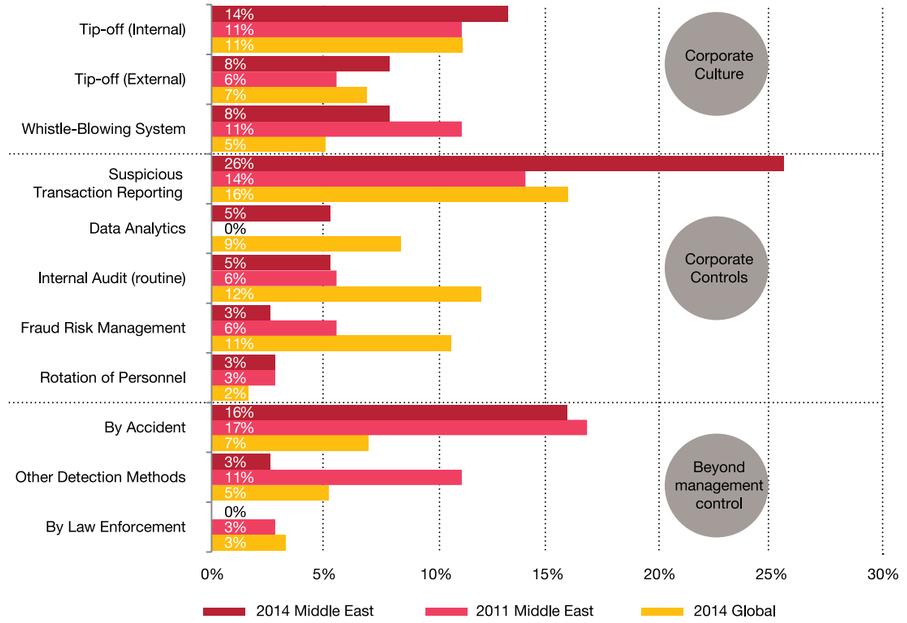
Tania Fabiani, Middle East Fraud Risk and Integrity Leader, PwC

## Detection

Detection methods can broadly be grouped into three categories: corporate culture, corporate controls, and 'beyond management control'. As discussed earlier, 63% of our survey respondents indicated that frauds were most likely to be perpetrated by internal employees – providing an opportunity to directly target fraud risk through reinforcement of corporate culture and controls.

Figure 20 below details the method by which the major fraud at reporting organisations was detected.

**Figure 20 : Detection of fraud**




## Corporate controls – more work is needed

Throughout our report we have highlighted the need for Middle East organisations to improve their focus on fraud risk management, principally through the establishment or enhancement of fraud risk assessments to improve the extent to which corporate controls target key fraud risks.

The methods by which frauds are detected reinforce this message: 16% of frauds are detected by accident, more than twice the average globally. Whilst it is pleasing to note that this percentage has decreased by one point from our 2011 survey, there is still real need for improvement.

Figure 20 above shows those methods of fraud detection which are having the greatest impact on the detection of major frauds.

Globally internal audit, fraud risk management techniques and data analytics – key components of corporate anti-fraud culture - are much more successful at detecting major frauds than in the Middle East. This highlights the real need for organisations in this region to focus on improving their internal anti-fraud controls.

## Focus on corporate culture - whistleblowing

Methods of fraud detection which rely on corporate culture in large part involve the readiness of the individual employee or counterparty to recognise and report questionable behaviour when they see it. Rather than relying on tip-offs management can provide a ready route for reporting through the establishment of an effective and accessible whistleblowing mechanism.

In our survey we asked respondents about the existence and effectiveness of whistleblowing mechanisms in their own organisations.

Despite the decline in whistleblowing as the method by which the major frauds in our respondent's organisations were detected, over 50% indicated that they had a whistleblowing hotline in place and 56% of those said that their mechanism was effective or very effective (global: 50%). Middle East respondents were therefore more positive about the effectiveness of whistleblowing than the global average.

In this region 56% of our respondents said that their whistleblowing hotline had been used in the past 24 months compared to 50% globally, with 8% indicating it had been used more than 50 times over that period.

This presents an interesting contrast: Middle East respondents report higher usage of whistleblowing than the global average and are more positive about its effectiveness in their businesses, yet the number of major frauds detected in this way is falling, and is lower than the global average.

**Figure 21: Organisations and whistleblower mechanism**

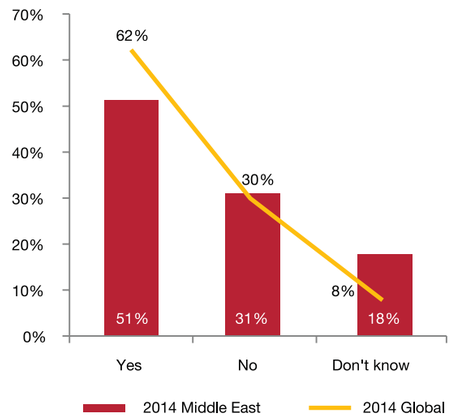
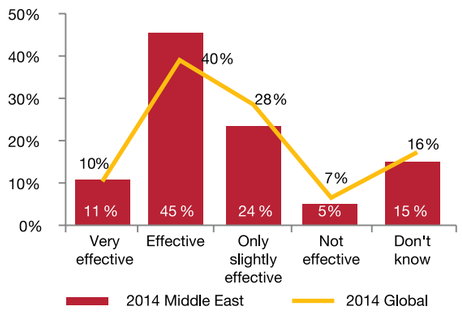



**Figure 22: Effectiveness of whistleblowing mechanisms**

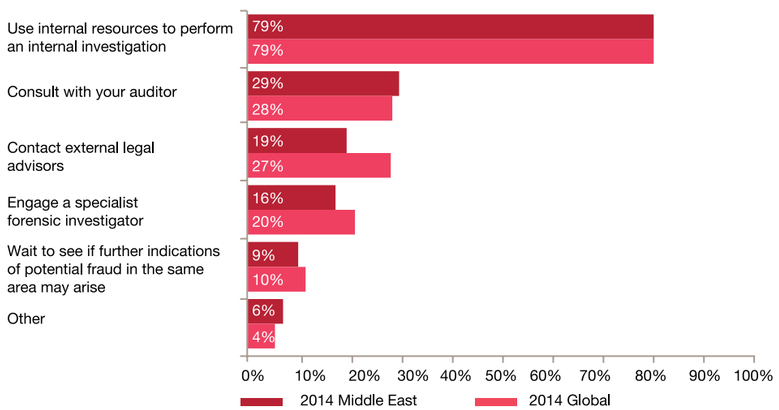



When a fraud is detected, what action are Middle East organisations most likely to take?

In this year's survey we asked our participants to outline their fraud responses where a potential fraud is identified. Almost four fifths of Middle East organisations said that they would use their internal resources to conduct an investigation, exactly in line with the global average.

Although 29% indicated that they would consult with their auditor, fewer respondents than the global average indicated that they would engage a specialist external party, either a specialist forensic investigator or their legal advisers, despite the benefits that a specialist resource might be able to provide.

**Figure 23: Actions taken when potential fraud is identified**





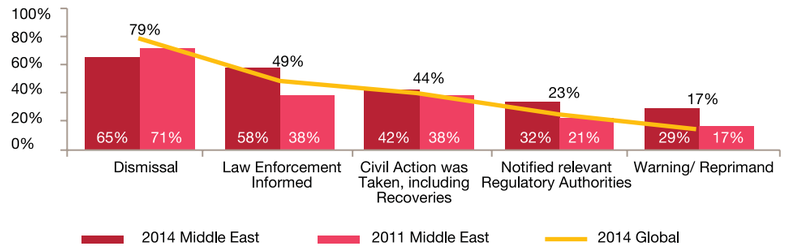

# Taking action

Taking decisive action against the perpetrators of economic crime helps to reinforce the message that fraud is not tolerated, and underlines a strong anti-fraud culture.

Our survey has assessed the action taken by Middle East organisations in response to economic crime. Consistent with our 2011 survey, where fraud has been detected the response has been decisive and aggressive whether the perpetrator is internal or external.

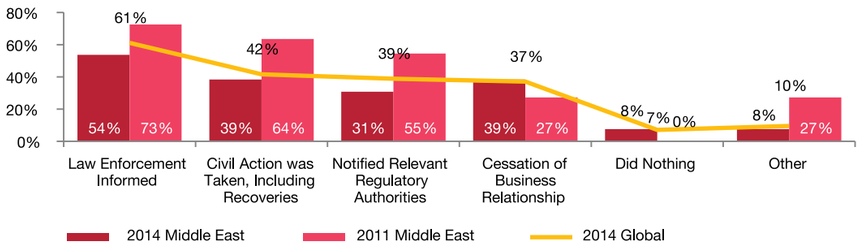
In response to incidents of ***internal*** fraud 65% of respondents indicated that they dismissed the perpetrators, 58% of the respondents notified law enforcement agencies and 42% took civil action.

**Figure 24 : Actions taken against internal perpetrator**




Our survey results show that external fraudsters represented approximately one quarter of all perpetrators of frauds detected. In these cases the majority of Middle East respondents informed law enforcement (54%), took civil action against the perpetrators (39%), ceased their business relationships (39%) and notified the relevant regulatory authorities (31%). Only 8% took no action at all.

**Figure 25: Actions taken against external perpetrator**



# *Methodology and acknowledgements*

## About the survey

We carried out our seventh Global Economic Crime Survey between August 2013 and February 2014. The survey had four sections:

- General profiling questions
- Comparative questions looking at what economic crime organisations had experienced
- Cybercrime fraud threats
- Corruption/bribery, money laundering and competition law/anti-trust law

Of the total number of respondents, 50% were senior executives in their respective organisations, 35% represented listed companies and 54% represented organisations with more than 1,000 employees.

The 2014 Global Economic Crime Survey: Middle East was completed by 232 respondents from nine countries in the region. Comparative indicators for respondents in the Middle East are provided below.

### Job titles of participants

| | % respondents |
|---|---|
| Manager | 34 |
| Chief Financial Officer/Treasurer/Controller | 21 |
| Head of Department | 13 |
| Chief Executive Officer/President/Managing Director | 9 |
| Senior Vice President/Vice President/Director | 7 |
| Other C-level Executive | 7 |
| Head of Business Unit | 4 |
| Board Member | 1 |
| Chief Security Officer | 1 |
| Don't know | 2 |

### Function (main responsibility) of participants in the organisations

| | % respondents |
|---|---|
| Finance | 32 |
| Audit | 16 |
| Executive management | 11 |
| Advisory/Consultancy | 11 |
| Compliance | 7 |
| Marketing and sales | 5 |
| Other (please specify) | 5 |
| Risk management | 4 |
| Information technology | 2 |
| Legal | 2 |
| Operations and production | 2 |
| Security | 1 |
| Customer service | 1 |
| Human resources | 1 |
| Research and development | 1 |

### Participating organisation types

| | % respondents |
|---|---|
| Private | 52 |
| Listed on a stock exchange | 25 |
| Government/state-owned enterprises | 16 |
| Others | 8 |

### Size of participating organisations

| | % respondents |
|---|---|
| More than 10,000 employees | 36 |
| 5,000 – 1,001 employees | 21 |
| 500 – 101 employees | 12 |
| 10,000 – 5,001 employees | 11 |
| 1,000 – 501 employees | 10 |
| Up to 100 employees | 8 |
| Don't know | 2 |

### Participating industry groups

| | % respondents |
|---|---|
| Financial services | 20 |
| Energy, utilities and mining | 12 |
| Professional services | 9 |
| Engineering and construction | 7 |
| Retail and consumer | 7 |
| Manufacturing | 6 |
| Technology | 5 |
| Insurance | 4 |
| Transportation and logistics | 4 |
| Communication | 4 |
| Other industries/business | 4 |
| Pharmaceuticals | 3 |
| Government / state-owned enterprises | 3 |
| Automotive | 2 |
| Chemicals | 2 |
| Entertainment and media | 2 |
| Hospitality and leisure | 2 |
| Aerospace and defence | 1 |



# *Terminology*

### Accounting fraud

Financial statements and/or other documents are altered or presented in such a way that they do not reflect the true value or financial activities of the organisation. This can involve accounting manipulations, fraudulent borrowings/raising of finance, fraudulent application for credit and unauthorised transactions/rogue trading.

### Asset misappropriation, including embezzlement/deception by employees

The theft of assets (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit.

### Bribery and corruption

The unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail. It can also refer to the acceptance of such inducements. Specific examples include kickbacks, extortion, gifts (with strings attached), facilitation payments, etc.

### Competition law/anti-trust law

Law that promotes or maintains market competition by regulating anti-competitive and unfair business practices conduct by organisations. Examples may include price fixing, excessive, predatory or discriminatory pricing, unfair trading terms, and tying (i.e., stipulating that a buyer wishing to purchase one product must also purchase all or some of his requirements for a second product).

### Cybercrime

Also known as computer crime is an economic offence committed using the computer and internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a byproduct in order to create the fraud and only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one.

### Economic crime

The intentional use of deceit to deprive another of money, property or a legal right.

### Espionage

Espionage is the act or practice of spying or of using spies to obtain secret information.

### Financial loss

When estimating financial losses due to fraud, the participants should include both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to "loss of business opportunity".

### Fraud risk assessment

Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to specifically consider:

1. The fraud risks to which operations are exposed;
2. An assessment of the most threatening risks (i.e., Evaluate risks for significance and likelihood of occurrence);
3. Identification and evaluation of the controls (if any) that are in place to mitigate the key risks;
4. Assessment of the general anti-fraud programmes and controls in an organisation; and
5. Actions to remedy any gaps in the controls.

### Human Resources fraud (recruitment and/or payroll fraud)

Fraud committed by members of the Human Resources department, including payroll fraud, ghost employees, pay-to-work, recruitment (i.e., hiring friends and/or relatives, hiring unqualified individuals, falsification of documents, etc.).

### Incentive/pressure to perform

The individual has some financial problem that he/she is unable to solve through legitimate means so he/she begins to consider committing an illegal act as a way to solve the problem. The financial problem can be professional (e.g., job is in jeopardy) or personal (e.g., personal debt).

### Insider trading

Insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, nonpublic information about the security. Insider trading violations may also include 'tipping' such information, securities trading by the person 'tipped', and securities trading by those who misappropriate such information.

### IP infringement (including trademarks, patents, counterfeit products and services)

This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing with off as genuine.

### Markets with a high level of corruption risk

While corruption risk levels can be subjective, for the purposes of this survey we suggest a territory with a Transparency International Corruption Perception Index ("CPI") score of 50 or less be considered a market with a high level of corruption risk. The link below the responses will direct you to the Transparency International list of territories and CPI scores.

### Money laundering

Actions intended to legitimise the proceeds of crime by disguising their true origin.

### Mortgage fraud

Mortgage fraud schemes employ some type of material misstatement, misrepresentation, or omission relating to a real estate transaction which is relied on by one or more parties to the transaction.

### Opportunity or ability

The individual finds some way that he/she can use (abuse) his/her position of trust to solve the financial problem with a low perceived risk of getting caught.

### Procurement fraud

Illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to his organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation.

### Rationalization

The individual finds a way to justify the crime to himself/herself in a way that makes it an acceptable or justifiable act.

### Tax fraud

An illegal practice where an organisation or corporation intentionally avoids paying its true tax liability.



# Contacts


### Forensic services partners

**John Wilkinson**
Middle East Fraud and Forensics Leader
Dubai, UAE
Email: john.d.wilkinson@ae.pwc.com

**Tania Fabiani**
Middle East Fraud Risk and Integrity Leader
Abu Dhabi, UAE
Email: tania.fabiani@ae.pwc.com

**Tareq Haddad**
Middle East Investigations Leader
Riyadh, Saudi Arabia
Email: tareq.haddad@ae.pwc.com

### Forensic services directors

**Achraf El Zaim**
Investigations, UAE
Email: achraf.elzaim@ae.pwc.com

**James Tebbs**
Head of Forensic Services, Qatar, Bahrain and Kuwait
Email: james.tebbs@qa.pwc.com

**Courtenay Smith**
Head of Corporate Intelligence, UAE
Email: courtenay.smith@ae.pwc.com

**Matthew Fritzsche**
Disputes, UAE
Email: matt.fritzsche@ae.pwc.com

**Dean Gilbert**
Head of Forensic Technology Services, UAE
Email: dean.gilbert@ae.pwc.com

### Editorial team

**Tareq Haddad**
Email: tareq.haddad@ae.pwc.com

**Anita D'Mello**
Email: anita.dmello@ae.pwc.com

**James Tebbs**
Email: james.tebbs@qa.pwc.com

**Tejasie Mendonca**
Email: tejasie.mendonca@ae.pwc.com


### Forensic Services

The PwC forensic services network is comprised of forensic accountants, economists, statisticians, former regulators and law enforcement, fraud examiners, and forensic technologists. We help organisations tackle the major financial and reputational risks associated with economic crime. We identify financial irregularities, analyse complex business issues, and mitigate the future risk of fraud.

***www.pwc.com/me***

To read our reports online scan the following QR codes on your smart phone or tablet.

***Global Economic Crime Survey 2014***

***Middle East Economic Crime Survey 2014***

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 184,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2014 PwC. All rights reserved. PwC refer to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.Please see www.pwc.com/structure for further details.

CDC/625/(2/2014)

*New Zealand insights from PwC's 2014 Global Economic Crime Survey*

# *Economic crime: What you don't know can hurt you*

**33%**
One third of New Zealand organisations report being victims of economic crime.

**40%**
Four in 10 New Zealand CEOs report being concerned by cyber threats, including the lack of data security.

**Five**
'Big fraud threats' most commonly affecting New Zealand organisations.

pwc

*pwc.co.nz/crimesurvey*

*#NZCrimeSurvey*

# Contents

# *Welcome to our New Zealand supplement to PwC's 2014 Global Economic Crime Survey.*

It will surprise few to learn that economic crime – such as fraud, corruption, cybercrime, IP infringement or accounting fraud – continues to be a major concern for New Zealand organisations of all sizes, across all regions and in virtually every sector.

Indeed, one third of New Zealand respondents to this year's survey reported their workplaces being victimised by economic crime in the past two years. It's an alarming finding and a reminder to all organisations to remain vigilant to the threats they face.

This is just one headline from the New Zealand supplement to our 2014 Global Economic Crime Survey: one of the broadest and most comprehensive economic crime surveys we have ever conducted, with 82 local respondents and over 5,000 global respondents contributing from every corner of the world.

But the real story is greater than economic crime persisting: it's also about economic crime threatening your business processes, eroding the integrity of your employees, and tarnishing your reputation. Which is why this year's report is focused on how and where it may be affecting you – so you can address the issue from both a preventive and a strategic perspective.

We thank all those who took the time to add their voice to this global study, in order to give us a better understanding of the fraud threats we face in New Zealand. Your contribution is invaluable.

Our report also focuses on enforcement activity; which touches on New Zealand's new anti-money laundering regime and high impact economic crimes, such as procurement fraud and cybercrime.

We hope our survey findings and analysis will serve your stakeholders well – including the Board, management, staff, suppliers, business partners and regulators – as both a useful reference point in an endless campaign and a strategic tool in your business arsenal in the year ahead.

Our senior forensics team of Stephen Drain, Campbell McKenzie and I would be pleased to discuss our findings with you personally, how they relate to your organisation, and what you can do to better protect your business.

Best regards,

***Eric Lucas***
Forensic Services Partner
PwC New Zealand

*Economic crime continues to be a major concern for New Zealand organisations.*

*One third of New Zealand respondents report their workplaces were victimised by economic crime.*

# *Economic crime: What you don't know can hurt you*

**Economic crimes fundamentally threaten the basic processes common to all businesses – paying and collecting, buying and selling, hiring and firing. Since close interaction with others is the foundation upon which virtually every business function is built, all organisations are exposed to various types of economic crime.**

**This is as true for New Zealand as it is anywhere in the world.**

While New Zealand business confidence is high and the economic outlook looks bright, we found fraud continues to hit New Zealand companies in the pocket – and while it can be hard to measure the cost of goods falling off the back of trucks, kickbacks, the theft of intellectual property and ideas – we know that financial costs are far from the only or most costly concern.

For the first time this year, we asked respondents about procurement fraud, reported by 19% of New Zealand organisations affected by economic crime. Procurement fraud is seen as a double threat, victimising businesses both in their acquisition of goods and services and in their efforts to compete for new opportunities.

With the Canterbury rebuild, increasing trade with emerging markets, rapid urbanisation - and our digital capabilities eliminating the tyranny of distance our businesses have faced for so long - new threats have arisen from fraudsters increasingly turning to innovative schemes and technology to assist their criminal activities.

These risks continue to evolve, and like a virus, economic crime adapts to the trends.

We must remain alert to the threats we face, particularly in this environment where we can expect investment activity to accelerate.

While the survey suggests New Zealand ranks lower for economic crime than many other countries, we must ask whether our organisations are adequately monitoring and aware of fraud and security breaches, or simply not reporting them.

For example, global respondents told us around a quarter have been a victim of cybercrime compared to New Zealand's 11%. Significantly, our respondents expect cybercrime to be double from current reported levels to 22%, over the next two years.

Furthermore, being a systemic problem, cybercrime's direct economic impact can be exceeded by the effect on employee morale, brand and reputation.

Pleasingly, the results of our Annual Global CEO Survey show New Zealand business leaders are beginning to take the threat of cybercrime seriously, with four in 10 worried about cyber threats and the lack of data security. Cyber worries are moving up the threat radar and on the minds of the c-suite.

With anti-money laundering legislation coming into effect in 2013, respondents also reported high awareness of the legislation (82%), and a similar number reported they were aware of the requirements to be fully compliant.

As trade with Asia increases, New Zealand businesses are increasingly exposed to countries which may have higher levels of corruption. There are significant risks for New Zealand entities in engaging in facilitation payments which seek to by-pass official processes or transparent contractual arrangements.

Encouragingly, the survey found 71% of New Zealand respondents have a whistleblowing mechanism, with 37% of crime detected through tip-offs. While corporate controls are responsible for detecting 56% of crimes.

# Economic crime in New Zealand

## What you need to know

Economic crime continues to be a major concern for organisations of all sizes, across all regions and in virtually every sector. One in three New Zealand organisations reports being hit by economic crime.

**33%**

***Financial losses are not the only concern: the true cost of fraud to reputation, employee morale and external relationships can be long lasting.***

## Most commonly reported types of economic crime

Five types of frauds are consistently reported – asset misappropriation, procurement fraud, bribery and corruption, human resources fraud and cybercrime.

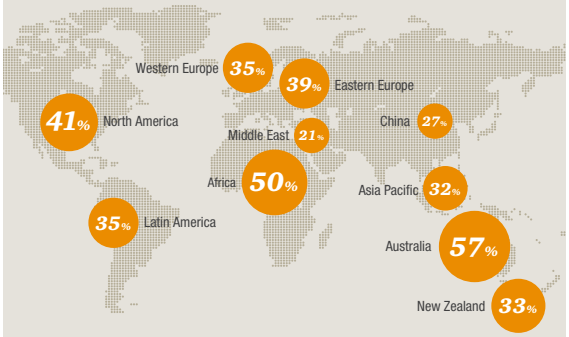

## The New Zealand c-suite gets the message

How ***concerned*** are you about the following potential business threats to your organisation?


New Zealand data from PwC's 17th Annual Global CEO Survey

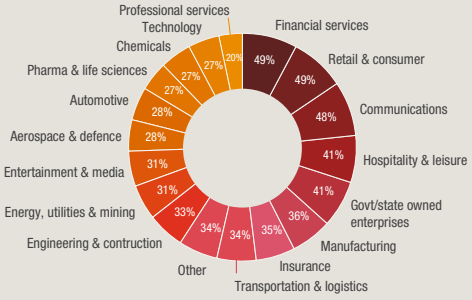
## Where does economic crime occur?

Economic crime is a pervasive global threat. The highest levels of economic crime are consistently reported by respondents in Africa (50%) and North America (41%).



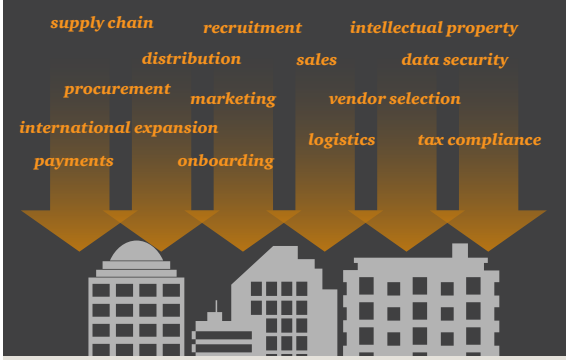

## Which industries are at risk? *A global outlook*

By industry, economic crime is most commonly reported in the financial services, retail and consumer, and communications sectors. Nearly 50% of respondents in each said they had been crime victims.



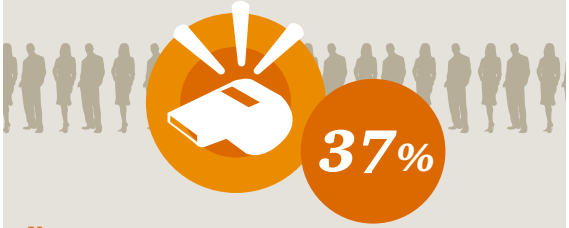

## Processes under threat

Economic crimes threaten the basic processes common to all businesses – paying and collecting, buying and selling, growing and expanding, sourcing and supply chain.




## To catch a thief

Tip-offs, including whistleblowing, detect 37% of economic crimes in New Zealand.




## Know your enemy

Businesses face threats from both internal and external sources and multiple angles. 70% of New Zealand organisations say the main fraud threat comes internally.

### Profile of a typical NZ internal fraudster

| | |
|---|---|
| Gender | male |
| Age | 31-40 years |
| Length of service | 5 years or less |
| Education level | High school level or less |

The internal threat has the greatest impact when senior managers are involved.

# What do the survey results tell us?

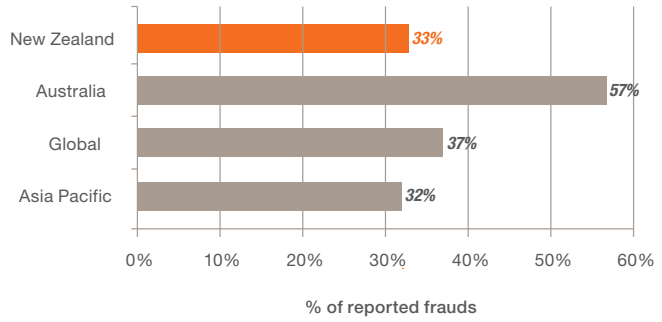
**Of the 82 New Zealand respondents, 33% have experienced some form of economic crime during the survey period.**

This ranks New Zealand 45th out of more than 95 countries that took part in the survey, and places us slightly below the global average of 37%, and significantly below our neighbours Australia (57%).

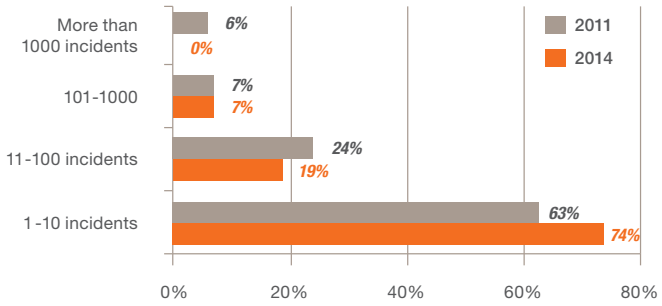
While the number of occurrences of economic crime appear to be decreasing in New Zealand, so too are the total number of incidents experienced. Over 74% of respondents said they had experienced less than 10 incidents over the survey period (2011: 63%). What's even more encouraging from a New Zealand perspective is that none of our respondents suffered more than 1,000 incidents (a decrease of 6.5% from 2011).

These findings are again consistent with New Zealand's image as one of the least corrupt countries in the world, and reflect Transparency International's 2013 Corruption Perception Index (where New Zealand again is perceived to have the lowest level of public sector corruption in the world).

## Percentage of organisations experiencing fraud




## Number of incidents of economic crime suffered by New Zealand organisations




New Zealand ranks

**45th**

out of more than 95 countries for reported incidents of fraud

# Types of fraud reported

**Consistent with last year's survey, our New Zealand findings show asset misappropriation is the most reported type of economic fraud (70%).**

## Types of fraud reported


Consistent with the global trend is an increase in the number of respondents suffering from incidents of bribery and corruption, with 15% of New Zealand respondents reporting their organisations have been a victim of this type of fraud. This is potentially linked to an increase in global awareness and is consistent with the findings from our 2014 Annual Global CEO Survey report, in which more than half of c-suite executives say they are concerned or extremely concerned by bribery and corruption.

Additionally, cybercrime continues to be an issue for New Zealand companies, with 11% of those who suffered some form of economic crime being the victims of a cybercrime. Also, it is highly likely that a number of respondents who have been victims of a cyber attack may not have an awareness of the crime. Unfortunately, far too often companies do not realise the true economic impact of a cyber attack until long after an incident has occurred.

Having included procurement fraud as a distinct category in this year's survey, it immediately registered as the second most reported type of fraud in New Zealand (19%). One likely reason, is the fact that New Zealand is in a period of growth due to the Canterbury rebuild following the earthquakes, and also has significant construction activity in Auckland, driven by immigration.

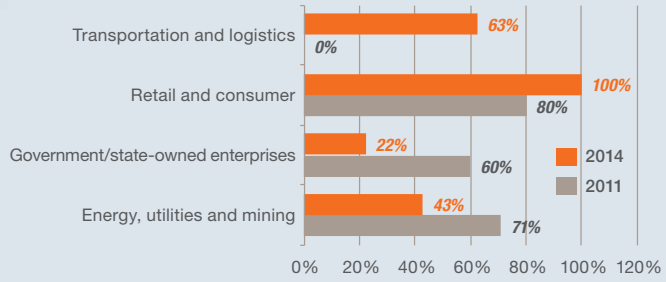
Globally, the high incidence of procurement fraud is likely driven by two distinct characteristics of today's economic environment. Firstly, business entities are becoming more interconnected, whether it be in outsourcing elements of the value chain, purchasing of materials or an increased reliance on suppliers: this is also consistent with the New Zealand findings of our 2014 Annual Global CEO Survey. Secondly, one of the effects from the recent global economic crisis is that companies have, and in some cases still are, replacing permanent in-house positions with more dispensable and scalable outside resources, with companies more willing to outsource non-core related tasks and in some instances even core tasks.

Interestingly, another distinct category that was added to this year's survey was HR fraud, which ranked joint third overall (15%) in terms of the types of fraud suffered. This is compared with a global ranking of sixth.

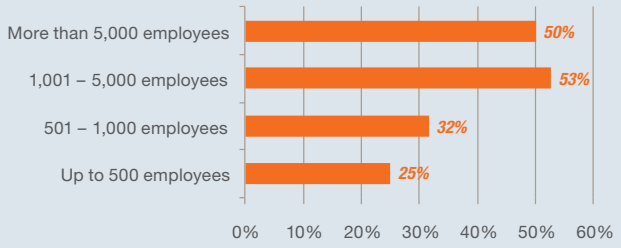
New Zealand respondents in 2014 reported 'other' economic crimes as insurance fraud, loan fraud and credit card fraud.

# Who is most affected?

### New Zealand industries experiencing economic crime




### Reported frauds based on organisation size in New Zealand



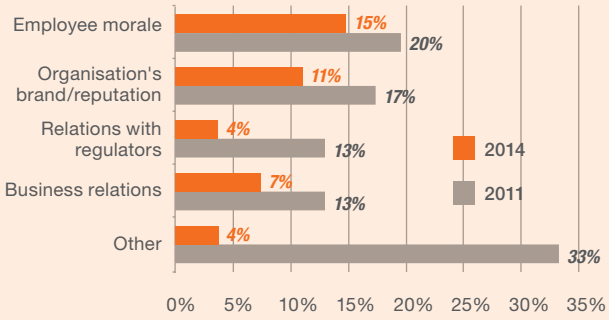

# Estimating the damage

Often, organisations do not fully appreciate the true financial impact of an economic crime until after it has occurred. Although in New Zealand, our survey findings indicate the financial impact of economic crime declined for this survey period, global trends indicate the impacts of economic crime continue to be an increasingly costly issue.

However, financial loss is not the only concern that companies face. We also asked New Zealand organisations about the 'collateral' damage to their business operations, including questions related to employee morale, brand/reputation, business relations and relationships with regulators.

Of those who had experienced fraud, 15% reported significant damage to employee morale (2011: 20%), 11% significant damage to reputation/brand (2011: 17%), 7% significant damage to business relations (2011: 13%) and 4% significant damage to relations with regulators (2011: 13%).

### Collateral damage associated with economic crime in New Zealand



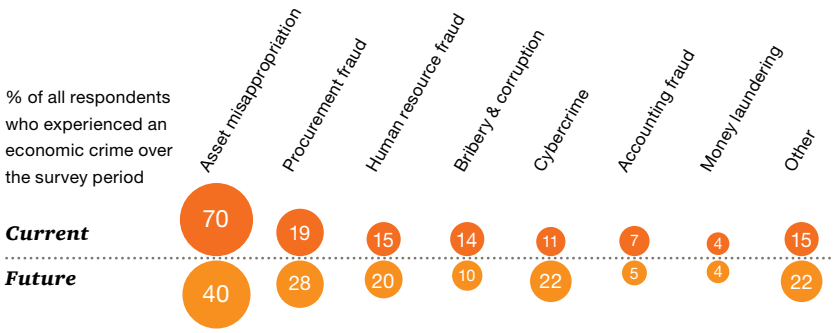

While the survey results may indicate that 'collateral' damage may be declining in New Zealand, it is imperative to remember the true cost of a fraud incident can be long lasting. While it's difficult to quantify these kinds of losses in strictly financial terms, one fact is crystal clear: if fraud affects hiring, retention, the ability to work with vendors, customers, and reputation, the impact will be felt all over the income statement – even if it isn't labelled as 'fraud'.

Fortunately, top management appear to understand this: more than four out of 10 New Zealand business leaders in our 2014 Annual Global CEO Survey see a 'lack of trust in business' as a key marketplace issue, with significant majorities recognising that business has a wider role to play in society than just building shareholder value (71%).

# Future predictions

**In addition to looking at economic crime suffered in the past, we also asked respondents to look forward and tell us which frauds they thought would pose the highest risks to their organisations over the next 24 months.**

## Types of fraud predicted in New Zealand over the next 24 months




Our findings show that New Zealand companies are predicting occurrences of economic crime, as well as the total number of reported incidents, to persist over the next 24 months. Yet, there is a strongly predicted shift in the types of economic crime expected to impact organisations.

We can see New Zealand companies remain very cautious and predict they will experience more economic crime in areas such as procurement fraud and cybercrime.

We also note that occurrences of bribery and corruption are predicted to drop back, close to 2011 levels, while asset misappropriation is also predicted to drop from the 70% reported this year to approximately 40% over the next 24 months.

# *Under the eye of enforcement*

## Long reaching effects

**Some types of economic crimes attract significantly more attention from government enforcement agencies than others. These types of economic crimes – i.e. money laundering, bribery and corruption and anti-competitive behaviour – arise from the failure of businesses to adhere to the expected code of business conduct established by countries around the world.**

Each of these crimes are subject to government enforcement by the relevant authorities and are subject to increasingly stringent standards, enforcement and harsh penalties. In an interconnected world, these types of economic crimes pose unique threats to organisations.

Violations of government legislation, such as the recent Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act), can lead to substantial fines and have long lasting reputational effects for organisations.

Moreover, such violations may be indicative of larger organisational issues, such as weak internal controls or a lack of an appropriate tone at the top. This in turn can have a substantive knock-on effect for organisations, including reputational harm and financial loss, as well as issues related to talent retention and costly disruptions to business plans.

In fact, the findings from our survey indicate that across all three government enforcement-related frauds, respondents cited reputational risk as having the greatest impact on their business operations by a significant margin.

### *Money laundering: A special concern for financial services*

Financial services companies report significant risk from an entirely different fraud than most other industries – money laundering. Money laundering represents a risk to financial institutions if they fail to have appropriate systems to deter, detect and report it.

Defined in our survey as actions intended to legitimise the proceeds of crime by disguising their true origin, the crime of money laundering exposes financial institutions in two ways:

1. Through access to laundered money provided to potential criminals.
2. Through the banking functions (e.g. bank accounts, loans, etc.) which fraudsters use to disguise funds.

### *What is the AML/CFT Act?*

The AML/CFT Act was implemented as part of New Zealand's requirements to meet its international obligations. The Financial Action Task Force (FATF), an international body of which New Zealand is a member, has a requirement to have appropriate legislation in place to minimise the risk of money laundering. The legislation helps to reduce criminal activity in New Zealand by ensuring the illegitimate proceeds of such crimes are not put through the financial system (e.g. deposited to a bank account, etc) to disguise the true nature of these funds.

Under the Act, reporting entities (primarily financial organisations) have certain obligations. These obligations include the appointment of an AML compliance officer, undertaking a risk assessment, and based on the results of the risk assessment, developing a programme to comply with the requirements of the Act. Reporting entities also need to have their programme audited every two years to ensure continued compliance.

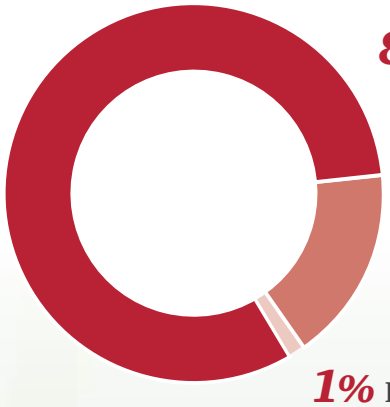
At its core, reporting entities will need relevant policies, processes and controls related to customer due diligence and account monitoring. This means financial institutions will need to ensure they have the appropriate rigour when it comes to their on-boarding process, specifically in relation to the identification and verification of new customers or if facilitating an 'occasional (one off) transaction'.

Under the Act, reporting entities are also required to have appropriate systems in place for reporting suspicious transactions to the New Zealand Police Financial Intelligence Unit (FIU).

# *Are New Zealand companies aware of their obligations?*

**In our survey, we asked respondents if they were aware that new anti-money laundering legislation had been enacted in New Zealand. Eighty-two percent of New Zealand respondents reported they were aware of the new legislation, and 81% also reported they were aware of their requirement to be fully compliant by 30 June 2013.**

Respondents' awareness of the AML/CFT Act enactment



**82%** Aware

**17%** Unaware

**1%** Don't know

Penalties for non-compliance can be severe and a corporate body can incur a fine of up to $5 million, as well as suffering substantial reputational damage in the market. For individuals, penalties can include imprisonment of up to two years and a fine of up to $300,000.

Consider the difficulty faced by an international financial institution managing its operations in a variety of cultural and legal environments, yet subject to the stringent legal standards of a developed Western economy. For example, it must train tellers how to identify and report what might be 'suspicious transactions' – because of their amount, currency, the frequency of deposit, identity of the depositor, or unexplained nature of the business.

The institution may be operating within a culture known for violence or intimidation towards uncooperative individuals, for deference to the demands of the wealthy, or one in which corruption is commonplace. It could be operating in an environment where the relatively large difference between the economic circumstances of customers, relative to bank employees, allows for gifts or threats to pave the way for inappropriate use of its facilities by those charged with conducting transactions, approving transactions or reporting issues.

## Sophisticated threats

Recently, a new form of money laundering threat has developed: alternative payment networks using 'virtual' currencies (e.g. Bitcoin). While the transactions on these sites may be 'virtual', they are backed by actual deposits in financial institutions around the world. Identifying such tainted funds is yet another challenge to bank compliance and operating systems.

So, operating in environments that pose a systemic threat of money laundering to the business processes of financial institutions is a unique challenge. Not only are money laundering schemes numerous and sophisticated, but they create a potentially significant tension between the equally laudable goals of acquiring and serving profitable customers and operating a wholly compliant institution across multiple jurisdictions.

## Bribery and corruption: Are the c-suite getting the message?

While it is not the most common form of crime reported, of all the types of fraud covered in our survey, bribery and corruption may pose the greatest threat to businesses because of the number of business processes it threatens. Sales, marketing, distribution, payments, international expansion, expense reimbursement, tax compliance, and facilities operations are all vulnerable processes.

While New Zealand consistently ranks among the least corrupt nations in the world, our survey results indicate the number of reported occurrences of bribery and corruption is increasing. This year's results show that of the New Zealand respondents who have reported an economic crime, 15% have experienced bribery and corruption during the survey period (11%: 2011). This compares to a global average of 27% and is broadly in-line with the global trend, where occurrences of bribery and corruption have increased by 3% on average.

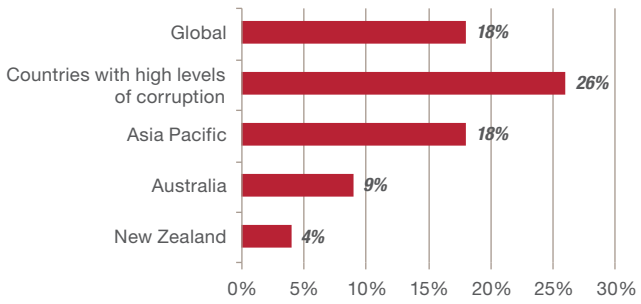
When such a crime threatens a company in so many ways, it deserves CEO attention. The findings from our 2014 Annual Global CEO survey show that over half of global CEOs now are either somewhat concerned or very concerned with the risks associated with bribery and corruption.

In New Zealand, the results are somewhat different; only 15% of our New Zealand CEOs indicated that risks associated with bribery and corruption are concerns for their organisations.

This is potentially linked to New Zealand's already good reputation for transparency and honesty. However, as the findings from our economic crime survey indicate, New Zealand CEOs should be more cognisant when it comes to considering the risks associated with this type of economic crime. Not only are the number of reported occurrences increasing, but of the three economic crimes falling under government enforcement, almost half of our survey respondents (49%) perceived bribery and corruption as having the most severe impact on their corporate reputation.

From a New Zealand perspective, 4% of those surveyed indicated they had been asked to pay a bribe over the survey period, while 4% also indicated they had lost an opportunity to a competitor which they believe had paid a bribe. While this compares very favourably to a global average of 18%, it is clear to see that New Zealand as a country is not immune from the threats associated with bribery and corruption.

**Percentage of respondents asked to pay a bribe**



# The corporate smuggler

The 'Grey Channel' is a system by which exporters send produce into China, avoiding a range of issues that may otherwise apply, including timing difficulties, health requirements, taxes and export quotas or other limits.

The arrangements appear to be reasonably common practice. The Grey Channel allows goods to reach Hong Kong, with a Chinese or Hong Kong trader taking responsibility for the final export to mainland China, often having re-characterised the nature of the goods (e.g. claiming they were sourced from somewhere other than their actual country of origin).

There seems little doubt that facilitation payments are made to officials in either or both Hong Kong and China, and such payments are most likely illegal.

Despite its apparent common use, the Grey Channel and other similar structures are illegal and the authorities in China and other countries have and will take enforcement action against companies that participate.

# Combating bribery and corruption

**The Crimes Act 1961 covers offences related to corruption of the Judiciary, Ministers of the Crown, Members of Parliament, law enforcement officers, public officials and the corrupt use of official information. Under the Act, it is an offence to corruptly accept or obtain a bribe for something done (or not done) in an official capacity. Penalties can include terms of imprisonment of up to 14 years.**

The Secret Commissions Act 1910 covers bribery and corruption-style offences, which are relevant to the private sector. Penalties can range from a fine of up to $2,000 or imprisonment of up to two years.

There are also other New Zealand laws which broadly assist the investigation of corruption (the Serious Fraud Office Act 1990) and for the taking of civil sanctions (the Securities Market Act 1978) relating to insider trading and market manipulation.

In addition, New Zealand has also signed the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, as well as the UN Convention against Corruption. Both of these conventions require member countries, such as New Zealand, to implement strong measures to combat bribery and corruption.

## Sales and marketing under threat

While the risk of bribery and corruption is a threat to many different types of transactions, it is of particular concern when companies are dealing with government agencies and state-owned businesses – and, consequently, with government officials.

For example: A pharmaceutical organisation would like to sell a recently developed medicine to a country that operates a public healthcare programme. The permission to sell the medicine, the decision to buy it and the price paid will likely be in the hands of government officials.

Or, an equipment company would like to sell their product to a state-owned enterprise whose senior executives are members of the political party currently in office. The specifications in the tender documents, the budget available for the acquisition, the ancillary support services needed for training, spare parts, and maintenance, the evaluation of the bid proposals – all will likely be decided by government officials.

If the territory has a culture that is relatively permissive to bribery and corruption, some of these officials may be predisposed to expect or at least be open to bribes. This exerts pressure on sales and marketing staff, who have been tasked by leadership with bringing a new product to a growing market – pressure which could be felt by individual staff as justifiably offering a bribe or kickbacks, or otherwise rigging the sales process to try and secure a better price.

While the profit potential will likely be obvious to the sales and marketing team, the systemic risk of operating in a culture with a 'high demand' component of the corruption equation may be less so. As we have often seen, the US Foreign Corrupt Practices Act (FCPA) and other enforcement tools frequently have far-reaching financial and organisational impacts. These can include altering your sales processes, sales incentives, distribution networks, authority levels and approval requirements for marketing activities and other payments, choice of agents and brokers, and in extreme cases, the ability to operate at all in certain countries.

# Competition and anti-trust law

**None of our New Zealand respondents reported suffering issues in the competition and anti-trust law sector.**

However, the New Zealand Productivity Commission has recently called to have competition law in this country strengthened. The commission argues there are some service sectors that lack intensity of competition which can drive efficiency and productivity gains in the sector. It says the current legislation is flawed and a strengthening of the law is required, specifically in relation to section 36 of the Commerce Act, which deals with the abuse of market power.

Our survey results very much reflect a European focus. The economic profiles of these territories, combined with EU competition laws, appear to be driving a high perception of risk in the region. Of the three economic crimes under the eye of government enforcement mechanisms (bribery and corruption, competition law, and money laundering), competition law was cited as a higher risk by one in four respondents in both Western Europe and Eastern Europe – with Asia Pacific, Africa, and both American continents showing less concern.

It appears that the EU Commission, which has been increasingly aggressive in pursuing high-profile actions against cartel, price-fixing and other forms of market abuse – including in the recent, highly publicised LIBOR affair – is having a definitive impact on the concerns and operations of EU-based companies.

# High impact economic crimes

## Procurement fraud: A growing opportunity, a growing threat

**Procurement fraud, defined for the purposes of our survey as 'illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to his organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation' – was added as a distinct category to this year's survey.**

**Generally, when an organisation goes into a commercial or public tender process or seeks to acquire goods and services for its own use – a common process across all industries – the potential for procurement fraud exists.**

**19%**

**of New Zealand respondents who experienced economic crime reported occurrences of procurement fraud.**

**2nd**

**most reported fraud – after asset misappropriation.**

**28%**

**of New Zealand respondents believe they are likely to encounter procurement fraud over the next 24 months.**

We anticipate that the significant response in this category is driven by the fact that New Zealand is in a period of growth due to the property rebuild in Canterbury and the significant housing construction activity in Auckland.

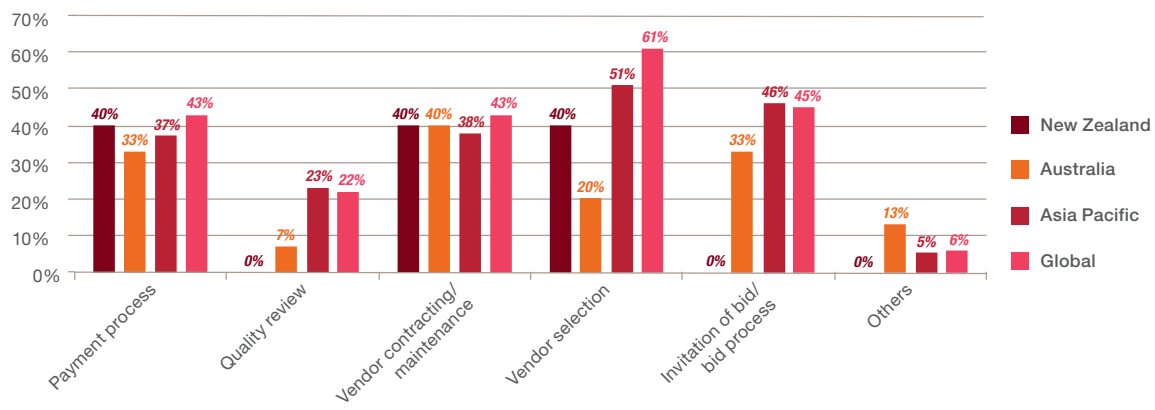
In addition, there has been an increase in more competitive public tender processes from governments and state-owned businesses, unleashing the possibility of fraudulent activity on the part of agents and other third parties. No doubt, in past surveys, procurement-related kickbacks, bid-rigging, or similar activities were reported as corruption. But with our new inquiry into where in the process procurement fraud primarily occurred, the connection has become clearer. Of the New Zealand respondents, 40% said procurement fraud had occurred during vendor selection, in the payment process and during vendor contracting / maintenance.

Moreover, our recently launched 2014 Global CEO Survey highlights a significant majority of businesses are focusing on making changes to their supply chain in response to global trends. Many are seeking deeper interconnections across their value chain, and using a more global supply model. And as suppliers become more integrated into companies' operations, the threat of significant disruption and monetary loss increases.

In addition, as economies have emerged from the recent economic crisis, a shift in employment practices seems to have occurred. Short-term, post-crisis measures, such as replacing permanent, in-house positions with more dispensable and scalable outside resources, have persisted with companies more willing to outsource tasks once part of their non-core and core operations.

Based on these responses, we see procurement fraud as a double threat. It victimises businesses in their own acquisition of goods and services. And it prevents companies from competing fairly and successfully for business opportunities subject to a commercial or public tender process.

### Procurement fraud occurence by stage



# Procurement fraud by industry

**In New Zealand, the industries that reported the most procurement fraud were core government and state owned industries (43%), engineering and construction (4%) and transport and logistics (4%). These sectors are heavily reliant on large outside suppliers and therefore the likelihood of procurement fraud is heightened.**

## Threats to the purchasing process

While our discussion has focused on external parties, it is important not to overlook the threat from within. In our experience, the requisitioning of goods is an area ripe for fraud. The threat is especially great in cultures where loyalty to family, friends, local community, or even national pride are strong influences – stronger perhaps than dry corporate policy statements or legalistic-sounding codes of conduct.

An individual within the purchasing and supply department may have a pre-existing relationship with a vendor who wants to win business from the organisation. The insider provides information on the bidding process, such as the bid amounts of competitors, to ensure an advantage for their preferred bidder. Or, the insider could approve a price higher than necessary.

Alternately, your controls may not function as planned. We have observed countless incidences of employees in approval roles acquiescing to pressure from 'the boss' to process payments that do not meet all aspects of policy and procedure. This tension between an executive's loyalty to the company versus their connectivity to the local milieu is a real and continuing threat to controls.

***In our experience, the requisitioning of goods is an area ripe for fraud.***

# Asset misappropriation

**Asset misappropriation, more commonly known as theft, is by far the most common economic crime experienced by organisations reporting fraud, with 70% of respondents suffering from it. This amount is more than three times the second highest occurring type of economic crime, procurement fraud (19%). While the individual impact of this fraud may be lower than that of cybercrime or government-enforced frauds, subject to specific enforcement regimes, the magnitude of the threat requires organisations to be vigilant.**

## (Not) falling off the back of a truck

This euphemism for asset misappropriation points to one of the fundamental business processes it attacks – distribution, logistics and warehousing.

For example, take a global operating retail company with warehouses of inventory. Not only are these products exposed to the organisation's own employees, they also constantly pass through the hands of third parties, leading to several points of vulnerability in the supply chain and distribution process. Schemes can be as simple as employees stealing inventory or more complicated endeavours, such as covering up a theft by marking good inventory as 'scrap', removing it from the premises, and then reselling it.

Another function which is commonly threatened by asset misappropriation is the expense reporting process – which further impacts on the cash disbursement function and potentially leading to collateral impacts, such as inaccurate books and records. Further, disbursements to employees which are illegitimate affect cash on hand and increase expenses.

## Are you protecting what matters most?

Intellectual property (IP) infringement and theft is often an especially damaging economic crime – and one that is very much on the mind of New Zealand CEOs, 31% of whom reported they are worried about being able to protect it, according to our Annual Global CEO Survey.

In our cybercrime section, we noted that organisations should focus their cyber security on protecting these crown jewels, rather than on just their network. In certain industries, intellectual property is the key asset that allows the company to win in the marketplace. Thirteen percent of New Zealand respondents indicated they expect to be threatened by this economic crime in the next 24 months, compared with none who actually reported occurrences in the survey period.

The gap between expectations and experience is a consistent theme in the area, and we believe it demonstrates another concept: successful crimes which target assets often go undetected or unreported. Our respondents appear to be aware that their IP is at risk, but their controls may not be detecting the actual attacks.

## *Accounting fraud: The connected threat*

Accounting fraud has always been one of the major crimes reported in our survey, and since 2005, has been cited by over 20% of our global respondents that experienced economic crime. This year was no exception with a global response rate of 22%. The picture is somewhat different in New Zealand, as only 7% of New Zealand respondents who had suffered economic crime report occurrences of accounting fraud.

# *Cybercrime: The risks of a networked world*

**The advancement of technology in business services, combined with the explosive growth in social media and data connectivity, has permanently altered, and in many ways, brought together the business and consumer landscapes.**

Unfortunately, connectivity and access also have a dark side – one which empowers motivated, sophisticated criminals who are able to operate below the radar. And because cybercrime operates largely unseen, organisations may never realise they are being targeted until long after the damage is done.

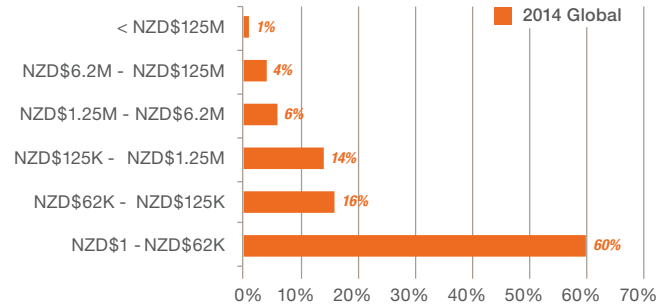
This fact alone makes the many varieties of electronic fraud one of the most threatening types of economic crime.

Our 2011 Global Economic Crime Survey was the first in our series to highlight cybercrime as a high-level threat to organisations. This year's survey confirms the significant, continuing impact of this crime on business, with now one in four global respondents reporting they have experienced a cybercrime – and over 11% of these suffering financial losses of more than US$1 million.

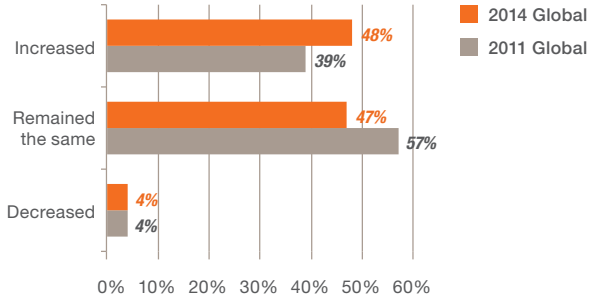
In a sign that organisations are taking this threat more seriously, our survey indicates that the perception of the risk of cybercrime is increasing at a faster pace than that of reported actual occurrences. This year, 48% of our global respondents said their perception of cybercrime risk at their organisation increased, up from 39% in 2011.

Reinforcing this, 40% of New Zealand CEOs in our latest Annual Global CEO Survey said they were concerned about cyber threats, including the lack of data security.

## Relative impact of cybercrime on organisations




## Perception of cybercrime




***40% of New Zealand CEOs in our latest Annual Global CEO Survey said they were concerned about cyber-threats, including the lack of data security.***

## What you don't know can hurt you

While one quarter of respondents reporting they have suffered a cybercrime is concerning enough, we must also consider that a significant percentage of those who did not report cybercrime may also have suffered an event – and not even know about it.

This underscores the challenge of the threat. Many entities do not have clear insight into whether their networks and the data contained therein have been breached, and they don't know what has been lost – or its value.

Further complicating the picture is a third aspect of the lack of transparency into cybercrime events: even when it is detected, cybercrime often goes unreported. Outside of privacy breaches in regulated areas such as 'identity theft', there are few regulatory conventions requiring disclosure. And often – such as in the case of theft of key intellectual property – there may be compelling competitive reasons for organisations to keep such losses confidential.

For example, if a confidential bid planning document were accessed by cyber criminals and utilised by rivals to gain an advantage, would a company disclose the incident? Are organisations adequately defending against such cybercrime breaches, and if they were discovered, how would they value the loss?

The bottom line is that much of the damage caused by these kinds of attacks is not disclosed, either because it is not known, because it is difficult to quantify, or because it is not shared.

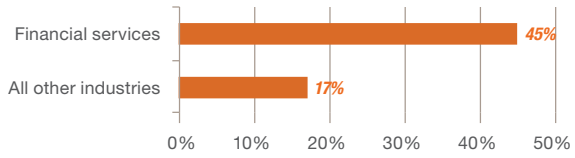
## Focus on financial services

Forty-five percent of global financial services organisations affected by fraud reported being victims of cybercrime – nearly twice the frequency as reported by all other industry sectors.

Why such a large percentage? Large, regulated financial institutions often have more and better system safeguards – which may increase the chance of a breach being detected. In addition, banks are where the money is.

Finally, financial institutions are an appealing target because they provide large amounts of customer and personal financial information online, which can potentially be accessed – and sold on the black market – as a precursor to organising a theft of funds.

Cybercrime impacting financial services



# A moving target

**In a changing technological landscape, the sophisticated adversary takes advantage by attacking new weaknesses. This is why it is essential for organisations to at least try to keep pace with the criminals who threaten them.**

Even when organisations are generally aware of the types of cyber threats they face, many do not truly understand the capabilities of cyber criminals, what they might target, and what the value of those targets might be. Yet, companies continue to make their critical data available to management, employees, vendors, and clients on a multitude of platforms – including high-risk platforms such as mobile devices and the cloud – because the economic and competitive benefits appear so compelling.

The uptake of 'cloud services' is also driving behavioural change, both at business and consumer levels. The 'digital disruption' of what were bricks and mortar businesses are forcing organisations to move quickly to embrace new sales channels, leveraging cloud services to do so. This introduces a more complex technology and business relationship which is proving to be a fertile ground for potential cyber criminals to exploit.

'Spear phishing' attacks, historically focused on financial institutions, are now being seen targeting retail consumers via social media. This connectivity, and simple fact that humans will normally use the same credentials for multiple systems, means a simple compromise of one set of access credentials could easily unlock a person's complete identity. A recent extension of this is the latest ransomware outbreaks, where a user's complete computer is encrypted and a ransom has to be paid to release the decryption key. While in the true sense this is not a new phenomenon – the scale, complexity and sheer brashness of these attacks on the public are unprecedented.

While nobody expects the benefits of technology to diminish, or for organisations to shrink their digital footprint, it's clear that – with more data accessible on more platforms – valuable data will remain under attack, and the cost of security breaches will continue to be steep. In fact, in every region, between a quarter and a third of organisations told us they believe they will likely encounter cybercrime in the near future.

# *Cybercrime is a strategic problem*

**Ultimately, cybercrime is not just a technology problem. It is a strategy problem, a human problem and a process problem.**

After all, organisations are not being attacked by computers, but by people attempting to exploit human frailty, as much as technical vulnerability. As such, this is a problem which requires a response that is grounded in strategy and judgement about business process, access, authority, delegation, supervision and awareness – not merely tools and technologies.

This is illustrated in at least four ways. First, knowing that people are often the weakest link in the security chain, hackers often exploit human naiveté through attacks such as 'spear phishing' – a targeted email approach supposedly sent from a source that you trust, such as your bank – to take advantage of the inattentive. Alternatively, hackers can try to break data encryption codes through the brute computing power of modern machines, or they can guess at, steal, or bribe their way to possession of an easy password.

Second, hackers 'productivity' improves not only through the use of new technology, but also through the better-organised use of people in the 'mule' capacity.

Third, cyber security solutions often require non-technical processes and tools – for example, training and awareness, and the involvement of legal and privacy experts for response, media relations, crisis management and remediation solutions in the wake of uncovering a cybercrime.

Finally, good security requires people to remain focused on their most important data. Companies that prioritise the data on their networks are able to focus on the 'crown jewels' – and spend their limited cyber security budgets wisely.

Thus, one of the key organising principles of cyber security is not a technical question for the IT staff at all. It is a business question for senior managers. Yes, your IT team has to know what the best tools and technologies are for your business, but know that will do little good if you are focused on protecting the wrong assets.

# Cybercrime threatens technology-enabled business processes

***The growing use of technology-enabled business processes makes cybercrime a very real threat to a wide variety of business operations. In our recent experience, the systems most threatened are those that contain data directly leading to financial assets that can be stolen or personal data that can be used to assemble an attack on financial assets. Technology-enabled business processes that are threatened by cybercrime include:***

- ***Point of sale purchases*** by debit and credit cards in the everyday retail environment.
- ***ATM transactions*** in the everyday banking environment.
- Preserving or respecting the ***privacy of customers.*** This is especially true in the health care industry where providers often maintain systems with considerable amounts of sensitive patient information, including identity, financial circumstances, insurance plans, and medical conditions.
- ***E-commerce or on-line sales processes.*** Same issues as penetration of point of sales systems in the retail store or banking environment, except that it is in the on-line environment.
- ***Electronic business communications (email).*** External cyber criminals can penetrate corporate communications systems and steal critical commercial information, intellectual property, and sensitive executive communications.
- Taking advantage of ***infrastructure weak points*** to accomplish any of the above – for example, penetrating Wi-Fi access points or intercepting other people's communications through them; attacking business operating systems using 'cloud' architecture by penetrating the server environment maintained by the cloud provider.
- ***Consumer incentives.*** Loyalty and other consumer incentive programmes that retain customer data and spending habits/preferences offer a treasure trove of data that can be used for identity theft and targeting for additional cybercrime.
- ***M&A.*** After the completion of a merger or acquisition, the company will often delay full integration of information security policies, processes and tools. This leaves vulnerabilities in a corporate IT environment which hackers can exploit – for example, by gaining access to databases from legacy enterprises that contain valuable intellectual property or other types of sensitive data.
- ***Supply chain.*** Suppliers, contractors and distributors are part of a company's ecosystem – often with authorised staff-like access to sensitive data and systems. Their risk is your risk, and a breach in the supply chain can have cascading effects on network security, or worse, allow direct access to sensitive data.
- ***Research, development and engineering.*** Proprietary technology, trade secrets, and intellectual property are targeted by nation-states, state-owned enterprises, and unethical corporations. Businesses have lost billions of US dollars in this way through theft by hackers and insiders of intellectual property to the benefit of competing organisations.
- ***Expansion into new markets.*** As a company moves into a new geographical market, it can become the target of the host government or local competitors who want to steal its technology, client lists or marketing plans. As the company is literally on another's 'home turf', the insider problem extends beyond employees, to facility providers, talent search firms, janitorial services, even local government agencies.

# *Identifying the fraudster*

## Know your enemy

Trying to profile a typical fraudster is difficult, but gathering as much information as possible on these individuals is important. Profiling can help to identify weaknesses in existing control environments, and as a result, allows for more targeted controls to be identified and implemented.

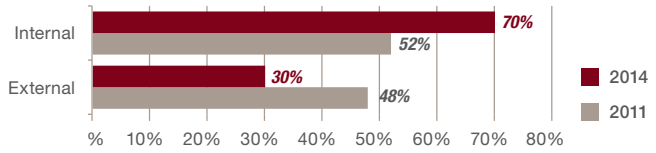
We asked respondents whose organisations had experienced economic crime, to profile the main perpetrators of the most serious frauds they had suffered. The results were interesting and very different to previous years. In 2014, 70% of New Zealand respondents reported that the main perpetrator of fraud was an internal party, whereas 30% reported the main perpetrator as being an external party. In 2011, the results were evenly split.

However, the one thing that remains constant among New Zealand respondents is the fact organisations in the financial services and retail sectors suffer far more fraud attacks from outside their organisations. This trend is potentially linked to the disproportionately high rate of cybercrime affecting financial services and the fact that cybercrime tends to involve perpetrators from outside an organisation.

On the other hand, New Zealand respondents in transport and logistics, as well as the government sector, reported all their occurrences of fraud came from internal perpetrators.

The silver lining of having most of one's fraud losses attributable to internal players – people you have some visibility over – is that there is good potential to mitigate the risks through improved internal policies, processes and controls. As we will see, this is more challenging with external fraudsters.

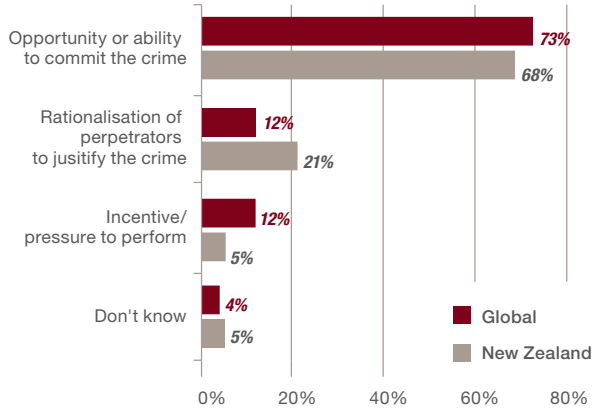
**Internal vs external fraudsters**




## What increases the likelihood of fraud?

**Anti-fraud practitioners commonly refer to a 'fraud triangle' – the three elements that are often present when a perpetrator commits fraud: pressure, opportunity and rationalisation.**


### Why does fraud occur in New Zealand?




This year we asked respondents what factor they felt had contributed the most to economic crime committed by internal parties. Almost 70% of New Zealand respondents indicated that the opportunity or ability to commit the crime was the factor that most contributed to economic crime, which is broadly in line with the global average of 73%.

While this news may at first seem anti-climactic, it's important to keep in mind that, of the three factors, opportunity is the one most in an organisation's control. The implication is that while life's pressures and the ability to rationalise may swirl around employees, if an organisation can limit the opportunity, they can do much to stop the fraud before it starts.

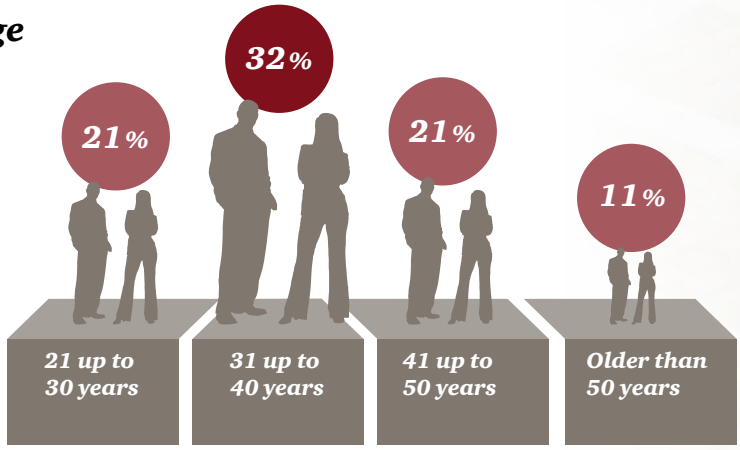
While we cannot plot the specific pressure or rationalisation behind each internal act of fraud, we can at least profile the fraudster. We asked respondents who had pointed to an internal party as the main perpetrator of economic crime to profile the fraudsters age, gender, length of service, and education level.

Our results indicate that the overall profile of the internal fraudster in New Zealand generally remained the same as in 2011 – middle-aged males, educated only to high school level or less, who have been with the organisation for five years or less.

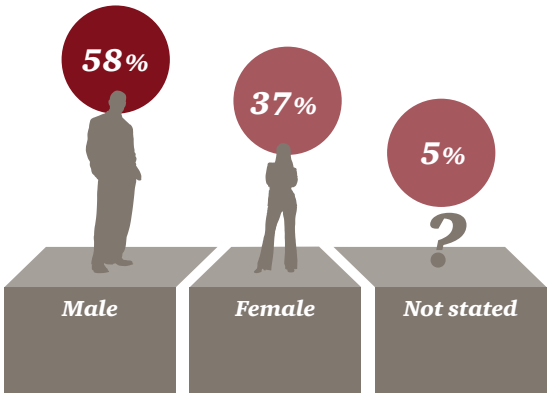
Globally, we did note some differences in certain regions and industries. For example, the percentage of senior management committing internal fraud in the Middle East was 25% higher than the global average, while in Latin America the percentage of junior staff committing internal fraud was 13% higher than the global average.

# New Zealand's typical internal fraudster

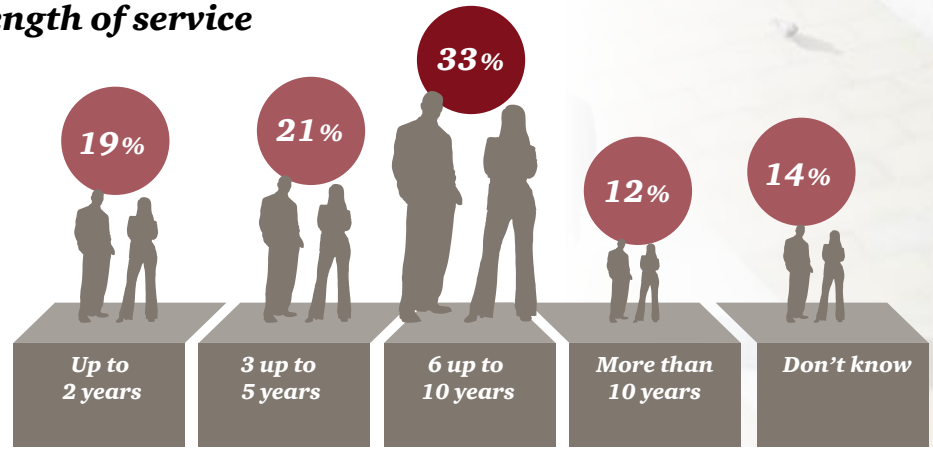
## Age




## Gender




## Length of service

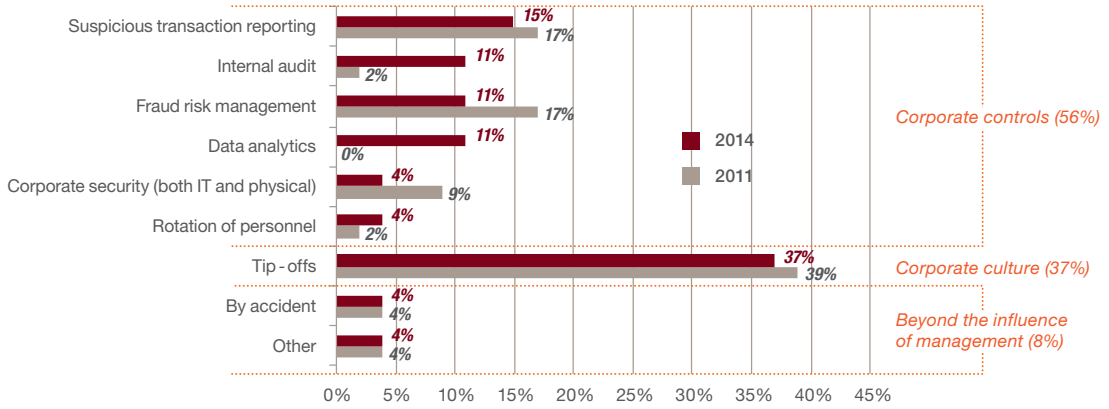


# To catch a thief

**Fraud is detected by various corporate controls, tip-offs and events beyond the influence of management.**

The below graph shows the methods by which major fraud was detected by organisations across New Zealand, over the last 24 months.

## Detection methods




Note: Data analytics was only added as a category in 2014.

The graph highlights the significance of a tip-off and avenues for tip-offs as the most effective method of fraud detection.

Our results indicate that 71% of New Zealand respondents now have a whistleblower mechanism in their organisation, with 22% of these respondents rating the service as effective, while a further 5% rated it as very effective.

Tip-offs, both external and internal, including via a formal whistleblowing channel, accounted for 37% of all methods by which frauds were discovered. This is consistent with the results from previous years and similar to other studies[1]. This is good news for New Zealand, as it appears that organisations here are realising the value of whistleblower hotlines as an effective forum for people to report concerns.

On 30 June 2013, the AML/CFT Act came into force. Compliance with this Act has meant that affiliated businesses operating in New Zealand have invested significant time and resources to ensure they have effective controls in place to monitor customer accounts and associated transactions. Many of these controls have been implemented through the use of electronic systems, which is likely linked to the high percentage of fraud detected through suspicious transaction reporting and data analytics.

Internal audit is now responsible for 11% of frauds discovered. This is back to pre Global Financial Crisis levels, having dropped significantly previously (2011: 2%). This may indicate that companies here are also beginning to refocus their efforts and investments when it comes to resourcing internal controls and internal audits teams.

1 ACFE 2012 Global Fraud Study, Initial Detection of Occupational Frauds from 'Tip', 43.3% and in 2010, 40.2%

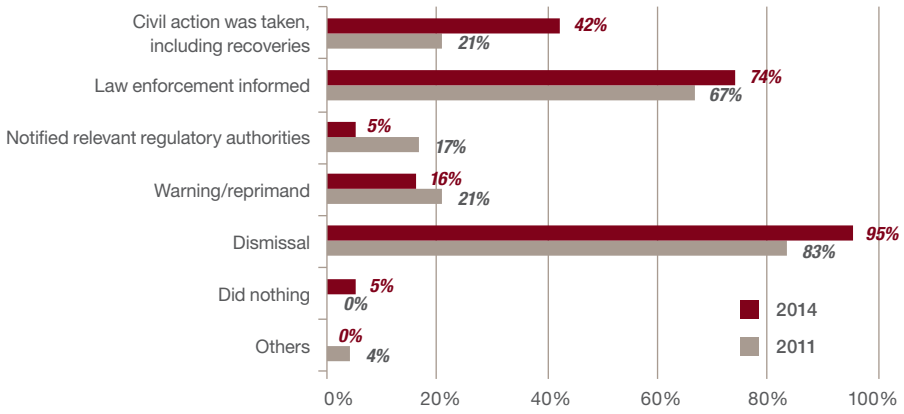
# Actions taken against fraudsters

**This year's survey confirms that organisations continue to respond to internal fraud aggressively, with 95% saying they are dismissing perpetrators once detected. Overall, the results indicate that aggressive actions such as dismissal (95%), informing law enforcement (74%) and civil action (42%) are on the increase.**

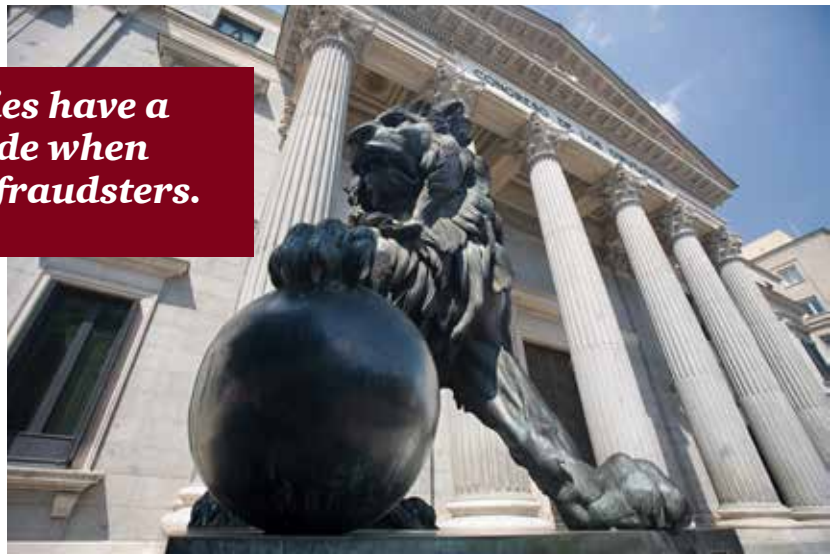
This indicates that New Zealand companies have a 'zero tolerance' attitude when dealing with internal fraudsters, with organisations now more willing to deal with fraudsters through official channels. The 12% increase in dismissals suggests that organisations see these fraudulent employees as detrimental to their organisations and are not afraid to replace them.

Civil action, including recoveries, has doubled since 2011, which suggests that response procedures are becoming more mature and effective, with organisations now more devoted to not just dismissing the fraudster but recovering their losses too.

## Actions taken against internal fraudsters in New Zealand




***New Zealand companies have a 'zero tolerance' attitude when dealing with internal fraudsters.***



# The external fraudster

**There has been a substantial change in the overall profile of the external fraudster since 2011. The number of frauds carried out by vendors and agents/intermediaries has significantly increased with the former now accounting for 25% of external fraud occurrences (2011: 9%) and the latter also accounting for another 25% (2011: 14%).**

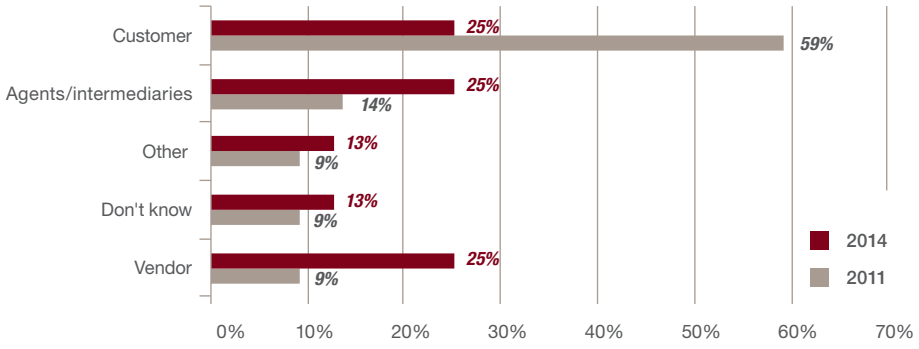
This increase is potentially linked to the large number of respondents (49%) we had in the following industries:

- Energy, utilities and mining (9%)
- Engineering and construction (6%)
- Government/state-owned enterprises (22%)
- Transportation and logistics (10%)

These industries are particularly vulnerable to external fraud from vendors and intermediaries, primarily because they have outsourced many non-core (and in some cases core) elements of their value chains, with a resulting increase on reliance on suppliers and intermediaries.

We also noted that the number of frauds carried out by customers was significantly down (25%) (2011: 59%), while worryingly, there was a significant increase in respondents who reported a 'don't know' when asked to profile the fraudster. As mentioned previously, knowing your enemy is imperative when combating economic crime, especially if trying to recover costs and identify better controls.

## Profile of the external fraudster



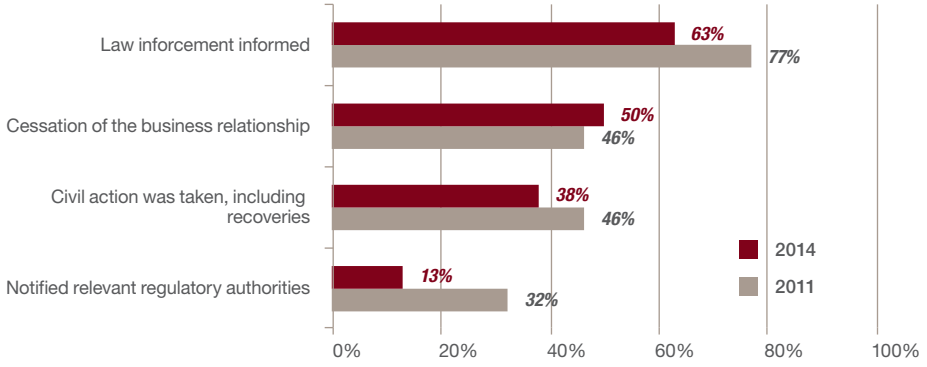

***Knowing your enemy is imperative when combating economic crime, especially if trying to recover costs and identify better controls.***

# Confront an external fraudster

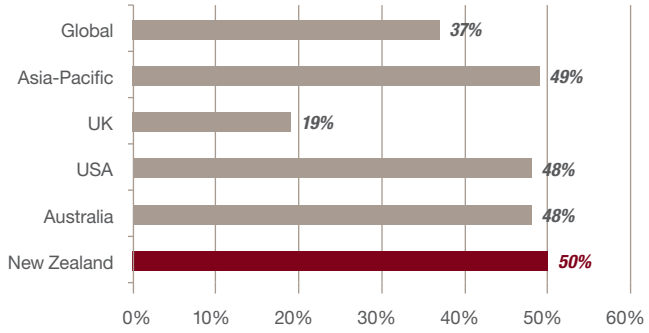
**Consistent with previous years, the most common action taken against an external perpetrator in New Zealand was informing law enforcement (63%). The global average was 61%.**

In addition, New Zealand companies appear to have little tolerance when it comes to dealing with third-party related fraud, with 50% of our respondents ceasing business relationships. This is similar to other developed economies, such as Australia (48%) and the USA (48%), and regionally puts us on a par with the Asia-Pacific average (49%).

## Actions taken against external fraudsters




## Cessation of business relationships



# *Who did we survey?*

**48**

questions to assess corporate attitudes, approaches and experience to fraud in the current economic environment

**82**

New Zealand respondents

**43%**

of all respondents were CFOs

**63%**

of companies surveyed operate in New Zealand only

**22%**

of organisations operate in government and state-owned enterprise sectors

**37%**

of all respondent companies had between 501 – 1,000 employees

**74%**

of those who had suffered some form of economic crime reported less than 10 incidents over the past 24 months

**63%**

of respondents estimated that the financial loss associated with incidents of economic crime was less than NZ$60,000

# Appendix

## Purpose of the 2014 survey

The aim of our survey was to assess corporate attitudes, approaches and experiences to fraud in the current economic environment, and particularly to understand whether the incidents of cybercrime-related fraud is becoming more prevalent in recent years, the prevalence of bribery/corruption, money laundering and anti-competition, and what types of fraud are most common.

## Terminology

### Accounting fraud

Financial statements and/or other documents are altered or presented in such a way that they do not reflect the true value or financial activities of the organisation. This can involve accounting manipulations, fraudulent borrowings/raising of finance, fraudulent application for credit and unauthorised transactions/rogue trading.

Asset misappropriation, including embezzlement/deception by employees.

The theft of assets (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit.

### Bribery and corruption

The unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail. It can also refer to the acceptance of such inducements. Specific examples include kickbacks, extortion, gifts (with strings attached), facilitation payments, etc.

### Competition law/anti-trust law

Law that promotes or maintains market competition by regulating anti-competitive and unfair business practices conduct by organisations. Examples may include price fixing, excessive, predatory or discriminatory pricing, unfair trading terms, and tying (i.e. stipulating that a buyer wishing to purchase one product must also purchase all or some of his requirements for a second product).

### Cybercrime

Also known as computer crime is an economic offence committed using the computer and internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a byproduct in order to create the fraud and only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one.

### Economic crime

The intentional use of deceit to deprive another of money, property or a legal right.

### Espionage

Espionage is the act or practice of spying or of using spies to obtain secret information.

### Financial loss

When estimating financial losses due to fraud, the participants should include both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to 'loss of business opportunity'.

### Financial terms

When estimating financial losses due to fraud, the participants should include both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to 'loss of business opportunity'.

### Fraud risk assessment

Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to specifically consider:

i. The fraud risks to which operations are exposed;

ii. An assessment of the most threatening risks (i.e. Evaluate risks for significance and likelihood of occurrence);

iii. Identification and evaluation of the controls (if any) that are in place to mitigate the key risks;

iv. Assessment of the general anti-fraud programmes and controls in an organisation; and

v. Actions to remedy any gaps in the controls.

### Human resources fraud (recruitment and/or payroll fraud)

Fraud committed by members of the human resources department, including payroll fraud, ghost employees, pay-to-work, recruitment (i.e. hiring friends and/or relatives, hiring unqualified individuals, falsification of documents, etc.).

### Incentive/pressure to perform

The individual has some financial problem that he/she is unable to solve through legitimate means so he/she begins to consider committing an illegal act as a way to solve the problem. The financial problem can be professional (e.g. job is in jeopardy) or personal (e.g. personal debt).

### Insider trading

Insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. Insider trading violations may also include 'tipping' such information, securities trading by the person 'tipped', and securities trading by those who misappropriate such information.

### IP infringement (including trademarks, patents, counterfeit products and services)

This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing with off as genuine.

### Markets with a high level of corruption risk

While corruption risk levels can be subjective, for the purposes of this survey we suggest a territory with a Transparency International Corruption Perception Index (CPI) score of 50 or less be considered a market with a high level of corruption risk. The link below the responses will direct you to the Transparency International list of territories and CPI scores.

### Money laundering

Actions intended to legitimise the proceeds of crime by disguising their true origin.

### Mortgage fraud

Mortgage fraud schemes employ some type of material misstatement, misrepresentation, or omission relating to a real estate transaction which is relied on by one or more parties to the transaction.

### Opportunity or ability

The individual finds some way that he/she can use (abuse) his/her position of trust to solve the financial problem with a low perceived risk of getting caught.

### Procurement fraud

Illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to his organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation.

### Rationalisation

The individual finds a way to justify the crime to himself/herself in a way that makes it an acceptable or justifiable act.

### Tax fraud

An illegal practice where an organisation or corporation intentionally avoids paying its true tax liability.

### About PwC Forensic Services

The Forensic Services group of PwC's global network of firms provides our clients with the full range of investigative response to fraud and other forms of economic crime. We also assist our clients in undertaking prevention measures to better protect themselves from fraud.

# Contacts

**Eric Lucas**
**Partner**
Forensic Services
+64 9 355 8647
eric.lucas@nz.pwc.com

**Colin Slater**
**Partner**
Risk and Control Solutions
+64 4 462 7244
colin.p.slater@nz.pwc.com

**Stephen Drain**
**Director**
Forensic Services
+64 9 355 8332
stephen.c.drain@nz.pwc.com

**Campbell McKenzie**
**Director**
Forensic Technology Solutions
+64 9 355 8040
campbell.b.mckenzie@nz.pwc.com

© 2014 PricewaterhouseCoopers New Zealand. All rights reserved. 'PwC' and 'PricewaterhouseCoopers' refer to the New Zealand member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details

pwc.co.nz/crimesurvey

#NZCrimeSurvey

# *Shifting beyond our borders: Economic Crime in Singapore*

**24%**
1 in 4 Singapore-based respondents have experienced some form of economic crime in the last two years.

**80%**
Asset misappropriation remains the most commonly experienced economic crime in Singapore and globally.

**70%**
Most Singapore-based respondents have operations in countries with high levels of corruption risk.

pwc

*http://www.pwc.com/sg/en/economic-crime-survey/index.jhtml*

# Contents

*Although Singapore-based companies are reporting lower incidences of fraud relative to the global average, we cannot be complacent as the battle against white collar crime is an ongoing one, and an increasingly borderless one.*

# *Foreword*

It will surprise few to learn that the incidence of economic crime reported in Singapore – such as procurement fraud, cybercrime, bribery and corruption - is lower than the rate recorded globally. Singapore's reputation as a safe and transparent place to do business is reflected in the views of the Singapore-based respondents to our 2014 Global Economic Crime Survey[1].

While this is encouraging, the risk of fraud for companies operating in Singapore as well as globally continue to evolve. Increasing reliance on technology poses great threats in the form of cybercrime, as evidenced in the several high profile incidents which have occurred in Singapore in the last few months. In addition, ongoing globalisation means that many Singapore-based companies are now doing business in environments with inherently higher corruption risks.

Although the Singapore respondents are generally reporting lower incidences of fraud relative to the global average, we cannot be complacent as the battle against white collar crime is an ongoing one, and an increasingly borderless one. Businesses need to continually assess the mechanisms they have in place for dealing with these risks, and consider if their current strategies are adequate in view of the increasing threats.

The Singapore edition of our 2014 Global Economic Crime survey turns the spotlight to the types of economic crime most commonly experienced in Singapore, together with the biggest perceived impacts on organisations. The report also provides guidance on how companies can manage these risks.

We trust that the report will be a valuable resource to stakeholders in all areas of your business. As the old Chinese Sun Tze saying goes, "know thy self and enemy to be successful" (知己知彼，百战不殆) - companies that understand their risk environment well and mitigate these threats appropriately will be poised to limit their losses to economic crime and be better positioned to respond to the ever changing global business environment we operate in.

Chan Kheng Tek
PwC Singapore Forensics Leader
February 2014

[1] Throughtout this report we refer to "Singapore-based" organisations, which consist of both local Singaporean companies or multinationals based in Singapore.

*In the last 24 months, one in four (24%) Singapore-based companies have experienced economic crime relative to one in three companies globally (37%).*

# The Big Picture

Our survey revealed that in the last 24 months, one out of every four Singapore-based companies (24%) experienced some form of economic crime. This result is certainly favourable relative to the global average of more than one third (37%). The number of incidents of economic crime experienced by Singapore companies was also significantly lower than the global average. Of the Singapore companies that suffered from some type of economic crime, 80% reported fewer than 10 incidents over the last 24 months as compared to the global average of 61%.

These results are not surprising given the strong emphasis on governance and controls in both the private and public sector in Singapore. The clean and transparent business environment coupled with our strong legal framework explains why Singapore ranks very highly in many global business surveys, such as the Transparency International's Corruption Perception Index 2013, in which Singapore received a fifth place ranking out of 177 countries and territories.[2] However, despite the good governance and safe business environment, one out of every four Singapore businesses still suffer fraud, and there is much high profile evidence of these cases occurring both in the private and public sector.

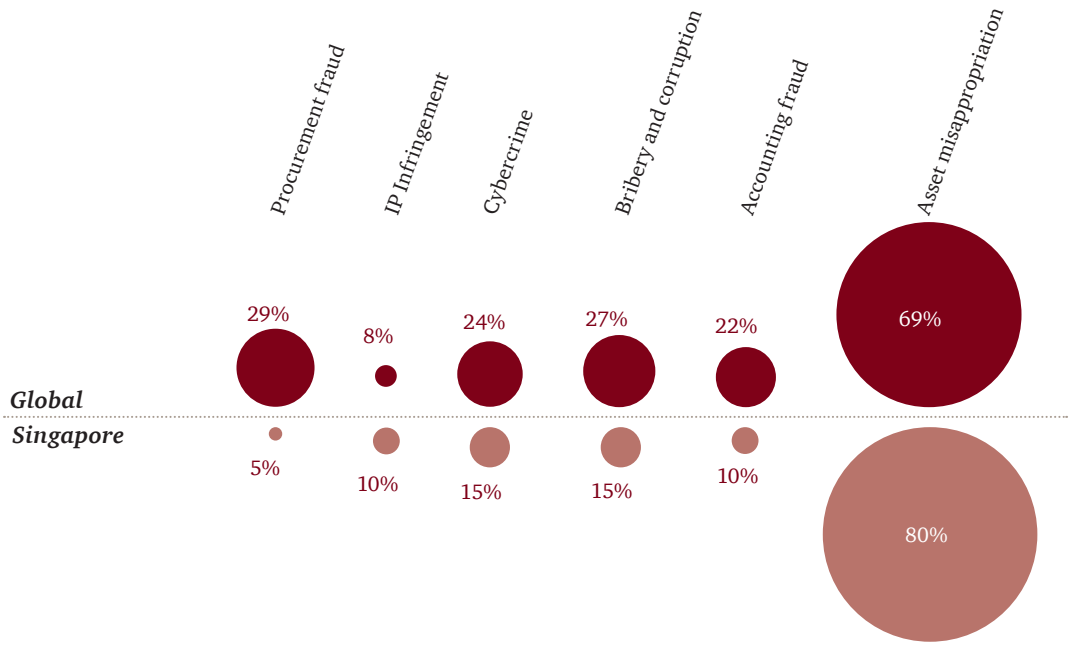
The message for Singapore-based companies is therefore clear - fraud is not something that can be eliminated. Organisations need to resist the temptation to become complacent. As our business environment and society evolve, and Singapore companies continue to expand beyond our borders, companies need to be vigilant and continually assess the risk of fraud.

[2] 2013 Corruption Perceptions Index, Transparency International, 2013

# Types of Economic Crime

Our survey results show that the main economic crimes experienced by Singapore-based companies were asset misappropriation (80%), followed by bribery and corruption (15%) and cybercrime (15%). Globally, asset misappropriation (69%), procurement fraud (29%), bribery and corruption (27%) and cybercrime (24%) featured as the most frequently experienced types of economic crime.

What types of economic crime has your organisation experienced within the last 24 months?[3]




[3] Note respondents may have experienced one or more types of economic crime in the last 24 months.

## Asset Misappropriation

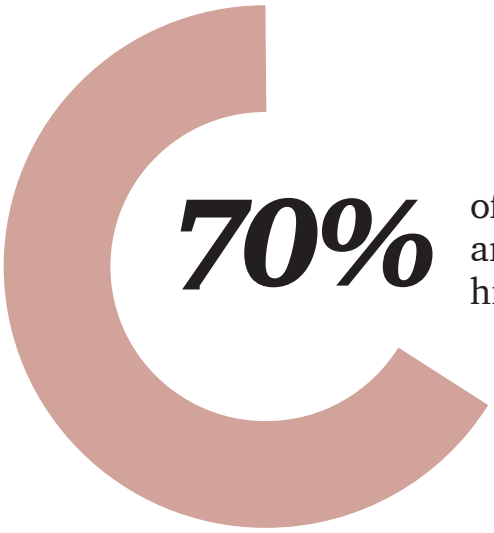
Asset misappropriation continues to be the most commonly experienced type of economic crime both in Singapore and globally.

The relatively high rate of asset misappropriation is consistent with what we regularly see in the whistle blowing investigations we have been involved in. In most circumstances, the key elements of the fraud triangle (pressure/motivation, opportunity and rationalisation) converge, causing staff members to turn to crime to finance their lifestyle (e.g., credit card or gambling debts or other financial pressure creates a motivation to commit fraud). Typically, the root cause for this type of fraud is due to a misplaced reliance on trust coupled with a weak compliance culture or attitude towards controls in the organisation (opportunity). The longer the perpetrator is employed by the company, the higher the level of reliance on trust in these long serving employees, which creates a false sense of security amongst management. Under such circumstances, the perpetrator may succumb to the temptation to dip their hands into the company's coffers and try to justify their actions based on some sense of entitlement (rationalisation).

## Bribery and Corruption

Due to a strong and efficient local legal framework, strict deterrence in the form of punishments, as well as the typically strong culture of anti-bribery/ anti-corruption compliance, only 15% of Singapore respondents reported incidents of bribery and corruption as compared to 27% of global respondents.

However, it is important to note that the risk of corruption for Singapore-based companies extends beyond Singapore. Our survey also found that 70% of Singapore-based respondents have operations in markets with high levels of corruption risk (compared to 50% globally). Increasing globalisation and the need for Singapore companies to look beyond the domestic market to stay competitive has resulted in 60% of Singapore-based companies pursuing an opportunity in a market with a high level of corruption in the last two years (compared to 38% globally). More than half of the Singapore-based respondents perceive that corruption/bribery is the highest risk in doing business globally compared to other risks such as money laundering and competition law.



**70%** of Singapore-based companies are operating in markets with high levels of corruption

## *Bribery in Singapore and beyond*

In 2013, Asian regulators stepped up enforcement efforts to crack down on bribery and corruption. There have been several examples of Singapore registered companies who have been allegedly involved in bribery or corruption outside of Singapore. Some recent cases include:

i. Bribery by a Singapore contractor - a Singapore-based contractor was charged in connection with alleged bribes paid to a US Navy ship commander and a Naval Criminal Investigative Service agent in exchange for information relating to the worldwide movement of Navy ships. The charges resulted in the loss of hundreds of millions of dollars in US Navy contracts affecting not only the specific entity but other Singapore businesses involved in the supply chain as well.[4]

ii. Bribery of an Indonesian oil and gas official - a Singapore-based crude oil trader is alleged to have made significant cash bribes and offered gifts to an executive with Indonesia's oil and gas regulator in order to gain favour in crude oil tenders.[5]

This trend reflects the greater importance for Singapore companies to perform risk-based due diligence on international business partners to mitigate potential bribery and corruption risks. Taking such preventive actions and implementing a robust anti-bribery and corruption compliance programme will substantially lessen the risk of falling prey to these types of crimes. In addition, doing so may also help companies avoid the wrath of the regulators in the event of a bribery investigation. In one recent case involving a Singapore-based employee of a major financial institution, US regulators dropped all charges against the organisation but prosecuted (and jailed) the rogue employee. The charges against the organisation were dropped on the basis that its compliance programme was sufficiently robust to provide "reasonable assurance" that its employees were not bribing government officials.

[4] http://www.reuters.com/assets/print?aid=USBRE99L00620131022

[5] http://sg.finance.yahoo.com/news/indonesia-energy-regulator-chief-detained-114731010.html

## Cybercrime

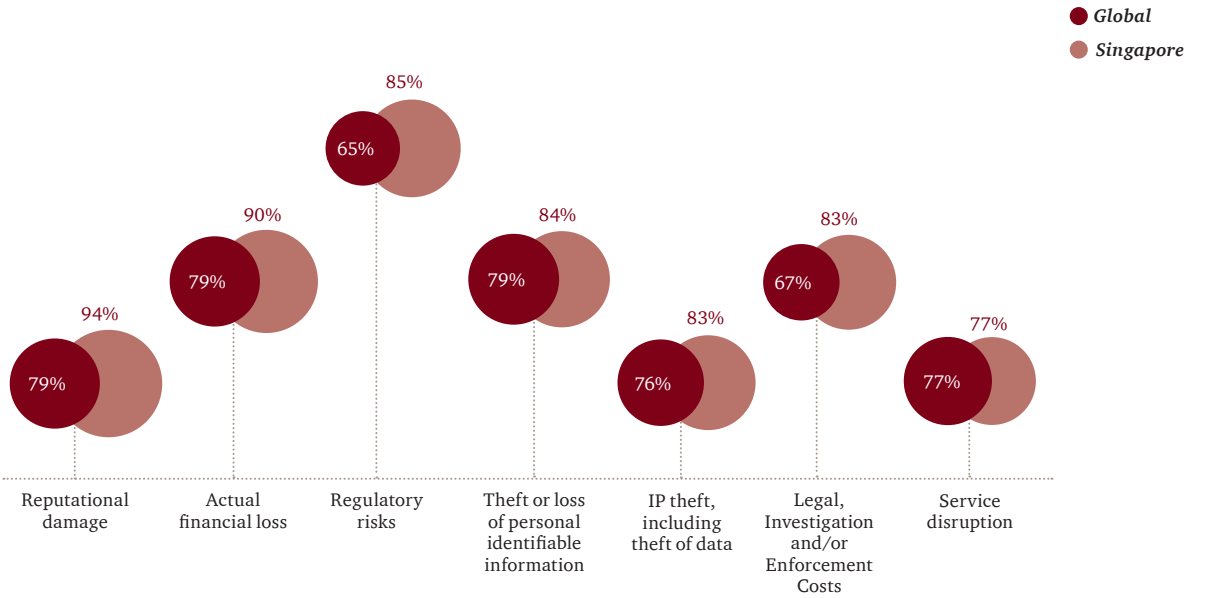
Singapore respondents reported fewer cyber incidents compared to global respondents, at 15% and 24%, respectively. While the survey revealed fewer cybercrime episodes in Singapore, the risk of cybercrime occurring here is clear and present. In our recent annual Global CEO Survey, PwC asked over 1,300 CEOs what they thought would be the next big thing to revolutionise their business, industry or society over the next 10 years. Somewhat unsurprisingly, technology was the most common response.[6] The various technologies underpinning this revolution are creating exciting opportunities for companies but also include a range of risks. These risks are evident from several prominent and high impact cyber incidents which have taken place in Singapore in the last 12 months, including:

i. In June 2013, a Singaporean traditional chinese medicine company had its website hacked and defaced with messages.[7]

ii. In November 2013, a Singapore government website was hacked into. The website's search function was impaired and images were overlaid on the webpage.[8]

iii. In December 2013, the Singapore branch of an international bank discovered that close to 650 of its private bank clients' details had allegedly been stolen. The purported theft of the bank statements did not occur through the banks' IT and data system. Instead the information was allegedly stolen from one of the servers of a third-party service provider which was hired by the bank to print bank statements.[9]

How concerned are you about the effects of each of the following types of cybercrime activity on your organisation?




[6] "Fit for the future: Capitalising on global trends" 17th Annual Global CEO Survey, PwC, 2014

[7] www.straitstimes.com/breaking-news/singapore/story/hackers-deface-eu-yan-sang-website-leave-haze-related-messages-2013062

[8] http://www.straitstimes.com/breaking-news/singapore/story/subpage-the-prime-ministers-office-website-hacked-investigations-ongoi

[9] http://www.straitstimes.com/breaking-news/money/story/account-information-stolen-nearly-650-clients-stanchart-singapores-private

*Organisations must ensure their cyber security policies and controls are implemented appropriately and continually test the effectiveness of these efforts.*

Despite the low incidence of cybercrime recorded in our survey, Singapore respondents are still rightly concerned over the various negative effects of potential cybercrime activity, with reputation damage listed as their biggest worry, followed by actual financial losses and regulatory risk. In response to the ongoing threats posed by cybercrime, on 15 January 2014, the Infocomm Development Authority (IDA) announced that the global network security firm FireEye had teamed up with IDA to open a facility dedicated to developing expertise in cyber security. [10]

The above measures are strengthened by Singapore's well-established legal and regulatory environment with regards to cybercrime (e.g., the Computer Misuse and Cybersecurity Act, MAS Internet Banking and Technology Risk Management Guidelines, and Instruction Manual 8 for the Singapore Government). Most recently, Singapore also enacted the Personal Data Protection Act (PDPA) which governs the collection, use, disclosure and care of personal data. The main data protection rules will come into force in July 2014. Organisations have the opportunity to strengthen their cyber security policies and controls by implementing a programme in compliance with the PDPA.

While the regulatory framework provides mandates and guidance, organisations must ensure their cyber security policies and controls are implemented appropriately, and continually test the effectiveness of these efforts. As companies increasingly rely on IT and electronic data, the use of automation in cyber security, policy compliance and data analytics becomes more important. Lastly, businesses also need to consider implementing and testing their cyber incident management capabilities, so that they will be able to effectively react to an incident when it occurs.

[10] https://www.ida.gov.sg/About-Us/Newsroom/Speeches/2014/Speech-by-Ms-Jacqueline-Poh-of-IDA-at-the-Opening-of-Fireeyes-Centre-of-Excellence

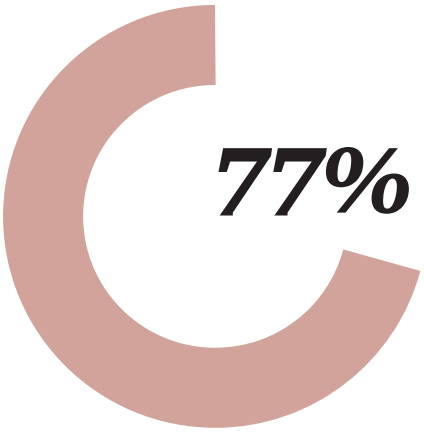
*As Singapore companies continue to expand their footprint in the region, procurement functions will be exposed to environments where fraud is a greater risk.*

## Procurement Fraud

In Singapore, companies experienced a significantly lower rate of procurement fraud as compared to the global survey respondents (5% compared to 29%). All of the Singapore-based respondents who reported procurement fraud in the last 24 months experienced it in the vendor selection process. There was not a single reported incident of fraud in the bid process, contracting or the payment process.

However, companies should again resist the temptation to become complacent in relation to procurement. Examples of common procurement fraud we continue to see in our investigations include incidences of theft of inventory, manipulation of bids by multiple vendors, kickbacks to procurement officers through inflated price of purchases and payment of bribes to buyers to place suppliers on the approved vendor list.

As Singapore companies expand their footprint in the region, the procurement department will be exposed to environments where fraud is a greater risk, and the individuals exposed to these challenges have to be well prepared to mitigate these potential procurement risks.

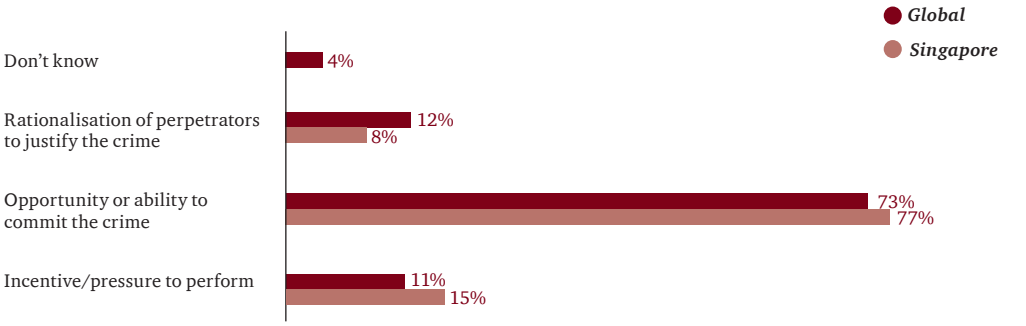


**77%** of Singapore companies felt the biggest factor contributing to economic crime occurring is opportunity or ability to commit the crime.

## Detecting Fraud

A significant majority of Singapore companies (77%) stated that the biggest factor contributing to economic crime occurring was opportunity or the ability to commit the crime. This reinforces the importance of a strong internal control framework coupled with a rigorous approach to compliance to minimise opportunities to commit economic crime.

What factor do you feel has contributed the most to economic crime committed by internal actors?

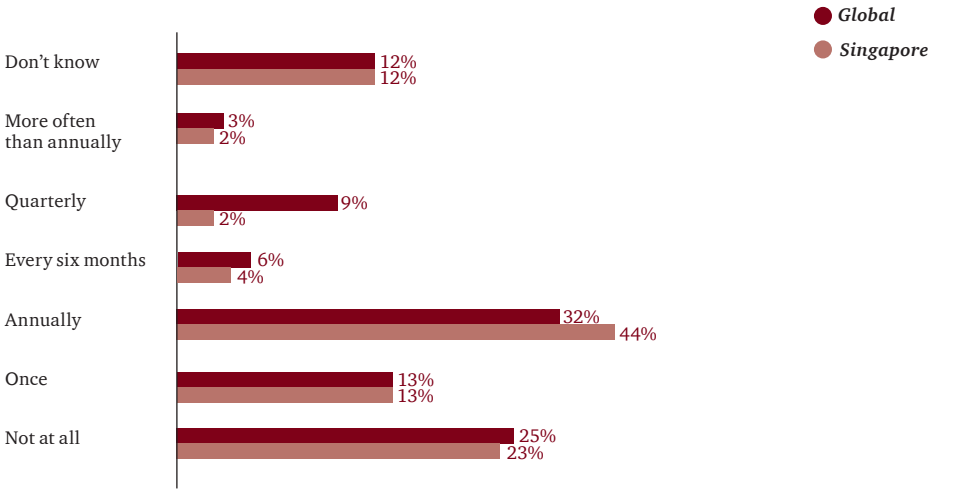



Encouragingly, our survey showed that the majority of Singapore companies do conduct fraud risk assessments. The percentage of companies which conducted a fraud risk assessment in the past two years does not vary significantly between Singapore (65%) and the global average (63%). Singapore companies tend to rely on annual assessments (44% compared to 32% globally), whereas global respondents seem to perform these more frequently, with 15% conducting assessments on a quarterly or half yearly basis, compared to 6% of Singapore-based respondents.

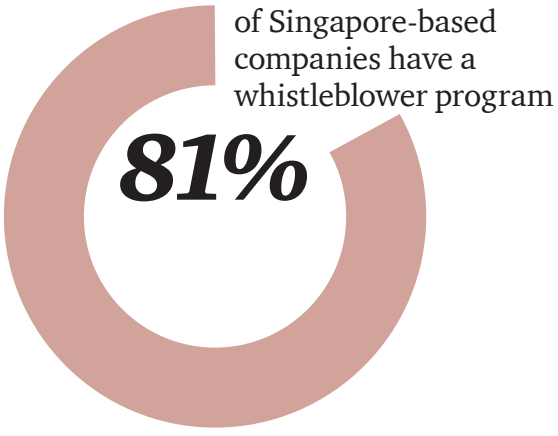
A fraud risk assessment is a tool that enables businesses to better mitigate risks through the introduction or strengthening of controls. The benefits of a fraud risk assessment include the identification of departments that pose the greatest risk of fraud; the evaluation of existing controls to determine whether they are operating effectively; and the identification of gaps where additional controls are needed.

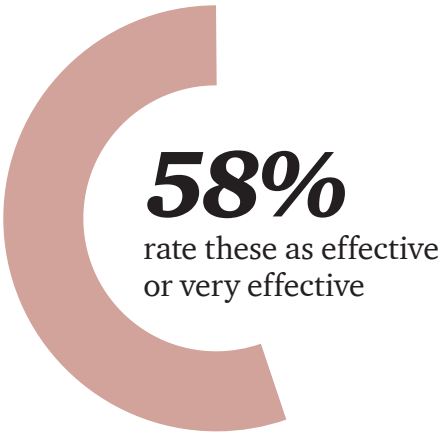
Notwithstanding the above, there remains a significant percentage of companies both in Singapore and globally (35% and 37%, respectively) that do not conduct fraud risk assessments or are unaware if they do. The reasons given by Singapore respondents for not conducting a fraud risk assessment was a perceived lack of value (37%) and being unsure what a fraud risk assessment entails (21%).

In the last 24 months, how often has your organisation performed a fraud risk assessment?




Apart from fraud risk assessments, whistleblower programmes have been gaining traction and are now widely adopted in Singapore. Singapore companies with whistleblower programmes have increased more than two-fold from a 35% adoption rate in 2005[11] to 81% in 2013. Not only is the adoption rate higher than the global rate of 62% in 2013; of the 81% of Singapore companies that have a whistleblower programme, 58% of these companies rate the whistleblower programme as effective or very effective as compared to 50% globally.

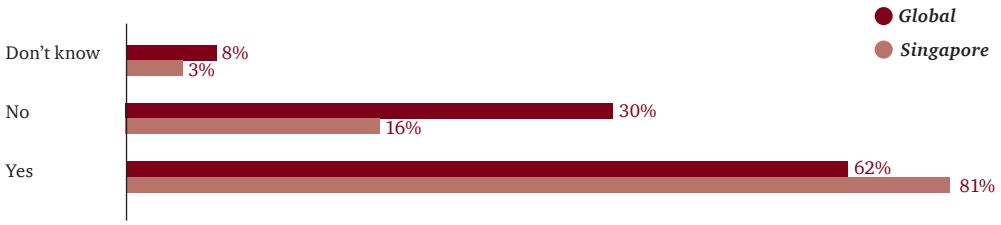


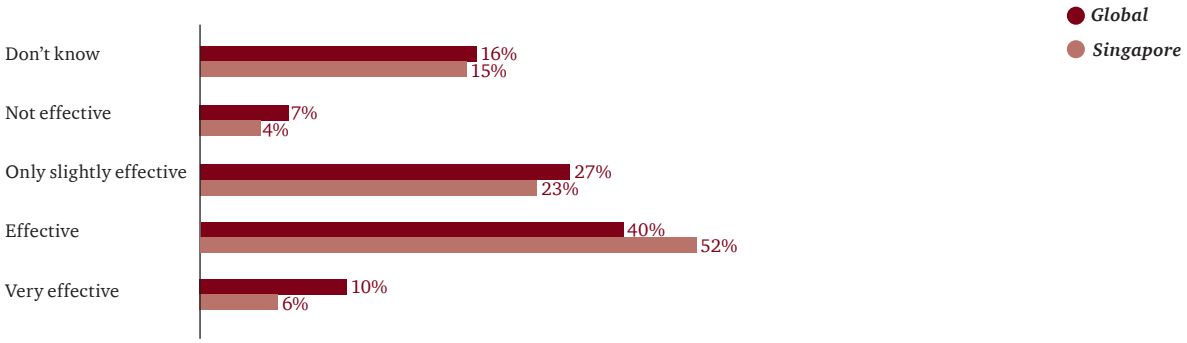

[11] Economic crime: people, culture & controls: The 4th biennial Global Economic Crime Survey, Singapore, PricewaterhouseCoopers

*Fraud risk assessments are enabling many companies to better mitigate risks through the introduction or strengthing of controls.*

Does your organisation in Singapore and Globally have a whistleblower mechanism?




How effective would you rate your whistleblowing mechanism in the prevention and detection of economic crime?



# *Terminology*

## Accounting fraud

Financial statements and/or other documents are altered or presented in such a way that they do not reflect the true value or financial activities of the organisation. This can involve accounting manipulations, fraudulent borrowings/raising of finance, fraudulent application for credit and unauthorised transactions/rogue trading.

## Asset misappropriation, including embezzlement/ deception by employees

The theft of assets (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit.

## Bribery and corruption

The unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail. It can also refer to the acceptance of such inducements. Specific examples include kickbacks, extortion, gifts (with strings attached), facilitation payments, etc.

## Competition law/Antitrust law

Law that promotes or maintains market competition by regulating anticompetitive and unfair business practices conduct by organisations. Examples may include price fixing, excessive, predatory or discriminatory pricing, unfair trading terms, and tying (i.e., stipulating that a buyer wishing to purchase one product must also purchase all or some of his requirements for a second product).

## Cybercrime

Also known as computer crime; an economic offence committed using the computer and internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a by-product in order to create the fraud and only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one.

## Economic crime

The intentional use of deceit to deprive another of money, property or a legal right.

## Financial loss/Financial terms

When estimating financial losses due to fraud, the participants should include both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to "loss of business opportunity".

## Fraud risk assessment

Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to specifically consider:

i. The fraud risks to which operations are exposed;
ii. An assessment of the most threatening risks (i.e., Evaluate risks for significance and likelihood of occurrence);
iii. Identification and evaluation of the controls (if any) that are in place to mitigate the key risks;
iv. Assessment of the general antifraud programmes and controls in an organisation; and
v. Actions to remedy any gaps in the controls.

## Human Resources fraud (recruitment and/or payroll fraud)

Fraud committed by members of the Human Resources department, including payroll fraud, ghost employees, pay-to-work, recruitment (i.e., hiring friends and/or relatives, hiring unqualified individuals, falsification of documents, etc.).

## Incentive/Pressure to perform

The individual has some financial problem that he/she is unable to solve through legitimate means so he/she begins to consider committing an illegal act as a way to solve the problem. The financial problem can be professional (e.g., job is in jeopardy) or personal (e.g., personal debt).

## Insider trading

Insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. Insider trading violations may also include 'tipping' such information, securities trading by the person 'tipped', and securities trading by those who misappropriate such information.

## IP infringement (including trademarks, patents, counterfeit products and services)

This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing them off as genuine.

## Markets with a high level of corruption risk

While corruption risk levels can be subjective, for the purposes of this survey we suggest a territory with a 2013 Transparency International Corruption Perception Index ("CPI") score of 50 or less be considered a market with a high level of corruption risk.

## Money laundering

Actions intended to legitimise the proceeds of crime by disguising their true origin.

## Mortgage fraud

Mortgage fraud schemes employ some type of material misstatement, misrepresentation, or omission relating to a real estate transaction which is relied on by one or more parties to the transaction.

## Opportunity or ability

The individual finds some way that he/she can use (abuse) his/her position of trust to solve the financial problem with a low perceived risk of getting caught.

## Procurement fraud

Illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to his organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation.

## Rationalisation

The individual finds a way to justify the crime to himself/herself in a way that makes it an acceptable or justifiable act.

## Singapore-based respondents

Companies who participated in the survey who are local Singaporean entities or multinational companies based in Singapore.

# Contacts

**Chan Kheng Tek**
PwC Singapore Forensics Leader
+65 6236 3628
kheng.tek.chan@sg.pwc.com

**Sam Kok Weng**
PwC South East Asia Regional Forensics Leader
+65 6236 3268
kok.weng.sam@sg.pwc.com

**Jimmy Sng**
PwC Singapore
Technology Consulting Leader
+65 6236 3808
jimmy.sng@sg.pwc.com

**Goh Thien Phong**
PwC Singapore
Corporate Recovery Leader/Forensics Partner
+65 6236 4018
thien.phong.goh@sg.pwc.com

*http://www.pwc.com/sg/en/economic-crime-survey/index.jhtml*

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2014 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.

www.pwc.com/sk/forensic-services

# *Global Economic Crime Survey 2014*

## Economic Crime is on the rise

## Report for Slovakia

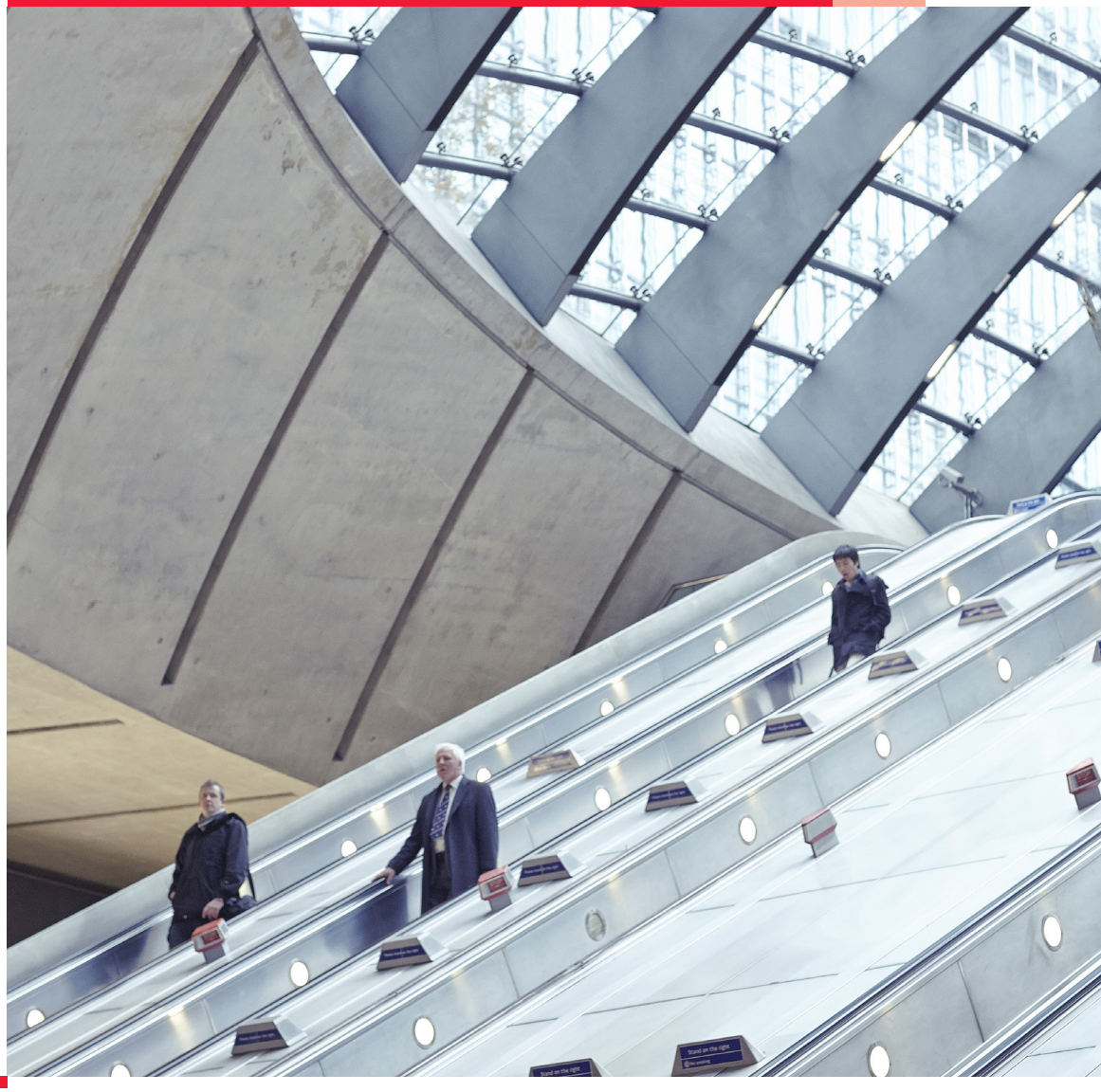
*Evolution of Fraud*

*Dangers of Crime*

*Cybercrime*

*Procurement Fraud*

*Corruption and Bribery*



pwc

# Contents



***The Global Economic Crime Survey 2014 was carried out by PwC. It is the largest survey of its kind with 5,128 survey participants from 99 countries, including 76 respondents from Slovakia.***

***The survey is intended not only to describe the current state of economic crime but also to identify trends and the perception of future risks.***

# Preface

In Lewis Carroll's 'Alice Through the Looking Glass', the Red Queen is reported as saying: *"Now, here, you see, it takes all the running you can do, to keep in the same place"*. In modern times, this has been used as an analogy of the theory of evolution.

We can take Mr Carroll's words as a very fine description of the development of the area of economic crime. Economic crime is constantly evolving and seeking new ways to thrive. Companies need to find new and more efficient ways to defend their assets or else they will be outpaced by the evolution of fraud.

The Global Economic Crime Survey 2014 supports this observation: economic crime is more common in the Slovak Republic and takes more diverse forms. Above all, procurement fraud has emerged as a standalone major category of fraud. We strongly advise companies to adjust their risk assessments accordingly.

Other interesting observations include a rise in the cost of economic crime, an increase in the share of fraud committed by agents or intermediaries, and generally the strict measures taken by companies against identified fraudsters.

We invite all entrepreneurs and managers to read through the report and to draw conclusions relevant to their undertaking. A global report available on www.pwc.com/crimesurvey and local variants for different countries including Slovakia are available to help companies doing business globally.

Last but not least, we would like to thank the survey participants who were kind enough to share their observations of fraud and provide their insights. We are especially grateful to the 76 responding entities from the Slovak Republic. All respondents share our belief that economic crime is too costly to ignore.

***Sirshar Qureshi***
Partner responsible for Forensic Services in CEE
PwC

***Michal Kohoutek***
Head of Forensic Services
PwC

# Main Findings

## The Dangers of Crime

**Econimic crime is on the rise**
Economic crime is increasingly common in the Slovak Republic. 34% of respondents indicated that their company has experienced economic crime within the last 24 months in the Slovak Republic; this represents a significant increase compared to GECS 2011 (21%). The current occurrence is in line with regional and global averages (38% and 37% respectively). 58% of organisations who suffered economic crime estimated the resulting total financial loss as USD 100,000 or more.

**Types of economic crime are more "creative"**
Traditionally, assets' misappropriation is the main type of crime seen (54%). However, fraudsters seek out new avenues from which to defraud their victims. The distribution of various types of economic crime is becoming more even, seeing an increase in the share of other types of crimes: bribery or corruption (31%), procurement fraud (31%), mortgage fraud (19%), cybercrime (12%), and money laundering (12%).

### *Cybercrime*

**Occurrence**
Globally, companies are more likely to suffer cybercrime than at any time in the past. A decline in the reported instances of cybercrime in the Slovak Republic (12% compared to 17% in GECS 2011) raises doubts regarding the ability of Slovak companies to detect cybercrime. The latency (share of undetected occurrences) of cybercrime may be even higher than in other countries.

**Risks of cybercrime**
In business practice, more and more reliance is being put on web applications, remote access and clouds. This increases the potential impact of cybercrime.

**High frequency of undetected cases**
Generally, cybercrime is dangerous as the victim companies might not detect the fraud taking place. We believe the latency is higher than the latency of asset misappropriation. Therefore, the real occurrence is most probably significantly higher than the number reported.

### *Procurement fraud*

**Occurrence**
Procurement fraud emerged as a standalone category of fraud, having been reported by 31% companies in Slovakia that were a victim of fraud. The top reported risk factor is the process of selecting vendor contracting /maintenance.

**Risks of procurement fraud**
Procurement fraud usually includes collusion between business parties. Therefore, the detection of this type of fraud is often difficult. However, there are ways to mitigate the risks. For example, companies with a large number of transactions and vendors may take advantage of data analytics to identify potential frauds or inefficiencies in procurement.

### *Corruption and bribery*

**Risks of corruption**
31% of companies that experienced fraud reported bribery and corruption. In comparison with the last survey, this represents an increase of 14 percentage points. Corruption is seen as the greatest risk in doing business globally, both in terms of reputation loss and monetary loss. This is supported by PwC's 17th Global CEO Survey 2014: 69% of Central and Eastern Europe ("CEE") Chief Executive Officers ("CEO") are concerned about the impact of corruption and bribery on their business. According to the PwC CEO Survey, corruption and bribery was the top threat to growth in the CEE region.

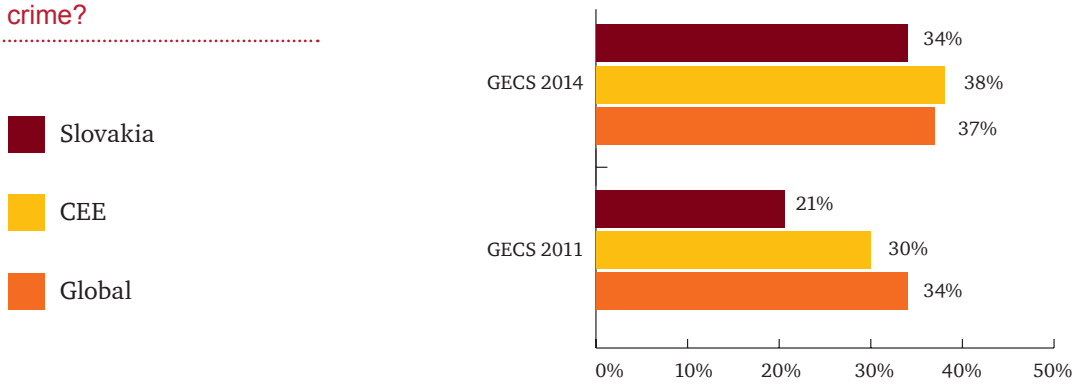
# *Economic Crime in the Slovak Republic*

## Central themes

### *Dangerous territory?*

We have seen a rise in reported economic crimes since the previous survey. In 2011, the number of Slovak companies detecting frauds (21%) was well below the regional and global average (30% and 34% respectively). This year, 34% of respondents indicated their companies had experienced economic crime in the past 24 months, which is in line with the global and regional average (37% and 38% respectively).

How many companies experienced economic crime?

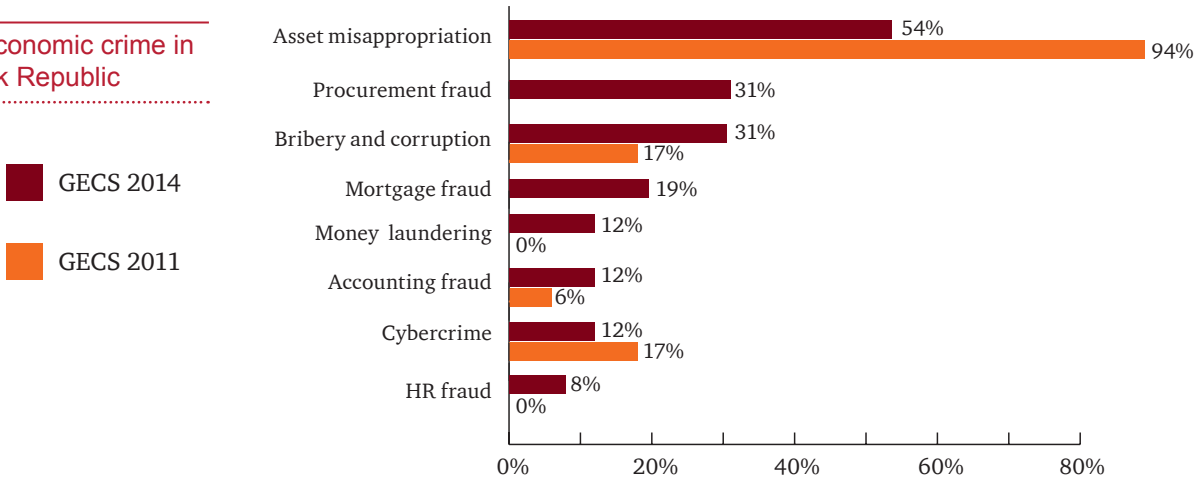



In order to understand the underlying reasons behind the increase, let us have a look at the changes in individual fraud categories.

# *Greater propensity to types of economic crime*

Attacks against corporate assets are more and more ”creative”. The relative share of asset misappropriation as the traditionally most common and simplest type of crime is decreasing in favour of more “creative” types of fraud.

Type of economic crime in the Slovak Republic




Since our first global economic survey in 2001, three types of fraud have consistently registered as leaders among respondents – asset misappropriation (usually by a wide margin), bribery and corruption, and accounting fraud. We added cybercrime as a distinct classification in 2011 and it immediately registered at 17%, alongside bribery and corruption, and accounting fraud.

This year, we added another new category – procurement fraud. Potentially driven by the on-going megatrend of outsourcing and organisational interconnectivity, procurement fraud received a significant response (31%), making it one of the most common types of fraud in the Slovak Republic.

The two other newly added categories of mortgage fraud (19%) and human resources fraud (8%) also reported significant occurrence in the Slovak Republic and it comes as no surprise that the overall number of organisations reporting economic crime in the Slovak Republic has increased so dramatically.

The most significant changes when comparing 2011 and 2014 were reported as the occurrence of money laundering (increase from 0% to 12%) and asset misappropriation (decrease from 94% to 54%). This seems to support the belief that the traditional type of fraud as asset misappropriation is still significant, however is decreasing in favour of “modern” types of fraud, or the schemes used by fraudsters are becoming more sophisticated and thus difficult to detect.

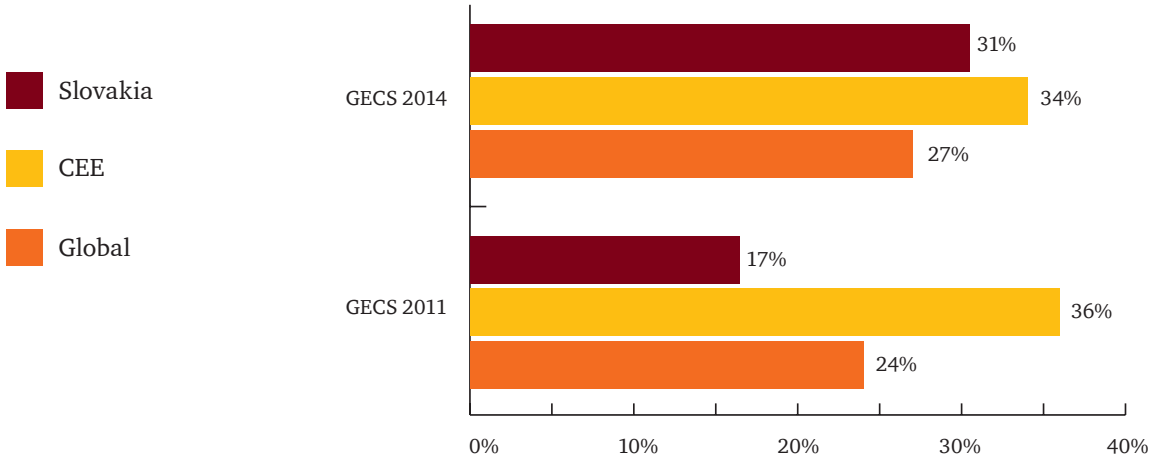
It is also quite likely that the relative occurrence of crimes such as bribery, cybercrime or procurement fraud is even higher. These types of crimes are difficult to detect. During our own forensic engagements, we encountered numerous instances of long-term schemes which were accidentally detected by the victim company.

Therefore, companies should pay adequate attention to the different fraud schemes they may be facing. Control over cash and other physical assets might not be enough.

## *Corruption and bribery*

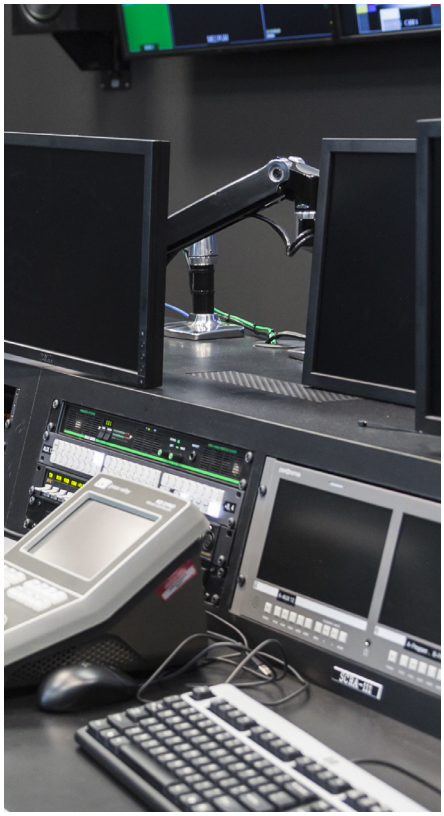
In recent years, corruption has become a topic of public discussion in the Slovak Republic, and for good reason. Corruption is among the most serious economic crimes and is seen as the greatest risk in doing business globally, both in terms of reputation loss and monetary loss. In terms of occurrence, it is the second most recorded type of economic crime in the Slovak Republic (31%) and the third globally in GECS 2014 (27%). CEE is, along with Africa, the region with the largest prevalence of corruption.

Share of corruption and bribery on fraud reported




PwC's 17th Global CEO Survey 2014 indicated that corruption awareness is on the rise, more than half of CEE CEOs considered corruption and bribery to be a threat.

According to GECS 2014, 20% of Slovak respondents indicated their company has been asked to pay a bribe in the last 24 months. 41% of respondents believe their company has lost an opportunity to a competitor which they believe had paid a bribe in the same period.



## *Procurement fraud*

For the first time, 2014 GECS included procurement fraud as a separate category within the economic crime category. 31% of Slovak companies which reported economic crime indicated that their companies experienced at least one instance of procurement fraud.

The reported high occurrence of procurement fraud exceeded even our expectations. As the detection of procurement fraud is difficult, it is probable that the actual occurrence is even higher.

This ranks procurement fraud as the second-to-third (together with bribery and corruption) most common reported type of fraud in the Slovak Republic. The most vulnerable point is vendor contracting and maintenance.

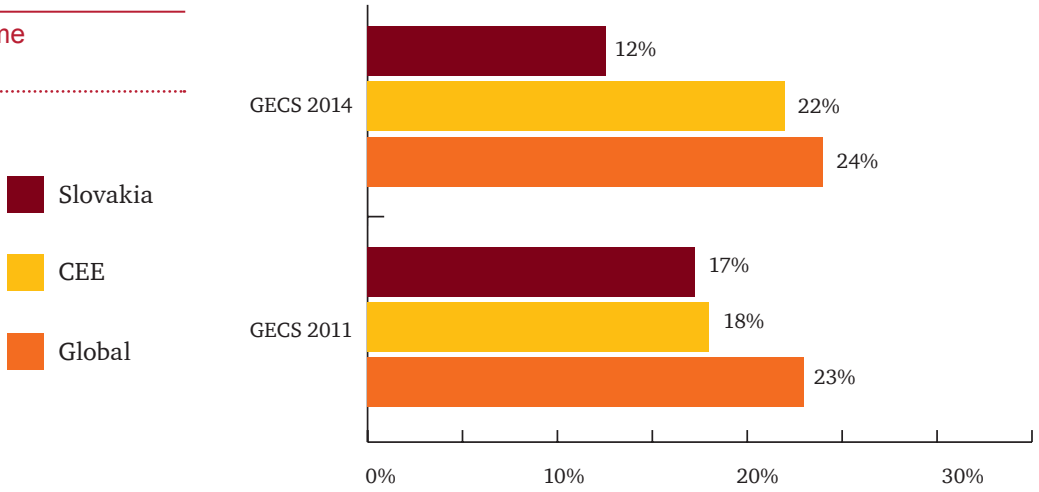
Generally speaking, when an organisation goes outside its own walls for services, goods or assets, the potential for procurement fraud exists. An increasing interconnectedness of business entities, together with more common outsourcing, makes companies more vulnerable to procurement fraud than ever before. Moreover, there are numerous ways procurement fraud can be committed. As a result, procurement fraud is one of the more difficult frauds to be detected and investigated.

## *Cybercrime*

Interestingly, the share of cybercrime as reported by Slovak companies is well below regional and global averages. The last share of 12% is even lower than the corresponding number from the previous pool (17%).

# *Cybercrime*

Share of cybercrime on fraud reported




Contrary to the low number of reported actual instances of cybercrime, 24% of respondents expect they will experience at least one occurrence of cybercrime in the next 24 months (see graph on page 14).

This raises certain doubts as to a possible gap between detection of cybercrime and its true occurrence. It is not clear why cybercrime's share in Slovakia, which is definitely a well-developed and computerised country, would amount to only half of its share in other countries. Therefore, we believe there is a risk that Slovak companies do not have the necessary abilities for detection (and prevention) of cybercrime. However, we have to bear in mind that almost one fourth of Slovak respondents thinks they are at risk of cybercrime and perceive a cybercrime occurrence likely in the forthcoming 24 months.

Modern companies are following trends in utilising technology to its full potential and to give their employees more freedom. People work from home using their own smart devices connected to cloud, respond to emails from internet cafes while on vacation, and review reports at airports. This is basically enlarging the perimeter that needs to be protected and deal with environments that are not fully under company control.

This is also a reason for a shift in security paradigm:
- 90s - respond after the breach;
- 00s - get ready for the breach; and
- 10s - assume the breach has happened or is underway.

It is not a question of whether the company will be subject to cyberthreat, but when and how it will happen. Successful companies are prioritising what matters most - guarding their crucial data against organised targeted attackers in the global business ecosystem covering fluid data moving around internally as well as to/ from business partners and other stakeholders. More than one half of respondents indicated that their perception of cybercrime risks has increased over the last 24 months. Theft of intellectual property, personal data or damage to reputation is of the greatest concern when it comes to cybercrime.

We can describe one of the cases we have worked on in the past. IT personnel in a large energy company found a computer in their server room, which they did not have in their books and they could not access it. At the same time they started to experience drop outs in internet connectivity, which was a significant issue due to online banking.

Through the investigation we have established the function of the unknown computer - one of the IT administrators was running a side internet business and he was misusing company resources for that. His cyber activity actually affected the whole business because they were not able to reconcile client payments as the online banking was not functioning.

**Tomáš Kuča,** Risk Assurance Partner leading our cyber security practice

**Aren't cybercrime and cybersecurity just more buzzwords?**
These are labels for the current phenomena in the information technology world. The rise of cybercrime is evident and supported by thousands of cases happening around us all the time. Cybersecurity is a preventative measure used to respond to this situation.

**What has changed in this field in the last couple years?**
In the past, companies responded after an incident occurred. In better cases they were building their protection in anticipation of a future incident. It would seem the current best approach for development of a cybersecurity policy is to assume a security breach has already happened.

The attackers have changed, which means they use sophisticated and persistent methods, they target specific information for strategic gains, they work across the globe, they are structured and organised and some of them act on behalf of states.

**What can be done to improve our situation?**
- Employ a chief information security officer and get him involved at the board level "the top of the house".
- Clarify roles and responsibilities in this area.
- Create a cyberincident response team.
- Invest in cyberskills of your employees.
- Set up cooperation with cybercrime experts.

### *Impact of economic crimes*

No discussion of economic crimes would be complete without trying to quantify the impact of fraud. After all, the anti-fraud effort is just another function of the company which should pay off to justify its existence.

In Slovakia 58% of respondents who experienced economic crime reported a total loss of at least USD 100,000. This is a reported loss by companies that usually care and try to prevent and detect fraud. How greater would the actual loss be if the company did not care and there were no counter fraud measurements?

There are also other negative impacts on the company besides purely financial losses. Companies report a clear impact on the company's reputation and employee morale as the greatest non-financial impact.

In this respect, we would like to point out that a negative impact on employee morale might serve as a trigger to secondary actions (fraud being perpetrated by frustrated or demotivated employees). "Everybody does it" or "they deserved it" has been observed many times as a handy rationalisation of first-time fraudsters!

# Managing fraud

### *Who commits fraud*

We tried to make a profile of the perpetrator of the most serious economic crime that the respondent companies had experienced.
There is an imbalance of internal and external perpetrators of the most serious fraud detected (31% against 58%).

It should come as no surprise that middle to senior managerial persons are much more likely to commit the most serious internal fraud than junior staff members. The most typical fraudster is male, 31 to 40 years old and has spent 6 to 10 years in the company.

The person most likely to commit the most serious external fraud is a customer, both in the Slovak Republic (53%) and globally (32%). As already indicated in GECS 2011, we would recommend that organisations continue their efforts on the prevention front: knowing your employees and your business partners prior to engaging with them is less costly than dealing with the consequences of fraud.

### *Prevention of fraud*

Why would someone decide to commit a fraud? Our survey indicates that by far the most significant contributing factor for internal fraudsters is simply opportunity.

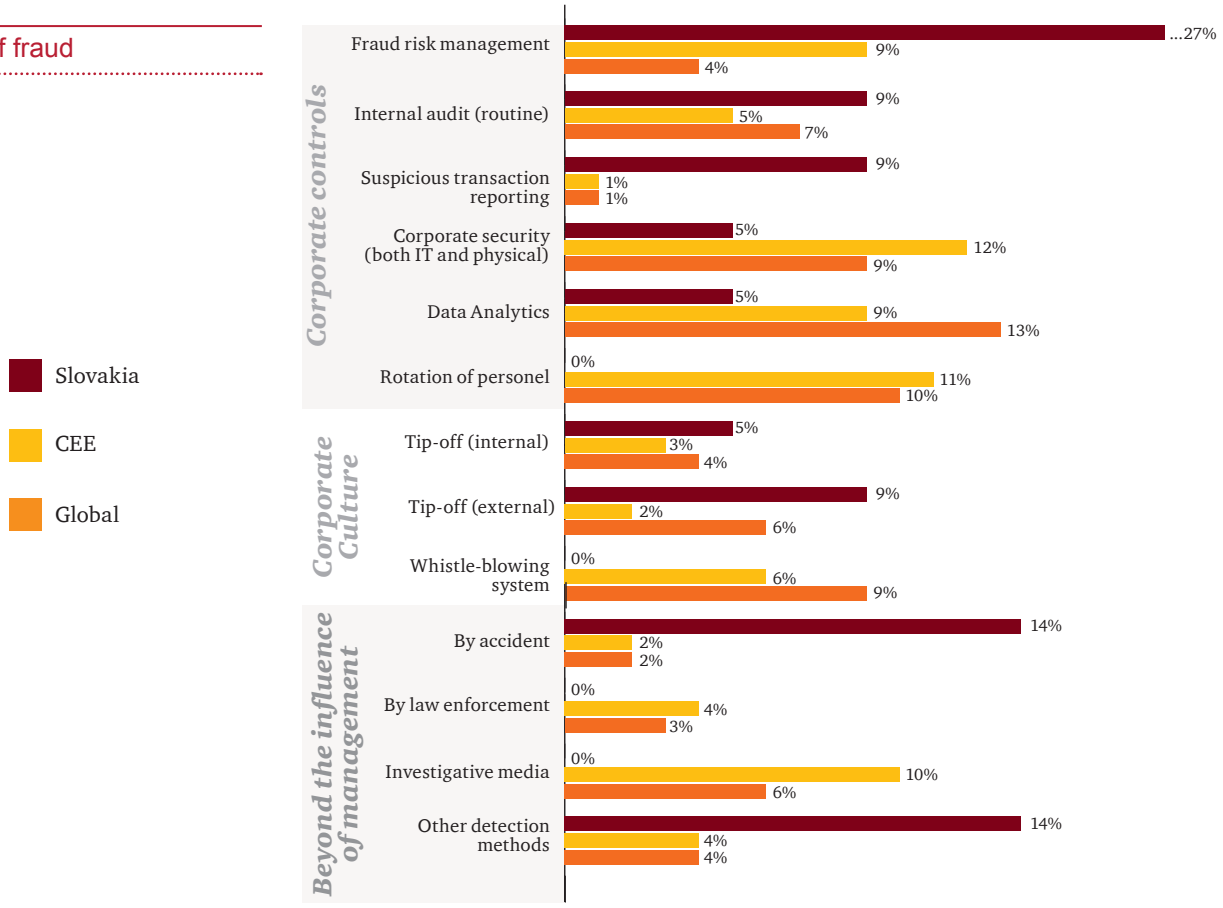
At the same time, out of the possible contributing factors, opportunity is the one most within a company's control. Therefore, a review of procedures in the areas most vulnerable to fraud may be an effective way to reduce the risk of falling victim to fraud.

## *Detection of fraud*

The survey results indicate a different distribution than the global results. In total 27% of Slovak organisations that reported economic crime have detected fraud via Fraud risk management which significantly above the regional and global results (9% and 4% respectively).

Detection by accident reached 14%, while globally the crime survey reported only 2%. This might indicate a potential link to the overall lower occurrence of fraud in Slovakia compared to CEE and global – the number fraud cases could remain undetected by the companies.

Detection of fraud




Numbers are rounded to the nearest whole number

And what's the first reaction of a company when a potential fraud is detected? Most companies resort to internal investigation. Interestingly, almost one fifth waits to see if further indications of potential fraud occur before they react.

**Pavel Jankech**,
Senior Manager in Forensic Technology Services

**Do you think that the measures that companies use to combat fraud are sufficient?**
Currently, companies primarily use preventative measures to combat fraud. This, however, increases the risk that fraud will remain undetected longer. Our experience shows that fraud is usually identified, on average, only after it has already been taking place for two years. The impact of such fraud can be really serious, and it's not just a pure financial loss. A company's reputation, employee morale, or business relationships with business partners are also at risk.

**What would you recommend to companies?**
A robust control environment is an absolute necessity. Nevertheless, it is never 100% bulletproof so we recommend the companies also implement detection mechanisms, such as regular data analytical tests or a continuous fraud detection system. Using detection measures will help a company to identify fraud sooner and thus reduce losses.

**What data test do you have in mind?**
Traditional methods seek to identify suspicious transactions (red-flags) through rule-based testing. Classic examples include round-sum invoices and late-night postings. The challenge is that red-flags are typically not unusual events, and therefore the outputs from the tests are long lists of exceptions with many false-positives, leading to a costly manual investigation. Moreover, these rules are already well known, so the fraudster can easily avoid them.

**How to proceed in these cases?**
Based on our experience, each fraud scheme can be classified into one of several categories. Each of the different types of fraud leaves a specific "footprint" in the data. Using advanced analytical techniques and visualisation, we can identify different patterns of behaviour that correspond to these tracks. This approach can be used proactively to identify potential weak areas of control in the company, or reactively in the investigation of a specific incident.

**What kind of advanced analytical techniques are they?**
These are advanced statistical methods or data mining techniques. These can help identify hidden patterns in the data behaviour. Each of the patterns indicates the behaviour of the supplier or user, and is compared with standard behaviour in the dataset. Unusual or anomalous patterns indicating fraud are subsequently investigated. Using a combination of techniques to visualise the data and detailed knowledge of the company, the investigation should just focus on unusual or anomalous behaviour. The results of detailed investigations shall apply retroactively to increase the accuracy of the search algorithm.

**What data is required for this type of testing?**
During the initial phase of the project we would seek to understand the specifics of the company and its business and its existing control environment to identify key risk areas for fraud. Based on those we would decide where to start looking for fraud. The main sources are typically data from ERP and accounting systems, or actual cash flows gathered directly from bank statements, but also other, less usual sources of data like car GPS records, physical entry access records, or call or network traffic logs can be utilised for analysis.

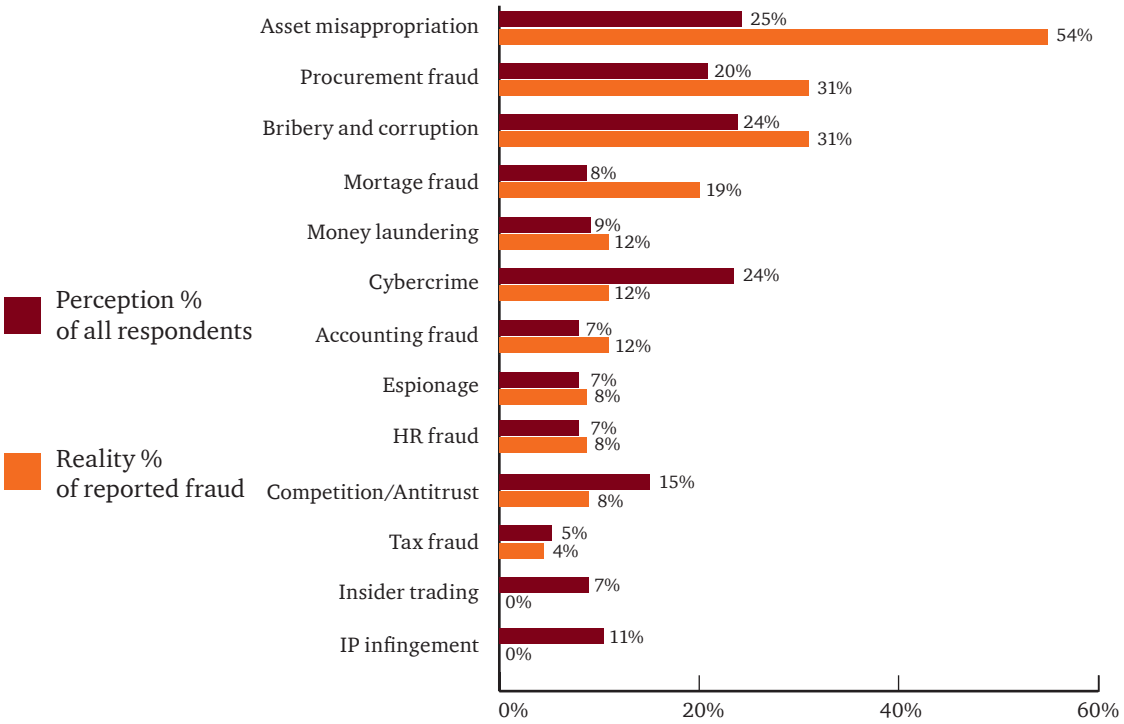
## *Remedial actions*

The survey indicated a clear stance of most companies against fraudsters, both internal as well as external. The occurrence of dismissals of internal perpetrators (100%) is even higher than in the previous survey (82%). This would suggest a high awareness of companies that fraud is costly. Especially in times of economic turmoil, there are few reasons to take fraud lightly. Civil action (38%) is preferred to law enforcement action (25%).

With an external perpetrator, dismissal is obviously not an option. The most preferred option is the termination of the business relationship (67%), with the notification of law enforcement authorities as the second most common action (60%).

# Expectations

We also asked which types of crime companies expect to face in the next 24 months. Please note that the following data depend on the perception of risks by the companies. This is not the same as the real extend of risk. Still, it is interesting to compare the perception of risks with the real occurrence. It would seem that companies underestimate the risk of asset misappropriations in spite of its reported occurrence.



# *Are you a member of our Fraud Forum?*

The Fraud Forum is a platform for sharing the knowledge and experience of managers and professionals dealing with fraud prevention, detection, and forensic investigation in companies. Membership in the Fraud Forum is extended to financial directors and specialists, internal auditors, risk and compliance managers, security and forensic investigation specialists, and company lawyers.

## The Fraud Forum offers

- professional updates and the latest information about trends in fraud prevention, detection and forensic investigation;
- participation in seminars and discussion forums on various topics relating to fraud in companies;
- opportunities to participate in surveys focused on fraud and obtain detailed conclusions and reports from the surveys; and
- opportunities to share knowledge and exchange experience and opinions with other.

Membership in the Fraud Forum platform is free and absolutely flexible – each member can participate in any and all activities that are of interest to him/her. By becoming a member of the Fraud Forum, you will have the opportunity to meet regularly with other members and share your knowledge, experience and ideas with them. We will send you updates, analyses and invitations to events organised by the Fraud Forum.

For registration form please follow the link www.pwc.com/sk/fraud-forum. If you have any questions relating to Fraud Forum platform, please contact **Jana Grošeková at: jana.grosekova@sk.pwc.com**.

# Contact


***Sirshar Qureshi***
Partner, CEE Forensic Leader
+420 251 151 235
sirshar.qureshi@cz.pwc.com

***Michal Kohoutek***
Head of Forensic Services
+420 251 151 231
michal.kohoutek@cz.pwc.com

***Pavel Jankech***
Senior Manager
Forensic Technology Solution
+420 251 151 336
pavel.jankech@cz.pwc.com

***Radoslav Ratkovsky***
Manager
Advisory Services
+421 259 350 585
radoslav.ratkovsky@sk.pwc.com

## *Bratislava*

**PwC, Námestie 1. mája 18, 815 32 Bratislava**
**tel.: +421 (0)2 59350 111, fax: +421 (0)2 59350 222**

## *Košice*

**PwC, Aupark Tower, Protifašistických bojovníkov 11, 040 01 Košice**
**tel.: +421 (0)55 32153 11, fax: +421 (0)55 32153 22**

**www.pwc.com/sk**


### About the Survey

The 2014 Global Economic Crime Survey was completed during September and October 2013. There were 5,128 respondents from 99 countries, including 76 respondents from Slovakia. Of the total number of respondents, 50% were senior executives from their respective organisations, 35% represented listed companies and 54% represented organisations with more than 1,000 employees. www.pwc.com/crimesurvey

pwc


© 2014 PricewaterhouseCoopers Slovensko, s.r.o. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Slovensko, s.r.o., which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.

www.pwc.com/sk/forenzne-sluzby

# *Globálny prieskum hospodárskej kriminality 2014*

## Hospodárska kriminalita je na vzostupe

Správa za Slovensko

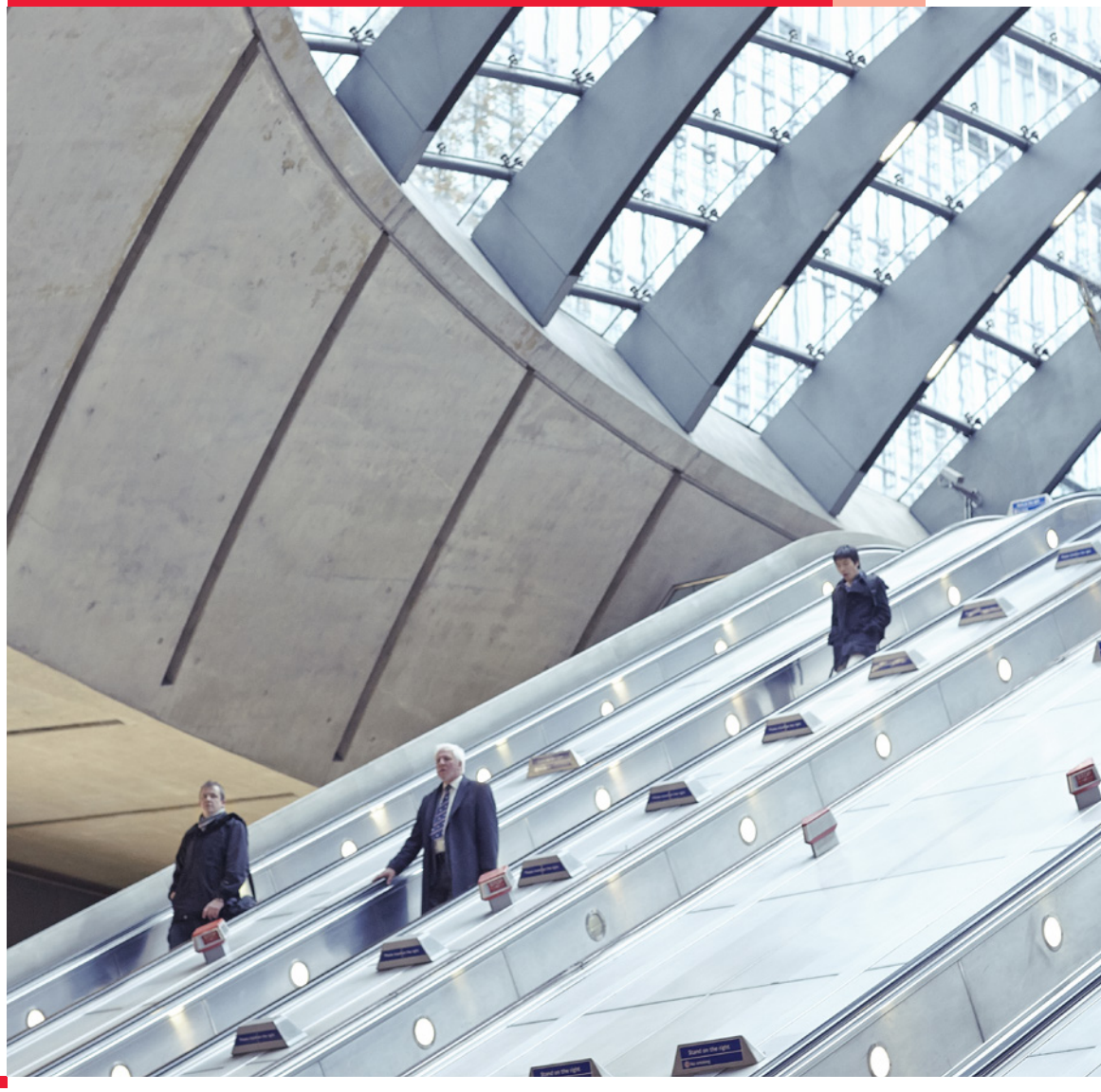
*Vývoj hospodárskej kriminality*

*Nebezpečenstvá kriminality*

*Počítačová kriminalita*

*Podvody v nákupnom procese*

*Korupcia a úplatky*



pwc

# Obsah



***Globálny prieskum hospodárskej kriminality, ktorý uskutočňuje spoločnosť PwC, je najväčším svojho druhu. V ročníku 2014 sa na ňom zúčastnilo 5 128 respondentov z 99 krajín, vrátane 76 reprezentantov zo Slovenska.***

***Zámerom prieskumu nie je len zistiť súčasný stav hospodárskej kriminality, ale aj identifikovať trendy a vnímanie rizík v budúcnosti.***

# Predslov

V príbehu Lewisa Carrolla „Alica za zrkadlom“ srdcová kráľovná vraví: *„Tu, ako vidíte, musíte utekať z celej sily, aby ste sa udržali na tom istom mieste.“* V modernej dobe sa jej slová môžu chápať ako analógia k teórii evolúcie.

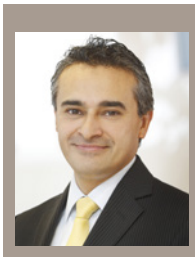
Spisovateľove slová nám tiež môžu slúžiť ako výstižný opis vývoja v oblasti hospodárskej kriminality. Hospodárska kriminalita sa neustále vyvíja a hľadá nové spôsoby svojho prežitia. Firmy musia hľadať stále nové a efektívnejšie cesty ako chrániť svoj majetok, lebo inak by ich evolúcia podvodu predbehla.

Globálny prieskum hospodárskej kriminality, ročník 2014, dáva za pravdu tejto skúsenosti: s hospodárskou kriminalitou sa na Slovensku stretávame čoraz častejšie a jej formy sú čoraz rôznorodejšie. Navyše, ako samostatná kategória hospodárskej kriminality, bol vyčlenený podvod v nákupnom procese. Preto organizáciám odporúčame, aby v tomto zmysle prispôsobili i svoje posudzovanie rizík, ktorým sú vystavené.

Ďalším zaujímavým zistením je nárast nákladov v dôsledku hospodárskej kriminality, nárast podielu podvodov spáchaných sprostredkovateľmi a vo všeobecnosti prísne opatrenia, ktoré firmy uplatňujú voči páchateľom.

Budeme radi, keď si podnikatelia a manažéri našu správu prečítajú a vyvodia z nej závery relevantné pre svoju organizáciu. Spoločnosti, ktoré pôsobia na medzinárodnej úrovni, môžu pre svoje podnikanie využiť ako výsledky celosvetového prieskumu, dostupné na www.pwc.com/crimesurvey, tak aj správy zamerané na konkrétne krajiny, ako je napríklad táto za Slovensko.

Na záver by sme chceli poďakovať všetkým účastníkom prieskumu, ktorí sa s nami podelili o svoje skúsenosti s hospodárskou kriminalitou a svojimi názormi. Naša osobitná vďaka patrí reprezentantom 76 organizácií na Slovensku, ktorí zdieľajú náš názor, že hospodárska kriminalita je príliš nákladná na to, aby sme ju ignorovali.



***Sirshar Qureshi***
Partner zodpovedný za Forenzné služby v CEE
PwC

***Michal Kohoutek***
Líder
Forenzné služby
PwC

# Hlavné zistenia

## Nebezpečenstvá kriminality

**Hospodárska kriminalita je na vzostupe**
Prípady hospodárskej kriminality na Slovensku majú stúpajúcu tendenciu. 34 % respondentov uviedlo, že ich spoločnosť sa za uplynulých 24 mesiacov stretla s hospodárskou kriminalitou. Ide o výrazný nárast v porovnaní so zisteniami prieskumu hospodárskej kriminality z roku 2011 (21 %). Súčasný údaj je podobný zisteniam na regionálnej a globálnej úrovni (38 %, resp. 37 %). Viac ako polovica organizácií (58 %), ktoré sa stretli s hospodárskou kriminalitou, odhaduje celkovú finančnú stratu v jej dôsledku na 100 tisíc amerických dolárov alebo viac.

**Formy kriminality sú čoraz rôznorodejšie**
Najrozšírenejšou formou hospodárskej kriminality je už tradične sprenevera majetku (54 %). Podvodníci však hľadajú nové spôsoby, ako poškodiť spoločnosti. Výskyt rôznych foriem hospodárskej kriminality sa stáva vyrovnanejší. Zaznamenali sme nárast podielu iných foriem hospodárskej kriminality: korupcia a úplatky (31 %), machinácie pri verejnom obstarávaní (31 %), podvody s hypotekárnymi úvermi (19 %), počítačové podvody (12 %), legalizácia príjmov z trestnej činnosti (12 %).

### *Počítačová kriminalita*

**Výskyt**
Z globálneho hľadiska je v súčasnosti pravdepodobnosť, že organizácia bude čeliť počítačovému podvodu, oveľa vyššia než v minulosti. Pokles nahlásených prípadov počítačovej kriminality na Slovensku (12 % v porovnaní so 17% výskytom podľa prieskumu z roku 2011) vyvoláva pochybnosti o schopnosti firiem na Slovensku odhaľovať počítačovú kriminalitu. Miera neidentifikovateľnosti počítačovej kriminality môže byť dokonca vyššia než v ostatných krajinách.

**Riziko počítačovej kriminality**
V obchodnej praxi je stále viac kladený dôraz na využívanie webových aplikácií, vzdialeného prístupu do informačných systémov, prípadně dáta v „cloude“, čo zvyšuje potenciálne riziko počítačovej kriminality.

**Problém odhalenia**
Vo všeobecnosti je počítačová kriminalita nebezpečná v tom, že organizácie, ktoré sú jej obeťou, nemusia zistiť, že sa na nich pácha podvod. Sme presvedčení, že počet „skrytých“ (neidentifikovaných) prípadov počítačovej kriminality je vyšší ako v prípade sprenevery majetku. Je preto veľmi pravdepodobné, že počet skutočných prípadov je oveľa vyšší než počet nahlásených prípadov.

### *Podvody v nákupnom procese*

**Výskyt**
Ide o samostatnú kategóriu hospodárskej kriminality, s ktorou sa na Slovensku stretlo 31 % organizácií, ktoré sa stali obeťou hospodárskej kriminality. Respondenti považujú za najväčšie riziko v tejto oblasti proces výberu dodávateľa.

**Riziká podvodov v nákupnom procese**
Obstarávanie zvyčajne zahŕňa dohodu medzi obchodnými partnermi. Preto je často zložité odhaliť tento typ podvodu. Existujú však spôsoby, ako zmierniť jeho riziká. Napríklad spoločnosti s veľkým počtom obchodných transakcií a dodávateľov môžu na odhalenie potenciálnych podvodov alebo neefektívneho obstarávania využiť pokročilé dátové analýzy.

### *Korupcia a úplatky*

**Riziko korupcie**
31 % organizácií, ktoré sa stretli s podvodmi, uviedlo, že išlo o korupciu a úplatky. V porovnaní s predchádzajúcim prieskumom sme v tejto oblasti zaznamenali nárast o 14 percentných bodov. Korupcia sa v celosvetovom meradle považuje za najväčšie riziko pri podnikaní čo sa týka poškodenia dobrého mena i finančnej straty. Tomuto tvrdeniu dáva za pravdu aj 17. ročník globálneho CEO prieskumu 2014 realizovaného PwC: 69 % generálnych riaditeľov („CEO“) v strednej a východnej Európe sa obáva dopadov korupcie na svoju firmu. Podľa tohto prieskumu predstavuje korupcia a úplatky najväčšiu hrozbu pre rast organizácií v strednej a východnej Európe.

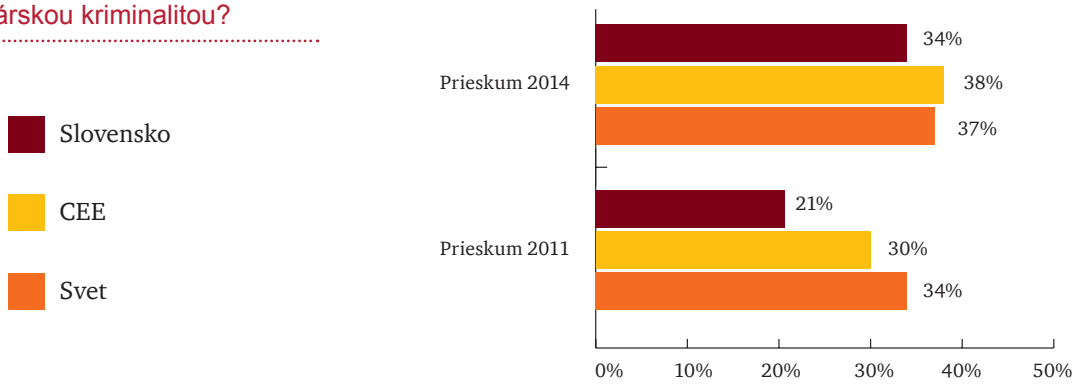
# Hospodárska kriminalita na Slovensku

## Hlavné témy

### Zhoršenie situácie?

V porovnaní s predošlým prieskumom sme zaznamenali nárast nahlásených prípadov hospodárskej kriminality. V roku 2011 bol počet organizácií, v ktorých bola odhalená hospodárska kriminalita (21 %), oveľa nižší než regionálny a globálny priemer (30 %, resp. 34 %). V tohtoročnom prieskume viac než tretina (34 %) respondentov uviedla, že sa vo svojej organizácii za posledných 24 mesiacov stretli s hospodárskou kriminalitou. Tento údaj zodpovedá globálnemu a regionálnemu priemeru, ktorý je 37 %, resp. 38 %.

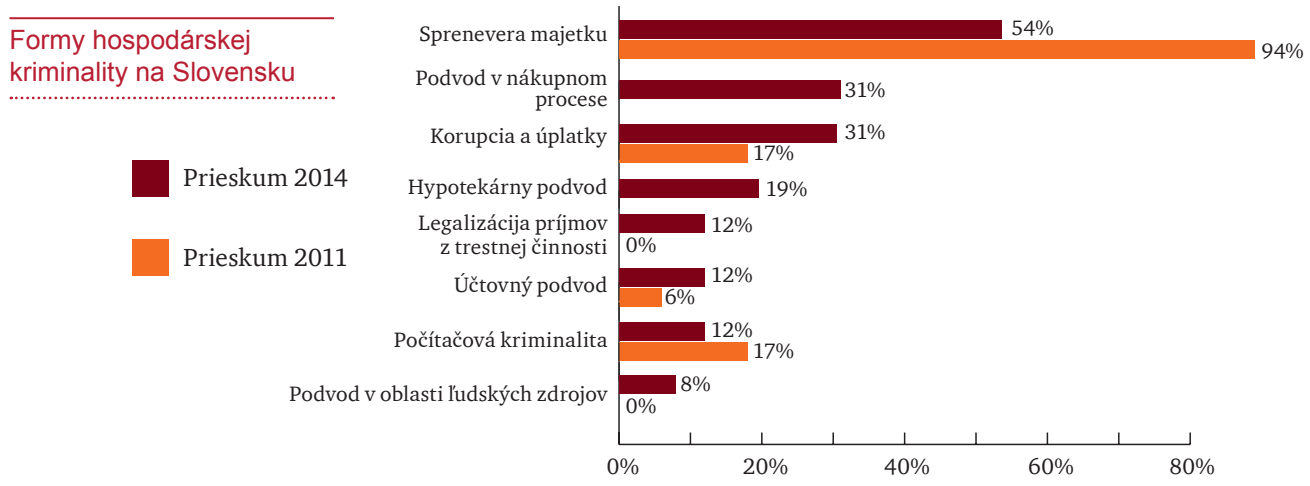
Koľko spoločností sa stretlo s hospodárskou kriminalitou?




Aby sme pochopili, čo stojí za týmto nárastom, pozrime sa na jednotlivé kategórie podvodov.

# *Veľká rozmanitosť hospodárskej kriminality*

Spôsoby útoku na majetok organizácií sú čoraz „kreatívnejšie“. Relatívny podiel sprenevery majetku, ako tradične najbežnejšieho a najjednoduchšieho typu hospodárskej kriminality, klesá v prospech iných „tvorivých“ foriem podvodov.




Od nášho prvého globálneho prieskumu v roku 2001 zotrvávajú na čele rebríčka tri typy kriminality – sprenevera majetku (zvyčajne s veľkým odstupom), úplatky a korupcia a účtovné podvody. V roku 2011 sme zaradili počítačovú kriminalitu ako osobitnú kategóriu, ktorá sa so 17 % ihneď zaradila do čela rebríčka spoločne s korupciou a úplatkami a účtovnými podvodmi.

Tento rok sme pridali ďalšiu novú kategóriu – podvod v nákupnom procese – ktorá sa do popredia dostáva vďaka súčasnému trendu outsourcingu a organizačného prepojenia. Percento respondentov uvádzajúcich túto formu ekonomickej kriminality je významné (31 %). Tým sa táto aktivita dostala medzi najčastejšie podvody na Slovensku.

Výskyt ďalších dvoch nových kategórií – podvodov s hypotekárnymi úvermi (19 %) a podvodov v oblasti ľudských zdrojov (8 %) je na Slovensku takisto významný a nie je prekvapením, že dramaticky vzrástol celkový počet organizácií, ktoré nahlásili výskyt hospodárskej kriminality.

Najvýznamnejšie zmeny v porovnaní rokov 2011 a 2014 nastali vo výskyte legalizácie príjmov z trestnej činnosti (nárast z 0 % na 12 %) a sprenevery majetku (pokles z 94 % na 54 %). Aj tieto fakty podporujú naše zistenie, že tradičné spôsoby podvodu, ako je sprenevera majetku, majú na hospodárskej trestnej činnosti stále ešte významný podiel, avšak ustupujú v prospech „modernejších“ typov podvodov, respektive páchatelia podvodov využívajú sofistikovanejšie a teda aj ťažšie odhaliteľné postupy.

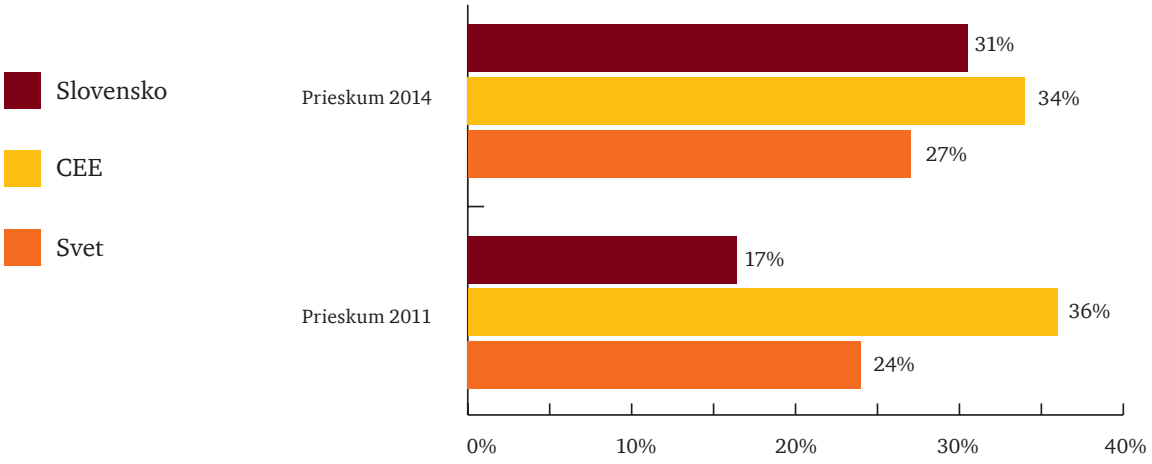
Je takisto veľmi pravdepodobné, že relatívny výskyt podvodov ako je korupcia, počítačová kirminalita a podvody v nákupnom procese, je dokonca vyšší. Tieto typy podvodov sa totiž ťažko odhaľujú. V rámci našich forenzných projektov sme sa stretli s početnými prípadmi dlhodobých podvodných aktivít, ktoré dotknutá organizácia odhalila len náhodne.

Preto je nevyhnutné, aby organizácie venovali dostatočnú pozornosť schémam podvodov, s ktorými by sa mohli stretnúť. Samotná kontrola peňažných prostriedkov a iného fyzického majetku nemusí byť dostačujúca.

## *Korupcia a úplatky*

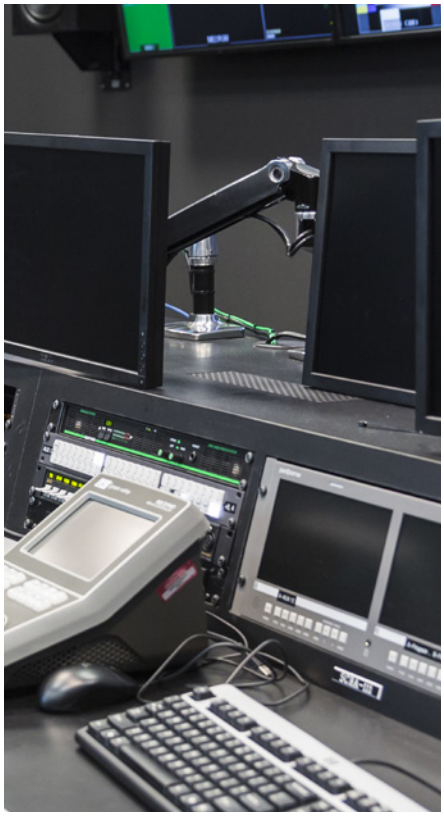
V posledných rokoch sa na Slovensku korupcia opodstatnene stala témou mnohých verejných diskusií. Korupcia a úplatky sú najzávažnejšou kategóriou hospodárskej kriminality a považujú sa za najväčšie globálne riziko pri podnikaní tak kvôli riziku poškodenia dobrého mena ako i finančnej straty. Čo sa týka výskytu, je druhou najčastejšie uvádzanou formou hospodárskej kriminality na Slovensku (31 %) a treťou v celosvetovom meradle (podľa prieskumu hospodárskej kriminality 2014: 27 %). Stredná a východná Európa spolu s Afrikou sú regiónmi s najväčším výskytom korupcie.

Podiel korupcie a uplácania na spáchaných podvodoch




17. ročník globálneho CEO prieskumu ukázal, že povedomie o korupcii rastie. 69 % CEO v strednej a východnej Európe sa obáva dopadov korupcie na svoju firmu.

Podľa prieskumu hospodárskej kriminality, 20 % respondentov na Slovensku uviedlo, že za uplynulých 24 mesiacov sa už stretli s prípadmi, keď sa od ich organizácie žiadal úplatok. 41 % respondentov je presvedčených, že v dôsledku poskytnutia úplatku konkurenčnou organizáciou, ich firma stratila obchodnú príležitosť.



## Podvod v nákupnom procese

Podvod v nákupnom procese bol v roku 2014 zaradený po prvýkrát ako samostatná kategória hospodárskej kriminality v rámci prieskumu. 31 % spoločností na Slovensku, ktoré sa už stretli s hospodárskou kriminalitou, uviedlo, že ich organizácia zaznamenala aspoň jeden prípad podvodu v nákupnom procese.

Uvedený výskyt podvodov v oblasti nákupov bol omnoho vyšší, než sme očakávali. Keďže odhalenie tohto typu podvodu nie je ľahké, je veľmi pravdepodobné, že jeho výskyt je ešte vyšší.

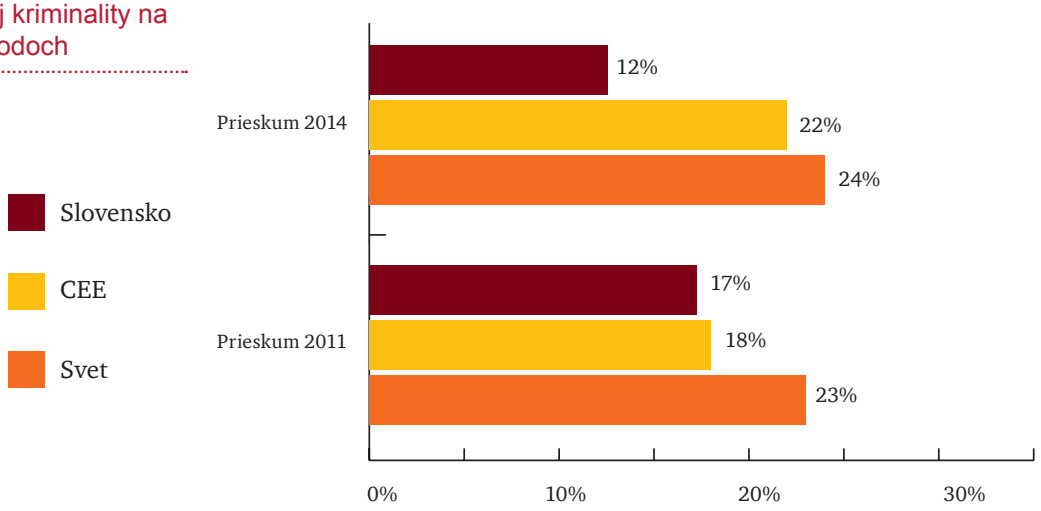
Podvod v nákupnom procese sa zaradil na druhé až tretie miesto (spolu s korupciou a úplatkami) ako najčastejšie uvádzaná forma hospodárskej kriminality na Slovensku. Najväčšie riziko súvisí s procesom výberu a zazmluvnenia dodávateľa.

Všeobecne povedané, ak organizácia hľadá služby, tovar alebo majetok v externom prostredí, existuje tu riziko podvodov. Rastúce vzájomné prepojenie podnikateľských subjektov a stále bežnejší outsourcing vystavuje organizácie vyššiemu riziku podvodov pri obstarávaní, než tomu bolo v minulosti. Navyše, spôsobov, ako spáchať podvod pri obstarávaní, je veľmi veľa. Tento typ sa preto radí k podvodom, ktoré sa najťažšie odhaľujú a vyšetrujú.

## Počítačová kriminalita

Je zaujímavé, že podľa zistení je podiel počítačovej kriminality v slovenských spoločnostiach dosť výrazne pod regionálnym a globálnym priemerom. Jej 12% podiel na celkovej hospodárskej kriminalite je dokonca nižší než podiel zistený v predchádzajúcom prieskume z roku 2011 (17 %).

Podiel počítačovej kriminality na spáchaných podvodoch




No i napriek nízkemu počtu nahlásených skutočných prípadov počítačovej kriminality takmer jedna štvrtina respondentov (24 %; pozri graf na str. 14) očakáva, že počas nastávajúcich 24 mesiacov sa najmenej raz stretnú s počítačovým podvodom.

Toto zistenie vyvoláva podozrenie, že medzi odhaleným a skutočným výskytom počítačovej kriminality existuje určitá medzera. Nie je jasné, prečo podiel počítačovej kriminality na Slovensku, krajine vyspelej a s vysokou koncentráciou používania počítačov, predstavuje len polovicu podielu zaznamenaného v iných krajinách. Preto sa domnievame, že spoločnosti na Slovensku čelia riziku v dôsledku nedostatku potrebných schopností na odhalenie (a prevenciu) počítačovej kriminality. Musíme však mať na mysli skutočnosť, že takmer jedna štvrtina respondentov je toho názoru, že im hrozí riziko počítačového podvodu a jeho výskyt považujú v nasledujúcich 24 mesiacoch za pravdepodobný.

Moderná spoločnosť sa snaží využívať plný potenciál technológií a dávať svojim zamestnancom viac slobody. Ľudia pracujú z domu s využitím svojich vlastných inteligentných zariadení pripojených ku cloudu, počas dovolenky odpovedajú na e-maily z internetových kaviarní alebo kontrolujú dokumenty počas čakania na letiskách. Podstatne sa tak rozširuje oblasť, ktorú je treba chrániť a je nutné sa vysporiadať s prostredím, ktoré nie je úplne pod kontrolou firmy.

Aj to je dôvod, prečo sa zásadným spôsobom mení prístup k počítačovej bezpečnosti:

- ponímanie 90. rokov – reaguj až po prelomení bezpečnosti
- postoj na prelome storočí – priprav sa na prelomenie bezpečnosti
- a teraz – predpokladaj, že k prelomeniu už došlo, alebo sa tak práve deje

Nie je otázkou, či sa firma stane cieľom počítačoveho útoku, ale kedy a ako k tomu dôjde. Úspešné spoločnosti si stanovujú priority ochrany svojich kľúčových dát pred organizovanými útočníkmi podľa ich významu. V globálnom prostredí ide pritom ako o dáta prúdiace vo vnútri spoločnosti, tak aj o informácie od obchodných partnerov a ďalších zúčastnených strán alebo k nim.

Viac ako polovica respondentov uviedla, že za posledných 24 mesiacov začala počítačovú kriminalitu viac vnímať. Najčastejším dôvodom k znepokojeniu v oblasti počítačovej kriminality sú krádeže v oblasti duševného vlastníctva, osobných údajov alebo poškodenia dobrého mena a obchodnej značky.

Pre dokreslenie môžeme uviesť prípad, na ktorom sme v minulosti pracovali. Zamestnanci oddelenia IT jednej veľkej spoločnosti pôsobiacej v energetickom priemysle objavili v serverovni počítač, ktorý nebol v majetku spoločnosti a do ktorého nemali prístup. Zároveň začalo dochádzať k výpadkom internetového pripojenia. Tie boli kvôli nutnosti prístupu do internetového bankovníctva pre spoločnosť veľkým problémom. Vyšetrovaním sme zistili, akú funkciu mal neznámy počítač – jeden z administrátorov IT viedol súkromný internetový obchod, a zneužíval k tomu zdroje spoločnosti. Firma nebola schopná overovať platby v internetovom bankovníctve. Činnosť tohoto zamestnanca tak ohrozila chod celej spoločnosti.

**Tomáš Kuča,** Partner oddelenia Riadenia rizík, ktoré sa špecializuje na oblasť počítačovej bezpečnosti

**Nie sú slová ako počítačová kriminalita alebo počítačová bezpečnosť len ďalšími módnymi výrazmi?**
Sú to názvy pre súčasný fenomén vo svete informačných technológií. Nárast počítačovej kriminality je nesporný, čoho dôkazom sú tisíce prípadov, ktoré sa neustále okolo nás vyskytujú. Počítačová bezpečnosť predstavuje preventívne opatrenia vyvolané touto situáciou.

**Čo sa v tejto oblasti zmenilo za posledné roky?**
V minulosti organizácie reagovali až potom, ako došlo k prípadu počítačovej kriminality. V lepších prípadoch budovali svoju ochranu podľa očakávaného výskytu v budúcnosti. Najvhodnejším prístupom pre vypracovanie zásad počítačovej bezpečnosti je predpokladať, že k jej porušeniu práve došlo.

Zmenili sa páchatelia, čo znamená, že používajú sofistikovanejšie a odolnejšie metódy, zameriavajú sa na získanie špecifických informácií na strategické účely, pracujú po celom svete, konajú v rámci organizovaných štruktúr a niektorí z nich aj v mene štátu.

**Čo môžeme spraviť pre zlepšenie situácie?**

- Obsadiť pozíciu lídra pre informačnú bezpečnosť s pôsobnosťou vo vrcholových štruktúrach organizácie.
- Presne špecifikovať úlohy a zodpovednosti v tejto oblasti.
- Vytvoriť tím zodpovedný za riešenie počítačových útokov.
- Investovať do zvýšenia počítačových zručností zamestnancov.
- Zabezpečiť spoluprácu s expertmi na počítačovú kriminalitu.

### *Dopad hospodárskej kriminality*

Žiadna debata o hospodárskej kriminalite by nebola úplná bez pokusu vyčísliť dopad podvodov. Koniec koncov aktivity realizované spoločnosťami na obmedzenie podvodov musia prinášať výsledky, aby obhájili svoju existenciu.

Viac než polovica respondentov na Slovensku (58 %), ktorí sa už stretli s hospodárskou kriminalitou uviedla, že ich organizácia utrpela stratu najmenej 100 tisíc amerických dolárov. Takúto stratu uvádzajú organizácie, ktoré sa o riešenie hospodárskej kriminality zaujímajú a snažia sa jej zabrániť a odhaľovať ju. O čo vyššie by boli straty z hospodárskej kriminality, ak by spoločnosť nekonala a nezavádzala opatrenia proti jej výskytu?

Nie sú to len finančné straty, ale aj ďalšie negatívne dopady, ktoré kriminalita prináša. Ako najväčšiu nefinančnú ujmu uvádzajú organizácie poškodenie dobrého mena a morálky zamestnancov.

V tejto súvislosti by sme chceli poukázať na skutočnosť, že negatívny dopad na morálku zamestnancov môže viesť k sekundárnym činom, ako sú podvody spáchané frustrovanými a demotivovanými zamestnancami. Tí, čo sa na tento skutok podujali po prvýkrát, často svoj čin zdôvodňujú slovami: „robia to všetci“ alebo „zaslúžia si to“!

# Riadenie rizika podvodov

### *Kto sú páchatelia podvodov?*

Na základe skúseností respondentov sme sa snažili vypracovať profil páchateľa najvážnejších foriem hospodárskej kriminality.
Medzi výskytom podvodov páchaných internými a externými páchateľmi nie je rovnováha (31 % a 58 %).

Nie je prekvapením, že na najzávažnejších interných podvodoch sa vo väčšej miere podielajú zamestnanci na stredných a vyšších manažérskych pozíciách než zamestnanci na nižších pozíciách. Typickým páchateľom podvodu je muž vo veku 31 až 40 rokov, ktorý v organizácii pracuje 6 až 10 rokov.

Najvážnejšie externé podvody najčastejšie páchajú zákazníci, a to ako na Slovensku (53 %) tak aj celosvetovo (32 %). Ako sme už uviedli v správe pre rok 2011, odporúčame organizáciám, aby pokračovali vo svojom úsilí v oblasti prevencie - je potrebné spoznať svojich zamestnancov a budúcich obchodných partnerov skôr, než s nimi uzatvoríme zmluvný vzťah; je to menej nákladné než riešiť následky podvodu.

### *Prevencia podvodov*

Čo vedie ľudí k spáchaniu podvodu? Náš prieskum ukázal, že veľký náskok pred ostatnými dôvodmi má u interných páchateľov jednoducho príležitosť. Súčasne však v porovnaní s ostatnými možnými faktormi, tento má organizácia najviac pod kontrolou.

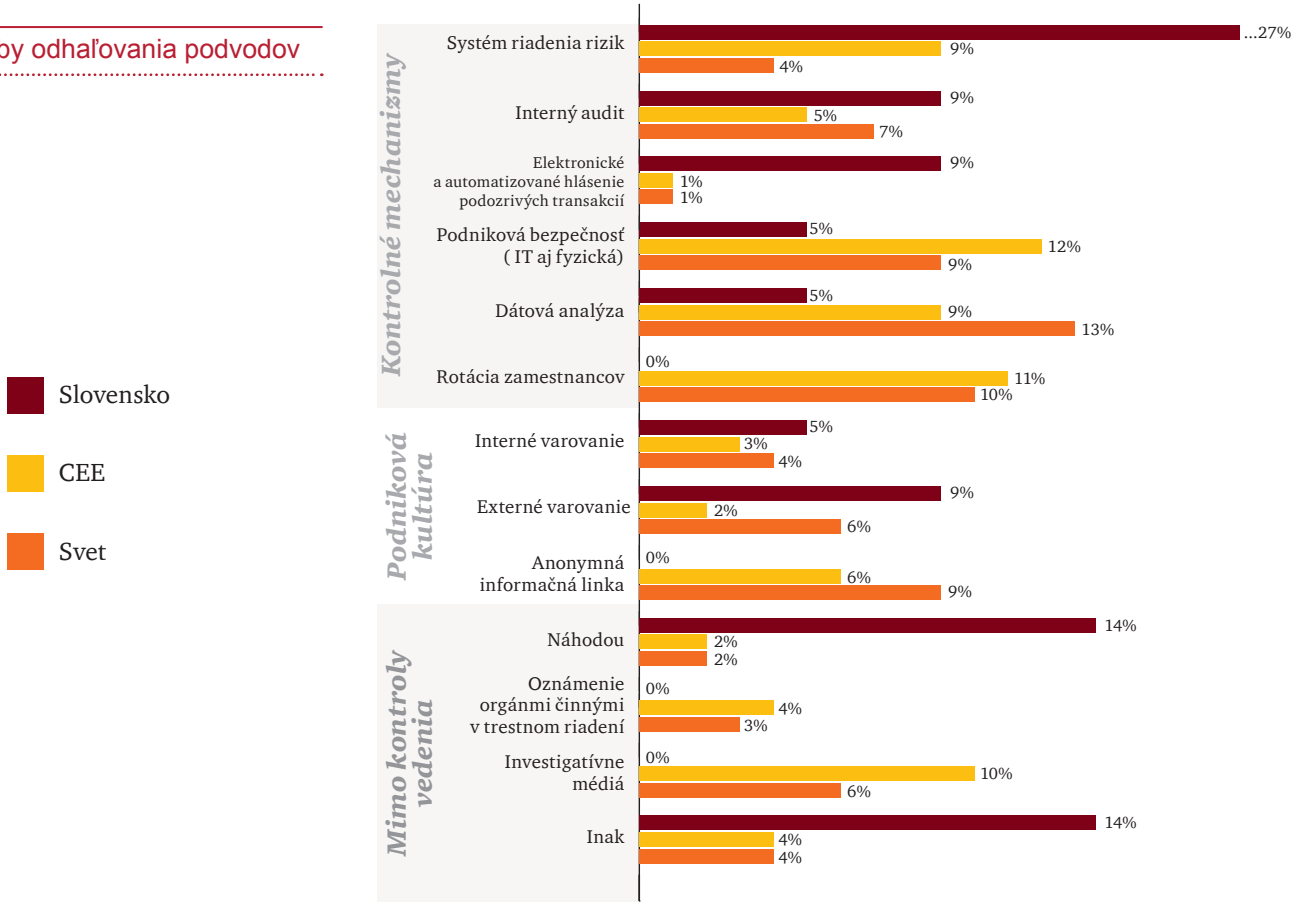
Preverenie postupov v oblastiach, ktoré sú najviac vystavené hrozbe podvodu, by preto malo byť efektívnym spôsobom, ako znížiť riziko, že sa organizácia stane obeťou podvodu.

## *Odhalenie podvodu*

Výsledky prieskumu na Slovensku sa nezhodujú s globálnymi zisteniami. Celkovo 27 % slovenských spoločností, ktoré sa stali obeťou podvodov, odhalilo hospodársky podvod vďaka systému riadenia rizík, čo je výrazne viac v porovnaní s regionálnymi a globálnymi výsledkami (9 %, resp. 4 %).

Náhodné odhalenie podvodov dosiahlo 14 %, zatiaľ čo celosvetový prieskum uvádza len 2 %. Táto skutočnosť môže súvisieť s celkovo nižším výskytom podvodov na Slovensku v porovnaní s krajinami strednej a východnej Európy a v globálnom meradle – mnohé prípady podvodov mohli zostať neodhalené.

### Spôsoby odhaľovania podvodov




Hodnoty sú zaokrúhlené na najbližšie celé čísla

Aká je prvá reakcia organizácií po odhalení potenciálneho podvodu? Väčšina z nich sa rozhodne pre interné vyšetrovanie. Je zaujímavé, že takmer jedna pätina spoločností počká, či sa objavia ďalšie indikátory podvodu a až potom podnikne kroky.

**Pavel Jankech**, Senior manažér oddelenia Forenzných technológií

**Myslíte si, že opatrenia, ktoré organizácie uplatňujú v boji proti podvodom, sú dostatočné?**
V súčasnosti využívajú organizácie najmä preventívne opatrenia, čo však zvyšuje riziko, že podvod zostane dlhšiu dobu neodhalený. Naše skúsenosti ukazujú, že podvody sa v priemere odhalia až po dvoch rokoch páchania. Dopad takýchto podvodov môže byť veľmi vážny a nespočíva len vo finančnej strate. Riziku čelí aj meno organizácie, morálka zamestnancov, alebo vzťahy s obchodnými partnermi.

**Čo by ste odporúčali organizáciám?**
Absolútnou nevyhnutnosťou je dôsledné kontrolné prostredie. Keďže ani toto nie je stopercentne spoľahlivé, odporúčali by sme, aby organizácie zaviedli mechanizmy na odhaľovanie podvodov, ako sú napríklad pravidelné analytické dátové testy alebo systém priebežného odhaľovania podvodov. Uplatnenie opatrení na odhaľovanie podvodov pomôže organizácii identifikovať podvod skôr a zároveň zabezpečí zníženie strát.

**Aké dátové testy máte na mysli?**
Tradičné metódy sa snažia identifikovať podozrivé operácie (varovné signály) pomocou testovania definovaných pravidiel („rule-based testing“). Klasickými príkladmi sú faktúry na okrúhle sumy a oneskorené účtovanie. Výzvou je, že varovné signály zvyčajne nie sú neobvyklé udalosti, a preto výstup z testov je dlhý zoznam výnimiek s množstvom falošných hlásení, ktoré vedú k nákladnému manuálnemu vyšetrovaniu. Navyše tieto zásady sú všeobecne známe a podvodník ich môže ľahko obísť.

**Ako postupovať v takýchto prípadoch?**
Zo skúseností vieme, že každú schému podvodu je možné zaradiť do jednej z viacerých kategórií. Každý z týchto typov podvodov zanecháva v údajoch špecifickú „stopu“. Použitím pokročilých analytických techník a vizualizácií je možné identifikovať rozličné vzorce správania, ktoré môžu korenšpondovať s týmito stopami. Tento prístup sa dá využiť proaktívne, na identifikovanie potenciálnych slabých miest v kontrolných mechanizmoch organizácie, alebo reaktívne, pri vyšetrovaní konkrétneho prípadu.

**Aké sú pokročilé analytické techniky?**
Ide o pokročilé štatistické modely a metódy data miningu.
To umožní identifikovať skryté súvislosti v skúmaných dátach. Každý zo vzorov indikuje správanie sa dodávateľa alebo užívateľa, ktoré je následne porovnané so štandardným, očakávaným vzorom. Nezvyčajné alebo anomálne vzory indikujú možný podvod a sú následne prešetrené. Použitím kombinácie techník na vizualizáciu dát a detailného poznania spoločnosti by sa vyšetrovanie malo zamerať iba na nezvyčajné a anomálne dátové indície. Výsledky z podrobného vyšetrovania sú potom retrospektívne aplikované na zvýšenie presnosti vyhľadávacieho algoritmu.

**Aké údaje sú potrebné pre tento typ testovania?**
V počiatočnej fáze projektu by sme sa mali snažiť spoznať špecifiká spoločnosti, jej podnikania a kontrolného prostredia, aby sme mohli identifikovať rizikové oblasti z pohľadu podvodov. Na základe tohto skúmania, sa rozhodneme, kde hľadať podvod. Hlavným zdrojom sú bežné údaje z podnikových informačných systémov, účtovných systémov alebo aktuálny cash flow, získaný priamo z bankových výpisov. Pre dátovú analýzu môžu byť použité aj ďalšie, menej obvyklé zdroje ako napríklad dáta z GPS automobilov, záznamy o vstupoch do budov, alebo sieťové logy.

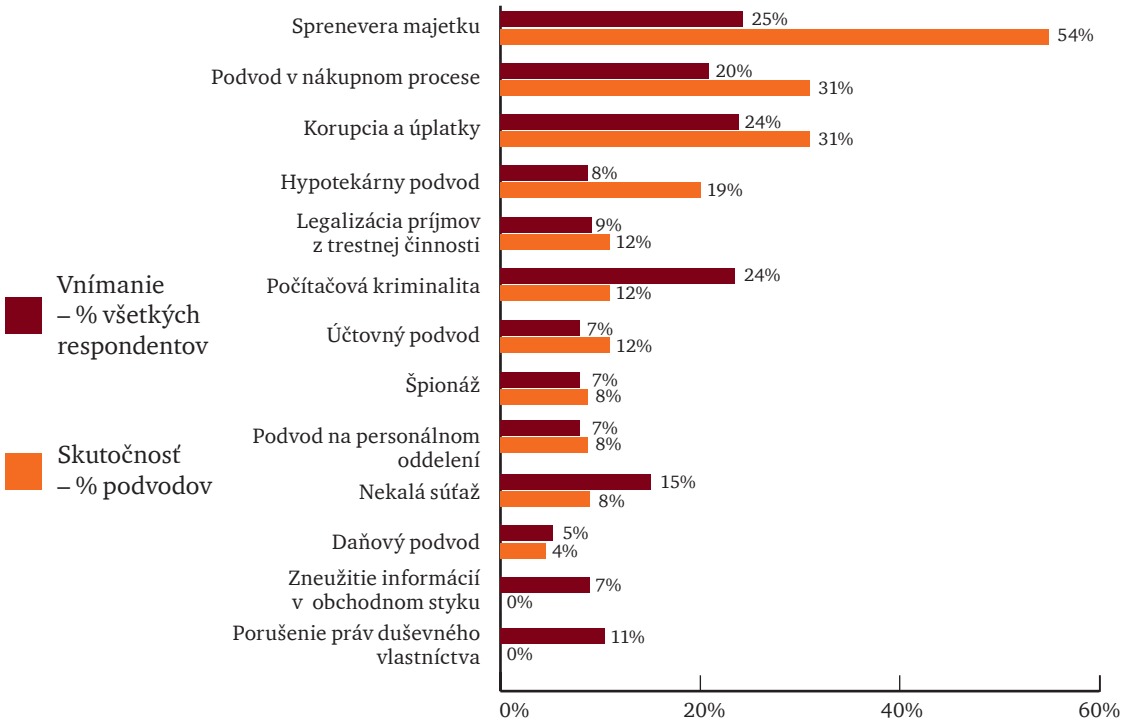
## *Nápravné opatrenia*

Výsledky prieskumu poukázali na jasný postoj väčšiny spoločností voči páchateľom, tak interným ako aj externým. Rozviazanie pracovného vzťahu ako opatrenie pri odhalení podvodu internými páchateľmi uviedlo 100 % respondentov, čo predstavuje nárast oproti zisteniam z predchádzajúceho prieskumu (82 %). Toto zistenie naznačuje, že organizácie si uvedomujú, že podvody sú nákladné. Najmä v časoch hospodárskej nestability je len málo dôvodov na to, aby sa podvody brali na ľahkú váhu. Občiansko-právne konanie (38 %) je uprednostňované pred trestným konaním (25 %).

Prepustenie externého páchateľa ako alternatíva neprichádza do úvahy. V tomto prípade sa najčastejšie uplatňuje ukončenie obchodného vzťahu (67 %), oznámenie orgánom činným v trestnom konaní je druhou najčastejšie uplatňovanou alternatívou (60 %).

# Očakávania

Respondentov sme sa ešte spýtali, akým typom hospodárskej kriminality budú podľa ich názoru čeliť ich organizácie počas nastávajúcich 24 mesiacov. Upozorňujeme, že nasledujúce údaje sú závislé na vnímaní rizika jednotlivými organizáciami, ktoré nie je zhodné so skutočným rozsahom výskytu rizika. Je však zaujímavé porovnať vnímanie rizík s ich skutočným výskytom. Zdá sa, že spoločnosti podceňujú riziko sprenevery majetku i napriek jeho uvádzanému výskytu.



# *Ste členom nášho*

# *Fraud Forum?*

Fraud Forum je platforma pre zdieľanie znalostí a skúseností manažérov a odborníkov, ktorí sa zaoberajú prevenciou, odhaľovaním a vyšetrovaním podvodov v organizáciách. Členmi Fraud Forum sa môžu stať finanční riaditelia a pracovníci finančných oddelení, interní audítori, manažéri rizík a compliance, špecialisti zaoberajúci sa bezpečnosťou či vyšetrovaním podvodov a podnikoví právnici.

## Fraud Forum svojim členom ponúka:

- získanie najnovších odborných informácií a aktuálnych správ o novinkách a trendoch v oblasti prevencie, detekcie a vyšetrovaní podvodov,
- účasť na seminároch a diskusných fórach o rôznych témach spojených s podvodmi v organizáciách,
- možnosť zapojiť sa do prieskumov súvisiacich s problematikou podvodov a získať podrobné závery a výsledky týchto prieskumov,
- zdieľanie znalostí a výmenu skúseností a názorov s ostatnými členmi.

Členstvo v platforme Fraud Forum je bezplatné a úplne flexibilné – každý člen sa môže zúčastňovať tých aktivít, ktoré sú preňho zaujímavé. Pokiaľ sa stanete členom Fraud Forum, získate možnosť sa pravidelne stretávať s ďalšími členmi, zdieľať s nimi svoje znalosti, skúsenosti a nápady. Budeme Vám zasielať aktuálne informácie, analýzy a pozvánky na semináre, ktoré Fraud Forum uskutočňuje.

Registračný formulár nájdete na **www.pwc.com/sk/fraud-forum**. Akékoľvek prípadné dotazy týkajúce sa tejto platformy Vám rada zodpovie **Jana Grošeková: jana.grosekova@sk.pwc.com**.

# Kontakt


***Sirshar Qureshi***
Partner zodpovedný
za Forenzné služby v CEE
+420 251 151 235
sirshar.qureshi@cz.pwc.com

***Michal Kohoutek***
Líder Forenzných služieb
+420 251 151 231
michal.kohoutek@cz.pwc.com

***Pavel Jankech***
Senior manažér
Forenzné technológie
+420 251 151 336
pavel.jankech@cz.pwc.com

***Radoslav Ratkovský***
Manažér
Poradenské služby
+421 259 350 585
radoslav.ratkovsky@sk.pwc.com


## *Bratislava*


**PwC, Námestie 1. mája 18, 815 32 Bratislava**
**tel.: +421 (0)2 59350 111, fax: +421 (0)2 59350 222**


## *Košice*


**PwC, Aupark Tower, Protifašistických bojovníkov 11, 040 01 Košice**
**tel.: +421 (0)55 32153 11, fax: +421 (0)55 32153 22**


**www.pwc.com/sk**

### O prieskume

Globálneho prieskumu hospodárskej kriminality 2014 sa počas septembra a októbra 2013 zúčastnilo 5 128 respondentov z 99 krajín, vrátane 76 respondentov zo Slovenska. Z celkového počtu respondentov 50 % boli vedúci pracovníci príslušných organizácií, 35 % reprezentovalo spoločnosti kótované na burze a 54 % organizácie s viac ako 1 000 zamestnancami.
**www.pwc.com/crimesurvey**

pwc

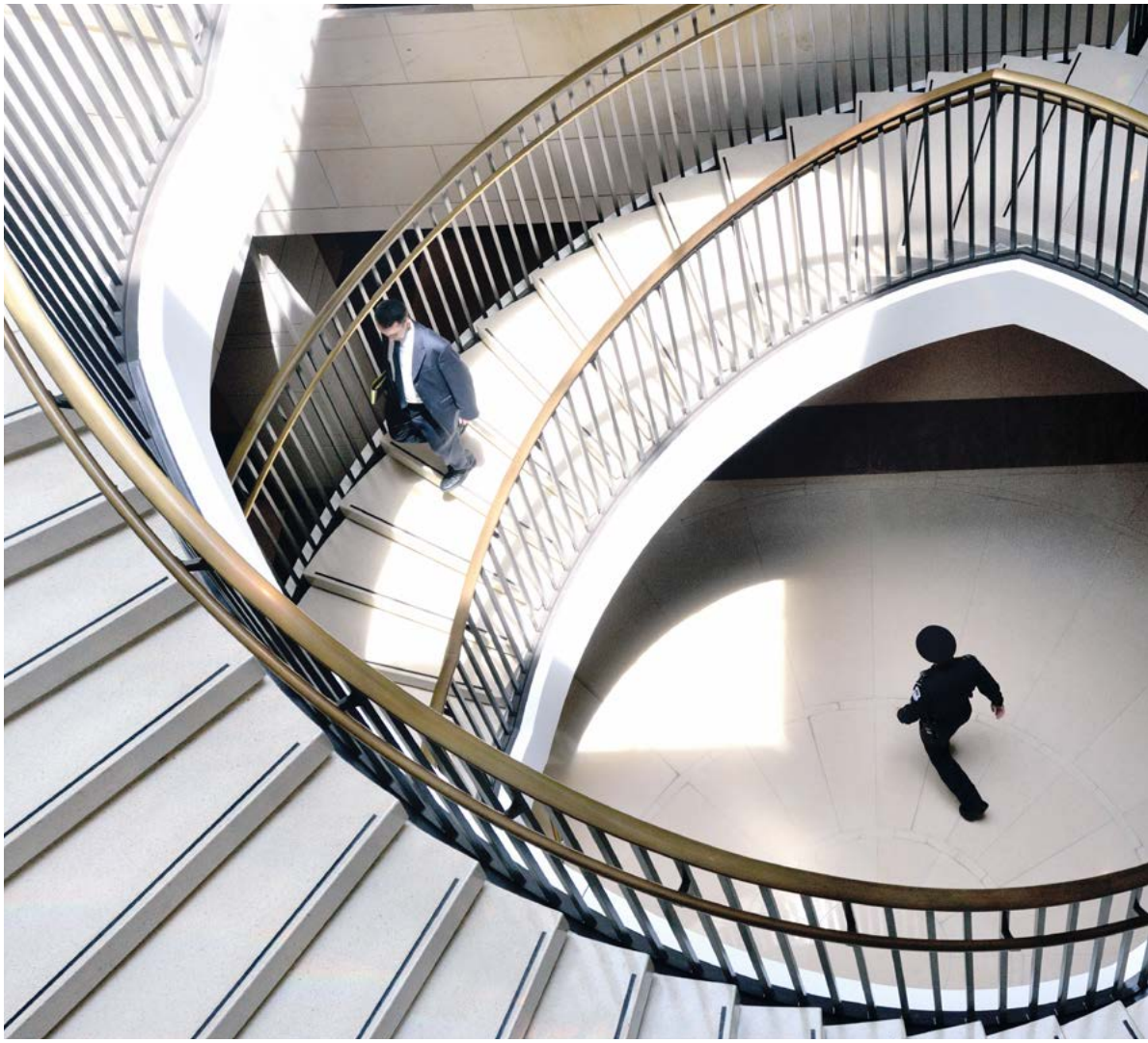

© 2014 PricewaterhouseCoopers Slovensko, s.r.o. Všetky práva vyhradené. Názov „PwC“ v tomto dokumente označuje spoločnosť PricewaterhouseCoopers Slovensko, s.r.o., ktorá je členom siete firiem PricewaterhouseCoopers International Limited, z ktorých každá je samostatným a nezávislým právnym subjektom.

# *Global Economic Crime Survey 2014*

## Resultat från Sverige

*För sjunde gången har PwC genomfört en omfattande global enkät kring ekonomiska oegentligheter. I denna rapport sammanfattar och kommenterar vi de svenska respondenternas svar.*

*Februari 2014*



pwc

*www.pwc.se/forensic*

# Introduktion

Ekonomiska oegentligheter drabbar alla typer av företag, organisationer och branscher och orsakar omfattande direkta och indirekta skador. Respondenterna i enkäten pekar på att förövarna till övervägande del utgörs av anställda, ofta i förtroendepositioner med omfattande befogenheter.

Att anställda är i majoritet bland förövarna gör dock att ekonomiska oegentligheter i stor utsträckning går att förebygga och att riskerna kan påverkas genom hur en verksamhet styrs och organiseras.

Ett bra förebyggande arbete, som exempelvis riskanpassade kontroller och adekvata metoder att utreda incidenter, medför ofta även andra positiva effekter än ren skadebegränsning.

***Värt att notera kring de svenska respondenternas svar:***

- Andelen som uppger att de har drabbats av ekonomiska oegentligheter närmar sig globala nivåer – en trend som håller i sig från tidigare års enkäter.
- Korruption och mutor uppges vara den näst vanligaste formen av oegentlighet – en markant ökning från tidigare enkäter och nu högre rankad jämfört med de globala respondenterna.
- En befarad hotbild befästs: en tredjedel av de svenska respondenterna, och hälften av de globala respondenterna, uppfattar att risken för att utsättas för IT-relaterad brottslighet har ökat och ytterst få uppfattar att risken har minskat.
- Riskanalyser, en fundamental del av det förebyggande arbetet, är fortfarande ett gravt eftersatt område vilket tydligt framgår vid en jämförelse med de globala respondenterna.

*Årets enkät baseras på svar från 5 128 respondenter i form av ledande befattningshavare i 99 länder. Den globala enkäten omfattar 91 respondenter i Sverige huvudsakligen verksamma i noterade och onoterade företag men även respondenter i offentlig sektor och offentligt ägda bolag. På nordisk basis omfattar den globala enkäten 335 respondenter. Den globala rapporten finns att ladda ned från* ***www.pwc.com/crimesurvey***

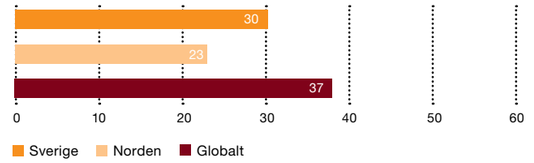
## *Var tredje svensk respondent uppger att de har drabbats – en nivå som närmar sig andelen bland de globala respondenterna*

Cirka en tredjedel, 30 %, av de svenska respondenterna uppger att de har drabbats av ekonomiska oegentligheter under de senaste 24 månaderna, vilket ligger nära nivån bland de globala respondenterna där 37 % har drabbats. En tillbakablick på tidigare års enkäter visar att skillnaden i andelen svenska och globala respondenter som drabbats har minskat. De svenska förhållandena ligger nu närmare det globala resultatet än i någon av de fyra senaste enkäterna.

En klar majoritet av respondenterna, både i Sverige och globalt, uppger att antalet ekonomiska oegentligheter de senaste 24 månaderna ligger mellan 1 och 10 fall. Det finns dock exempel i enkäten där respondenter uppger att de har drabbats av mer än 1 000 fall de senaste 24 månaderna vilket bedöms hänföras till större företag i särskilt utsatta branscher.

Intressant att notera är också att en klar majoritet av samtliga respondenter uppger att antalet fall av oegentligheter, och de ekonomiska skadorna, de senaste 24 månaderna inte har minskat, utan har ökat eller kvarstår på samma nivå som tidigare.

**Andelen som drabbats av ekonomiska oegentligheter**




*Andel av respondenterna som drabbats av ekonomiska oegentligheter de senaste 24 månaderna. Alla siffror är i procent.*

## *Män i förtroendeposition är överrepresenterade*

I linje med tidigare års enkäter uppger en majoritet av de drabbade respondenterna att förövaren i de mest allvarliga fallen varit anställd.

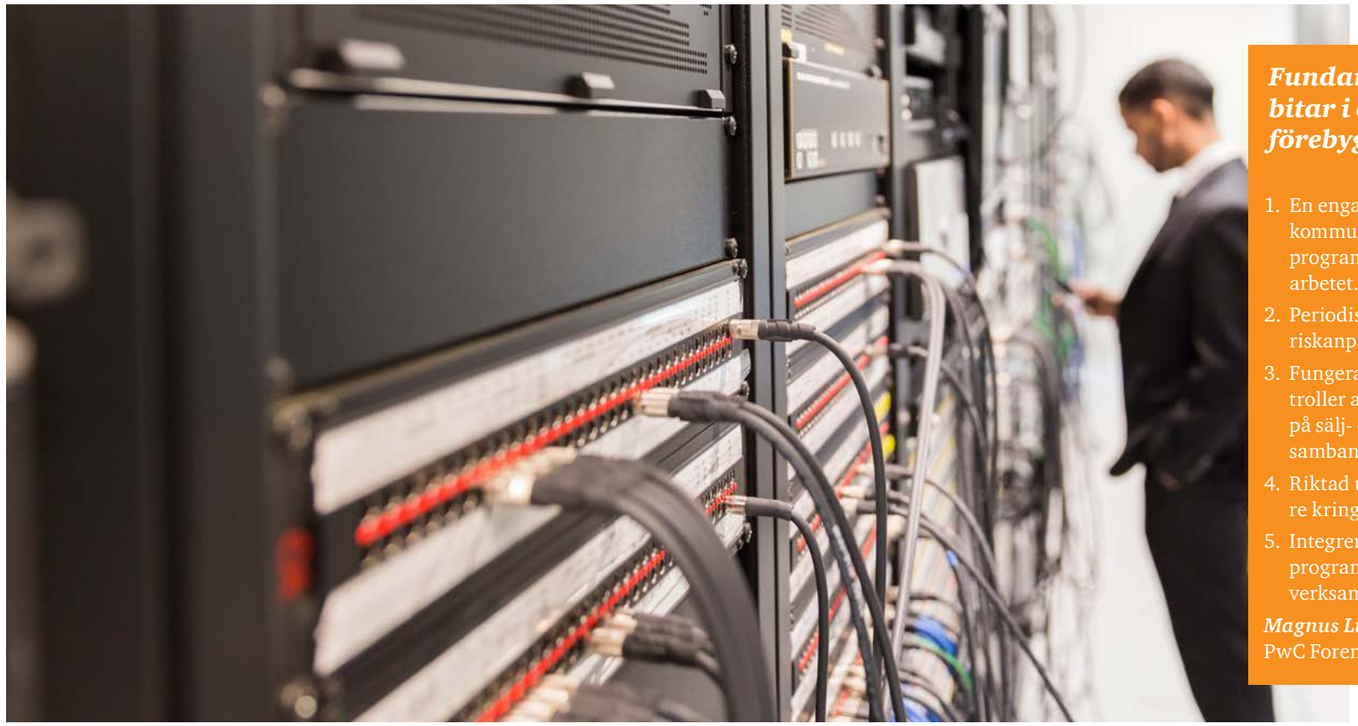
Vidare framkommer att en majoritet av de interna förövarna utgörs av topp- eller mellanchefer. Chefer har en förtroendeställning och kan utöva starkt inflytande där de verkar, vilket kan utnyttjas för att kringgå bristfälliga kontroller och oupptäckt begå brott.

Att anställda ofta är involverade i ekonomiska oegentligheter innebär dock att verksamheter kan minska riskerna exempelvis genom utformning av en riskanpassad intern kontroll – en chans till förbättringar som alltför många inte utnyttjar.

Män är överrepresenterade bland de som uppges som de huvudsakliga interna förövarna. En rimlig förklaring är att män, förutom att generellt vara överrepresenterade i brottssammanhang, också i större utsträckning innehar förtroendepositioner där möjligheterna att begå brott med liten upptäcktsrisk är större.

## Externa förövare finns oftare bland affärspartners

Vad gäller externa förövare uppger en majoritet av respondenterna att kunder är vanligast, men även att leverantörer förekommer i stor utsträckning. Bland respondenterna globalt anges agenter och andra former av mellanhänder som den näst vanligaste externa kategorin av förövare efter kunder. Ett resultat som troligen har ett starkt samband med korruptionsrisker. En bättre kontroll av agenter, återförsäljare och distributörer minskar den risken och är en viktig del i det förebyggande arbetet.



### *Fundamentala bitar i ett bra förebyggande arbete*

1. En engagerad ledning som kommunicerar ett tydligt program för det förebyggande arbetet.
2. Periodiska riskanalyser och riskanpassade kontrollåtgärder.
3. Fungerande processer för kontroller av affärspartners - både på sälj- och inköpssidan och i samband med förvärv.
4. Riktad utbildning av medarbetare kring risker och policies.
5. Integrering av det förebyggande programmet i den ordinarie verksamheten.

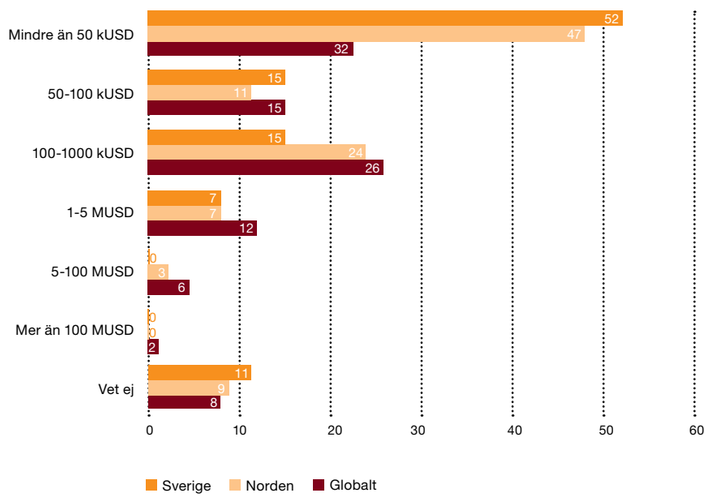
***Magnus Lindahl***
PwC Forensic Services

## Direkta ekonomiska skador kan svida…

De direkta ekonomiska skadorna av de oegentligheter som drabbat de svenska respondenternas verksamheter uppges till övervägande del ligga i intervallet upp till 1 MUSD (cirka 6,5 MSEK) med en tyngdpunkt på skador upp till 50 kUSD (cirka 300 kSEK). Samma mönster återges av de globala respondenterna men där finns också en relativt stor andel i intervallet 1 MUSD och uppåt med exempel på skador över 100 MUSD.

De riktigt stora ekonomiska skadorna kan vara en återspegling av att det utomlands, till skillnad från i Sverige, finns exempel på relativt stora bötesbelopp i samband med myndighetsingripande. Ingripanden som också medför andra direkta kostnader exempelvis i form av utredningskostnader och kostnader för aktiviteter med syfte att möta nya krav som ställs på verksamheten i en sådan situation.

**Storleken på de direkta ekonomiska skadorna**



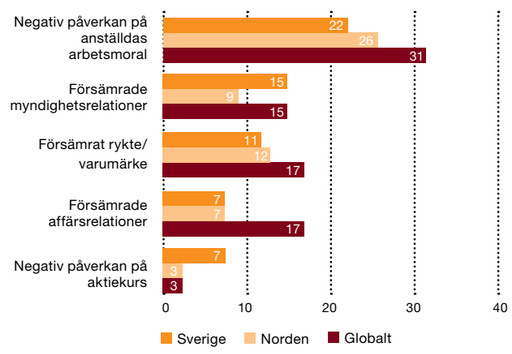

*Fördelning av de direkta ekonomiska skador från oegentligheter de senaste 24 månaderna. Alla siffror är i procent.*

## …men de indirekta skadorna är ofta betydligt allvarligare

De indirekta ekonomiska skadorna är svåröverskådliga men inte desto mindre allvarliga. Förtroendeskador och svårigheter att rekrytera och bibehålla skickliga medarbetare samt försämrad arbetsmoral lyfts tydligt fram av respondenterna som exempel på indirekta skador som följer av att en verksamhet drabbas av oegentligheter. Raserade relationer med viktiga kunder och leverantörer är andra former av indirekta skador som lyfts fram och som kan få mycket svåra följder.

Även om de indirekta skadorna kan vara svåra att mäta i kronor och ören så är en sak klar, effekterna är negativa, långvariga och ofta med svåra följder. När ekonomiska oegentligheter påverkar möjligheterna att rekrytera rätt folk, försämrar relationen med kunder och leverantörer får det negativa effekter på resultatet även om det inte klassificeras som ”oegentligheter” i resultaträkningen.

**Typer av indirekta skador**




*Fördelning av de indirekta skadorna från oegentligheter de senaste 24 månaderna. Alla siffror är i procent.*

# *Förskingring och trolöshetbrott alltjämt i topp*

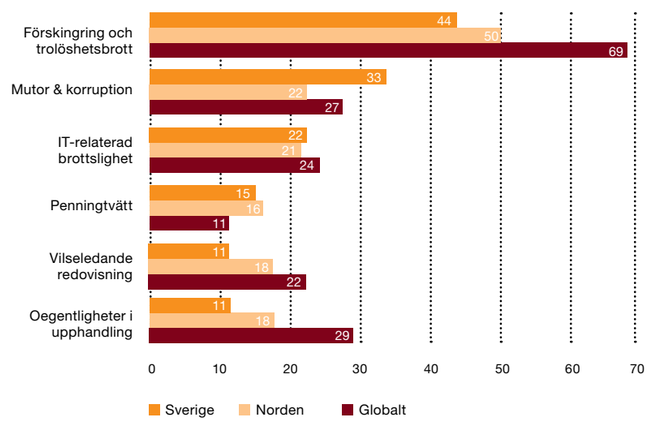
I likhet med tidigare års enkäter är förskingring och trolöshetsbrott den klart vanligaste typen av oegentligheter.

Denna typ av oegentligheter innefattar exempelvis fall där medarbetare på finans- och ekonomiavdelningar utnyttjar brister och svagheter i kontrollrutiner kring medelshanteringen och med låg risk för upptäckt kan genomföra otillbörliga utbetalningar.

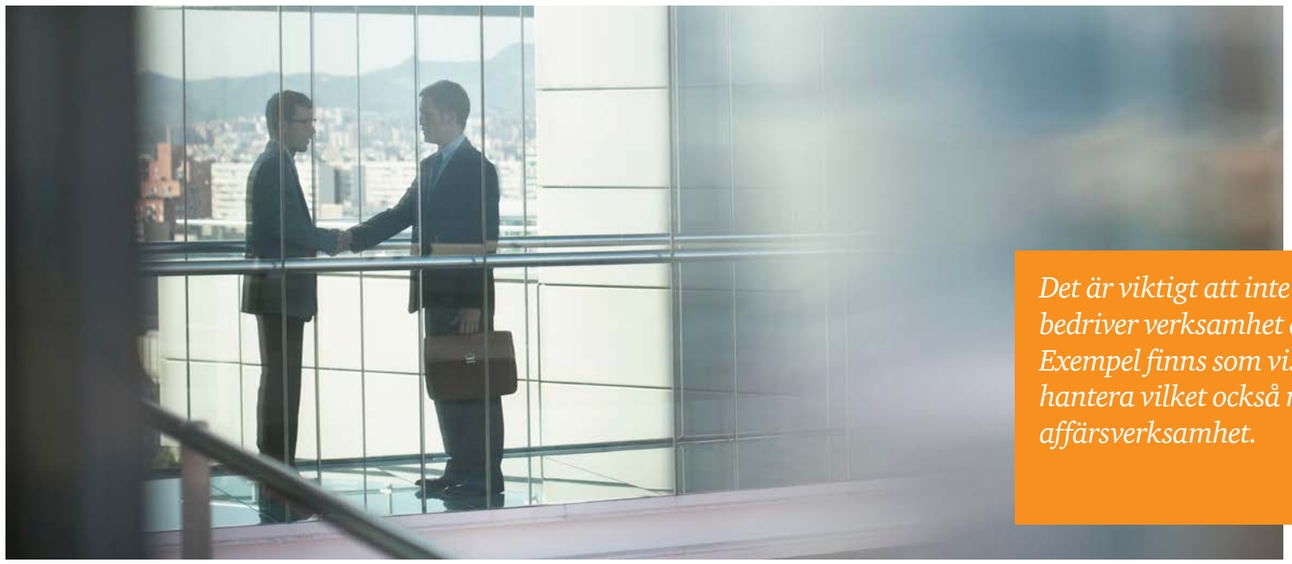
Den direkta skadan i varje enskilt fall kan vara begränsad men i större omfattning blir den sammanlagda skadan kännbar och kan också materiellt påverka riktigheten i bokföring och i skattebetalningar som i sig medför kostnader för rättelser och andra former av korrektiva åtgärder.

Anmärkningsvärt är att korruption och mutor bland svenska respondenter uppges vara de näst mest vanligt förekommande oegentligheterna. Cirka en tredjedel av de svenska respondenterna som drabbats av ekonomiska oegentligheter uppger att de har drabbats av korruption och mutor. En nivå som överträffar de globala respondenternas ranking där den näst vanligaste formen uppges vara oegentligheter i samband med upphandling.

**De sex vanligaste formerna av oegentligheter bland de svenska respondenterna**




*Fördelning av de vanligaste formerna av oegentligheter de senaste 24 månaderna. Alla siffror är i procent.*



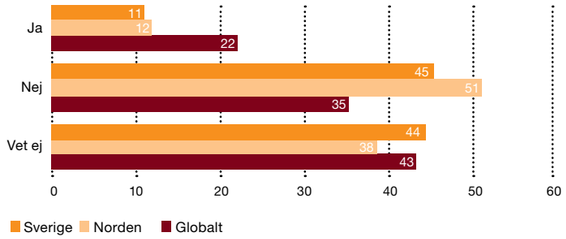
# *Risken för korruptionsskandaler skrämmer men hanteras inte på ett adekvat sätt*

Nästan var tionde svensk respondent uppger att verksamheten de representerar någon gång de senaste 24 månaderna blivit uppmanad att betala en muta. Motsvarande siffra är väsentligt högre för de globala respondenterna där nästan var femte uppger att deras verksamhet uppmanats att betala mutor.

Drygt var tionde svensk respondent anger vidare att de förlorat en affär på grund av att en konkurrent har betalat mutor. Bland de globala respondenterna uppger var femte att de har förlorat en affär till en mutande konkurrent.

Korruptionsrisken är också den risk som uppges vara det största hotet vid internationella affärer i jämförelse med penningtvättsrisker och risker kring kartellbildning och konkurrenshämmande aktiviteter. Det är framför allt risken för förlorat renommé som skrämmer. De eventuella finansiella förlusterna av korruption oroar de svenska respondenterna i mindre utsträckning jämfört med respondenterna globalt. Denna skillnad skulle kunna förklaras av att utländska rättsordningar, i synnerhet den amerikanska, men även i andra länder, medger påföljder och böter som vida överstiger vad som är aktuellt i Sverige.

**Andel som uppgett att de har förlorat en affär för att en konkurrent har betalat mutor**




*Andel som uppgett att de har förlorat affärer för att konkurrenter har betalat mutor under de senaste 24 månaderna. Alla siffror är i procent.*

*Det är viktigt att inte ta seden dit man kommer när man bedriver verksamhet där det finns risker för korruption. Exempel finns som visar att risker går att förebygga och hantera vilket också medför en långsiktig och hållbar affärsverksamhet.*

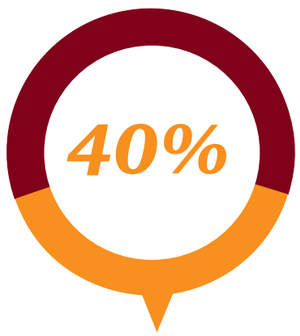
Magnus Brändstedt,
PwC Forensic Services

# *Korruptionsrisker påverkar tillväxtmöjligheter på högriskmarknader*

Ungefär en tredjedel av de svenska och nordiska respondenterna och hälften av de globala respondenterna representerar verksamheter som är verksamma på marknader som förknippas med en hög risk för korruption. Vidare uppger ungefär en tredjedel av alla respondenter att de under de senaste 24 månaderna har haft affärsmöjligheter på dessa marknader.

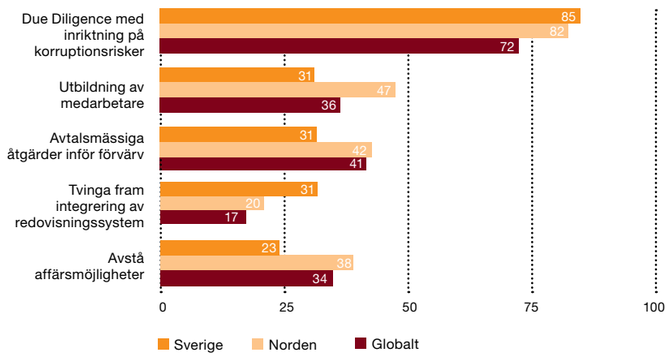
Av dessa uppger cirka 40 % att risken för korruption inverkat på verksamhetens strategi att fullfölja affärsmöjligheten. De vanligaste formerna av åtgärder för att hantera problemet är due diligence med inriktning på korruptionsrisker, utbildning av medarbetare, avtalsmässiga åtgärder inför förvärv och att helt enkelt avstå från affärsmöjligheten.

Anmärkningsvärt är dock att en majoritet uppger att någon förändring i strategi inte har skett eller att de inte vet om det har skett någon sådan förändring trots ökade risker för mutor och korruption. Att också lagstiftningen i många länder, inklusive Sverige, ställer större krav på verksamheter att på ett systematiskt sätt arbeta för att minska risken för mutor gör inte saken mindre anmärkningsvärd.




40% av de svenska respondenterna uppger att risken för korruption har inverkat på företagets affärsplan eller strategi. Detta är i paritet med vad de nordiska och globala respondenterna har angivit.

**Korruptionsförebyggande åtgärder**



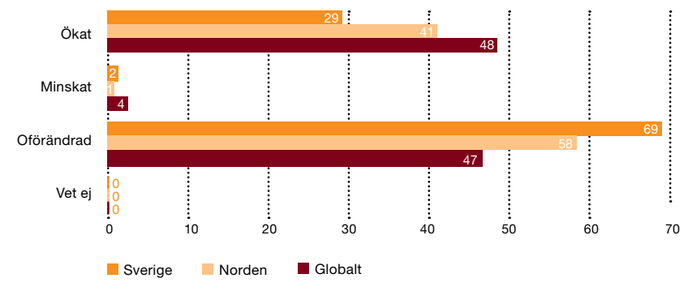

*Fördelning av åtgärder för att undvika korruption på utsatta marknader, de senaste 24 månaderna. Alla siffror är i procent.*



# *Riskerna för IT-relaterad brottslighet uppges öka...*

IT-relaterade brottslighet uppges vara den tredje vanligaste formen av oegentligheter bland de svenska respondenterna. Cirka en tredjedel av de svenska respondenterna upplever vidare att risken för IT-relaterad brottslighet har ökat under den senaste 24-månadersperioden vilket kan jämföras med respondenterna globalt där nära hälften upplever att risken har ökat under samma tidsperiod.

**Ökning av IT-relaterad brottslighet**




*Respondenternas uppfattning om förändringen kring risk för IT-relaterad brottslighet de senaste 24 månaderna. Alla siffror är i procent.*

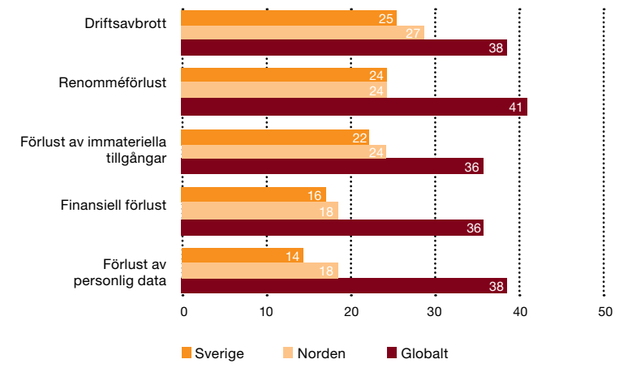
## *...med många negativa följdeffekter*

De främsta orosmomenten, till följd av IT-relaterad brottslighet, som de svenska respondenterna pekar ut är driftsavbrott, renomméförlust och förlust av immateriella tillgångar. Var och en av dessa är allvarlig nog att skada en verksamhet både på kort och lång sikt.

De svenska och nordiska respondenterna verkar dock inte uppfatta riskerna med IT-relaterad brottslighet som lika allvarliga som de globala respondenterna som i mycket större utsträckning betraktar ovan nämnda följdeffekter av IT-relaterad brottslighet som ”mycket oroande”. Detta trots att förekomsten av IT-relaterad brottslighet uppges ligga på ungefär samma nivå bland alla respondenter.

En förutsättning för att kunna förebygga oegentligheter på ett effektivt sätt är att det finns en medvetenhet kring riskerna. Givet att riskerna bedöms som betydligt allvarligare bland de globala respondenterna är det rimligt att anta att åtgärder också prioriteras högre och att de därmed är bättre rustade att förebygga de skador som IT-relaterad brottslighet medför.

**Följdeffekter av IT-relaterad brottslighet**




*Andel av respondenterna som svarat att de är ”väldigt oroade” för olika typer av följdeffekter från IT-relaterad brottslighet mot deras organisation.*

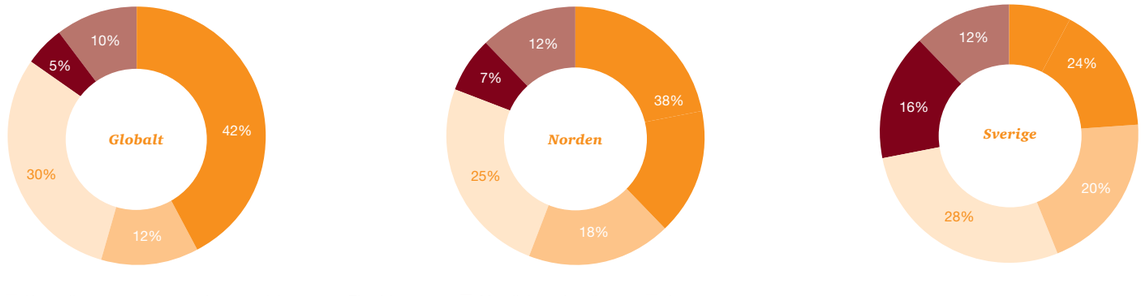
# Riskanpassade kontroller – det bästa sättet att upptäcka oegentligheter

Respondenterna uppger att tips av olika slag, interna, externa samt tips från whistleblowersystem, är en av de viktigaste källorna till att oegentligheter uppdagas. En annan viktig källa för upptäckt är olika former av kontrollprocesser som exempelvis övervakning av transaktioner och dataanalyser.

Andra kontrollprocesser som medför många upptäckter är insatser som specifikt syftar till att minska risker för oegentligheter samt kontroller som sker inom ramen för exempelvis fysiskt säkerhetsarbete och på IT-avdelningar.

Bilden som framträder är att upptäckten av oegentligheter drivs av omständigheter som verksamheterna inte själva kontrollerar samt av specifika, riskanpassade åtgärder. En viktig lärdom av detta är att fokusera resurserna smart och kostnadseffektivt genom en effektiv tipshantering och att anpassa kontroller efter verksamhetens faktiska risksituation.

**När det gäller det allvarligaste ekonomiska brottet ni upptäckt, hur upptäcktes det?**



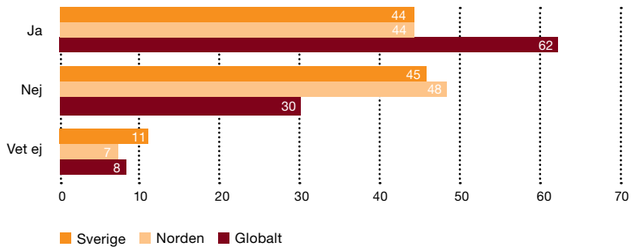

*Fördelning av hur det allvarligaste ekonomiska brottet har upptäckts under de senaste 24 månaderna. Alla siffror är i procent.*

# Vikten av systematisk tipshantering

Trots att tips av olika slag är en av de viktigaste källorna till upptäckt av oegentligheter anger knappt hälften av de svenska respondenterna att de implementerat ett whistleblowersystem. Denna andel är lägre jämfört med bilden som ges av de globala respondenterna. En majoritet av de svenska och globala respondenterna som implementerat ett dylikt system uppger att whistleblowersystemet har använts fler än en gång under den senaste 24-månadersperioden, samt att de upplever att ett whistleblowersystem är ett effektivt sätt att upptäcka ekonomiska oegentligheter.

Ett whistleblowersystem är en enkel och förhållandevis billig åtgärd som kan fånga upp många allvarliga händelser i en organisation. Förutsättningen för att ett whistleblowersystem skall bli effektivt är dock att det finns utarbetade rutiner för hur tipsen skall hanteras och utredas samt att information om systemet når alla berörda på ett adekvat sätt.

**Förekomst av whistleblowersystem**




*Andel av respondenterna som har ett whistleblowersystem. Alla siffror är i procent.*




# Tillfället gör tjuven…

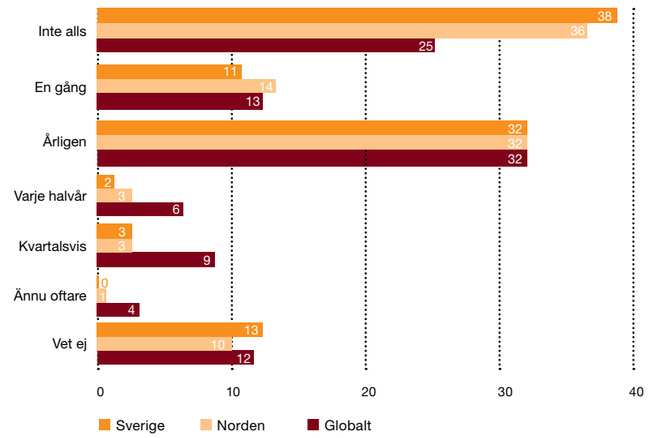
Studien bekräftar att det är tillfället som gör tjuven. Cirka 3/4 av samtliga respondenter pekar ut själva möjligheten att begå oegentligheter som den enskilt viktigaste faktorn när det gäller oegentligheter begångna av anställda.

## …men många underlåter att kartlägga riskerna

I tidigare studier har vi observerat att nordiska, och i synnerhet svenska respondenter, uppgett att en stor andel oegentligheter upptäckts av ren tillfällighet, ett mönster som också återkommer i årets studie.

Ett av flera viktiga verktyg för att motverka ekonomiska oegentligheter är att göra en risk- och sårbarhetsanalys och utifrån denna prioritera och anpassa kontrollåtgärder. Ett rimligt antagande är att det finns ett samband mellan hur ofta en risk- och sårbarhetsanalys genomförs och hur många fall av ekonomiska oegentligheter som upptäcks. Ur detta perspektiv är det anmärkningsvärt att närmare 40 % av de svenska respondenterna uppger att några riskbedömningar inte görs överhuvudtaget.

**Andel som genomfört en riskanalys**




*Andel av respondenterna som har genomfört en riskanalys under de senaste 24 månaderna. Alla siffror är i procent.*

Ytterligare 24 % uppger att de inte vet om en sådan analys har genomförts eller att den endast har genomförts vid ett tillfälle de senaste 24 månaderna. Denna siffra skall ställas i relation till de globala respondenterna där endast var fjärde respondent uppger att ingen riskanalys har genomförts. Den vanligaste förklaringen till varför riskanalyser inte har genomförts uppges vara att man inte vet hur en riskanalys genomförs eller att nyttan bedöms som låg. Detta visar tydligt på att förståelsen av riskerna och hur dessa hanteras är en kulturfråga som många, exempelvis i företagsledningar och styrelser, har att jobba med framgent.

# *För mer information kontakta oss!*

**Ulf Sandlund**
0709-29 36 07
ulf.sandlund@se.pwc.com

**Magnus Lindahl**
0709-29 30 25
magnus.lindahl@se.pwc.com

**Magnus Brandstedt**
0723- 53 05 48
magnus.brandstedt@se.pwc.com

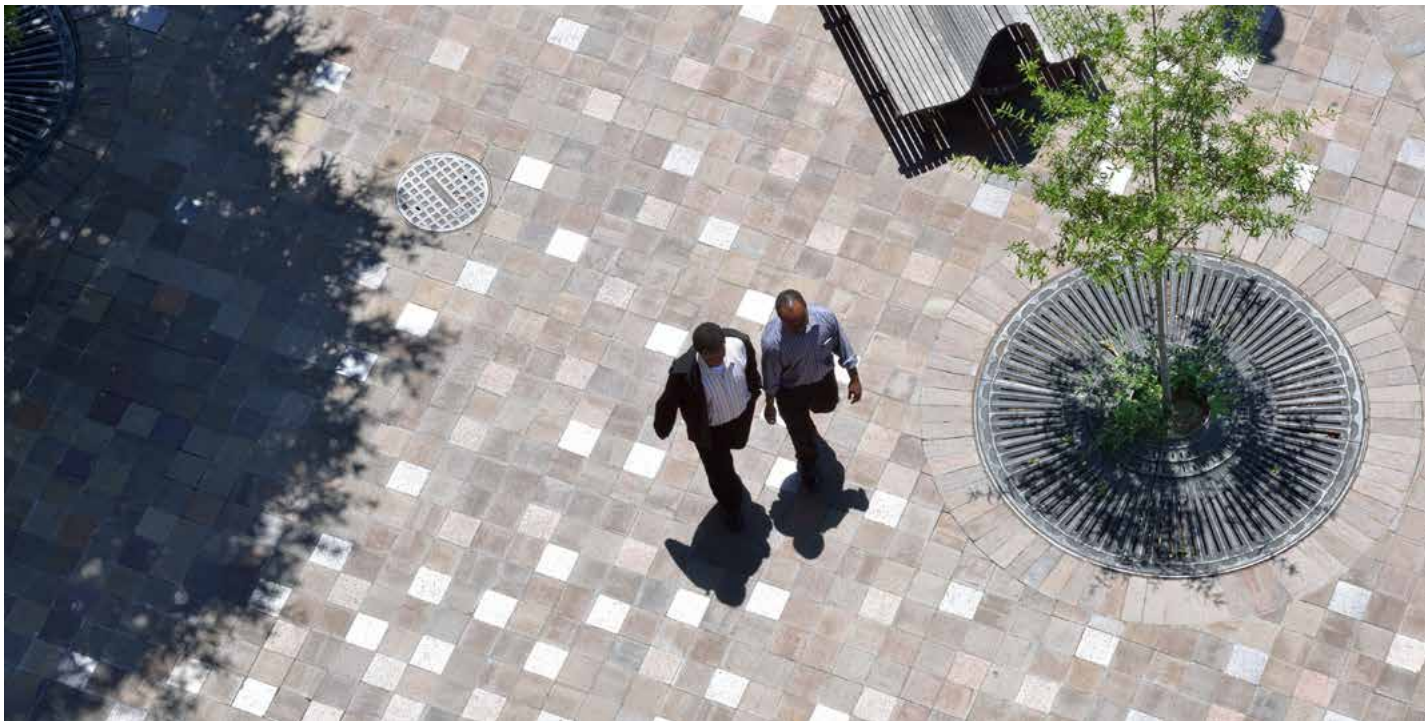
PwC Sverige är marknadsledande inom revision, redovisning, skatte- och affärsrådgivning med 3 800 medarbetare på 100 kontor runt om i landet. Med erfarenhet och unik branschkunskap utvecklar vi värden för våra 60 000 kunder vilka utgörs av globala företag, svenska storföretag och organisationer, mindre och medelstora, främst lokala företag samt den offentliga sektorn.

PwC Sverige drivs som en självständig och oberoende juridisk enhet. Vi ingår i det globala nätverket PwC och delar våra kunskaper, erfarenheter och lösningar med 184 000 medarbetare i 157 länder för att utveckla nya perspektiv och praktiska råd.

pwc

© 2014 PricewaterhouseCoopers i Sverige AB. Att mångfaldiga innehållet helt eller delvis är förbjudet enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk. Förbudet gäller varje form av mångfaldigande genom tryckning, kopiering etc.

# Economic Crime: A Swiss Perspective



**37%**
More than one in three organisations report being victimised by economic crime.

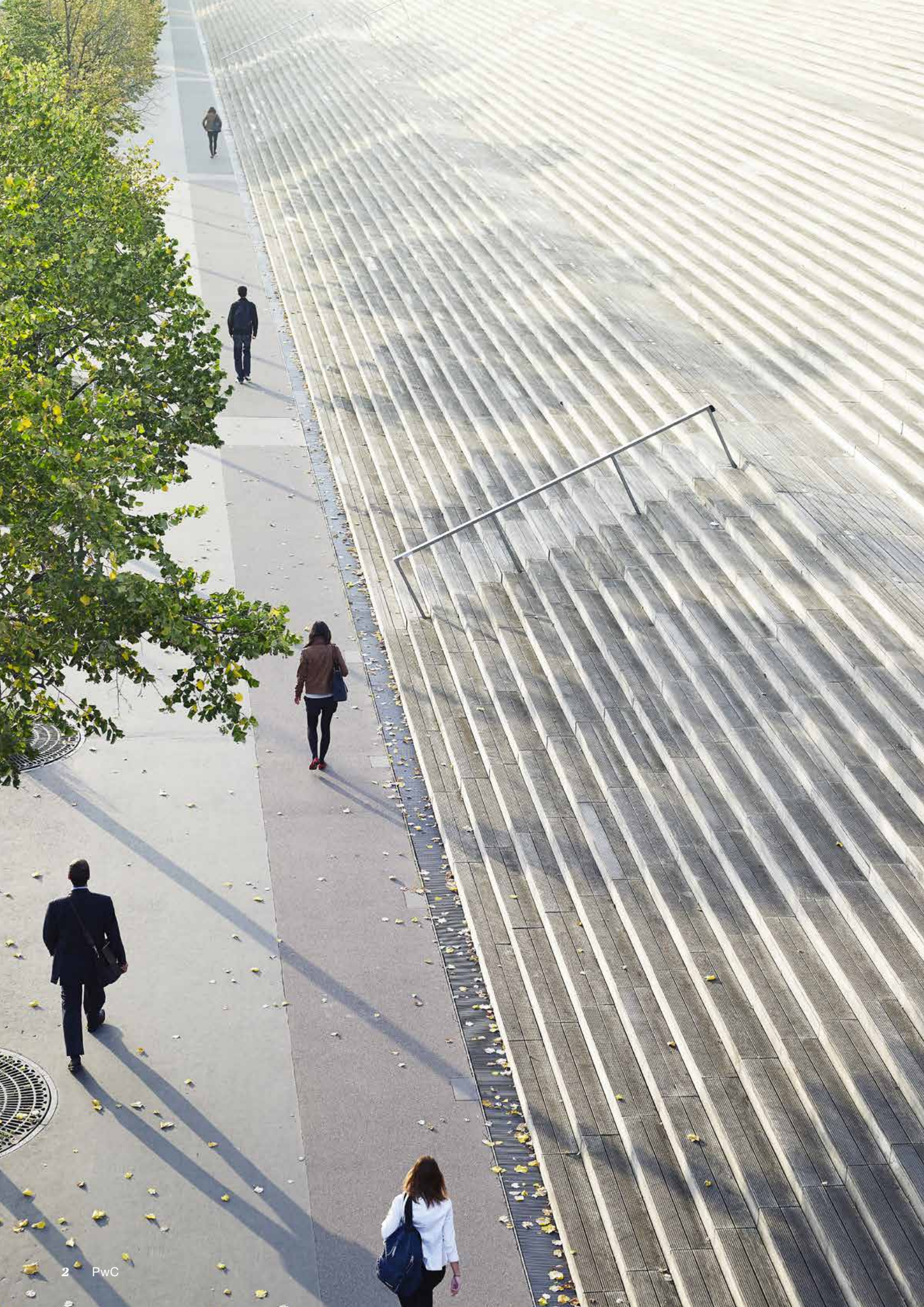
**71%**
of economic crime was detected through corporate controls and anti-fraud corporte culture mechanisms.

**26%**
After asset misappropriation, cybercrime is the second most reported type of economic crime.

pwc

*Economic crime continues to be a major concern for Swiss organisations.*

# Contents



# *Foreword*

Given the trend identified in our previous survey, it comes as no surprise that economic crime still persists, affecting one in three Swiss organisations. This year, the Global Economic Crime Survey looks at the major types of fraud in more detail, focusing on how these acts threaten business processes, whilst the Swiss-specific edition of the survey provides a local view of how economic crime has developed in the past 24 months. Some of our highlights include:

**Incidents of fraud have not lessened –** The percentage of respondents having experienced economic crime in the last 24 months increased from 18% to 37%.

**Cybercrime is here to stay –** 26% of Swiss respondents that were affected by economic crime, reported incidents of cyber-attacks at their company. Although awareness of cybercrime has improved, a significant percentage of respondents were not able to determine the extent of damage to their organisation caused by this type of crime.

**Less reported bribery and corruption –** Only 3% of Swiss respondents that have been affected by economic crime over the past 24 months reported incidents of bribery and corruption despite operating in high-risk countries. However, a significant number recognise it as a threat, with 37% ranking this type of economic crime as the greatest risk to their organisation when doing business globally.

**The fraudster profile and actions taken –** This year we have observed the return of the traditional fraudster who is male, between the age of 41 and 50 and has been with the company for several years. We also see that Swiss companies are more stringent in dealing with internal infractions; more of them are choosing to dismiss (2011: 60% versus 2014: 82%) or even take civil action against the fraudster (2011: 30% versus 2014: 59%).

**Detection methods –** This year's survey shows that, whilst the overall effectiveness of corporate controls has remained relatively unchanged during the survey period, there has been an increase of fraud detected thanks to corporate culture (from 24% in 2011 to 35% in the past 24 months). This suggests heightened awareness of the need to foster an anti-fraud corporate culture at Swiss companies.

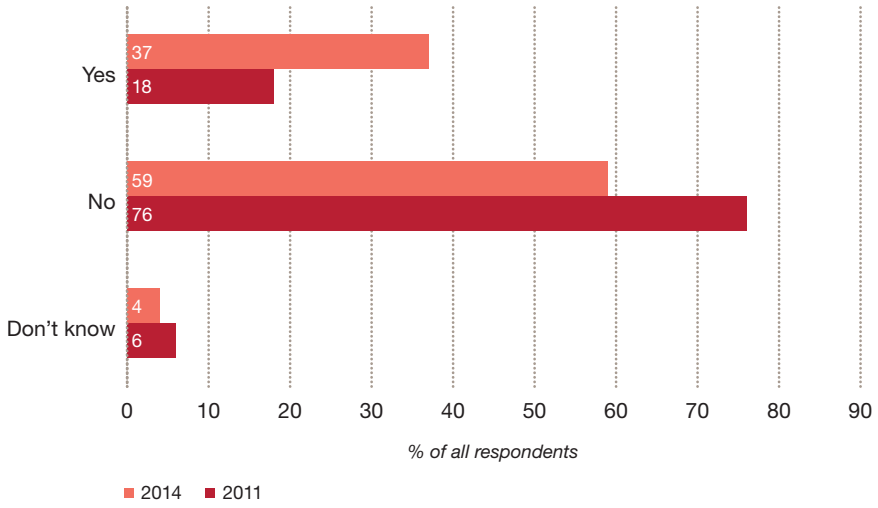
*According to our respondents, asset misappropriation continues to be the most significant economic crime affecting Swiss organisations.*

# The current fraud environment

## Economic crime and Switzerland

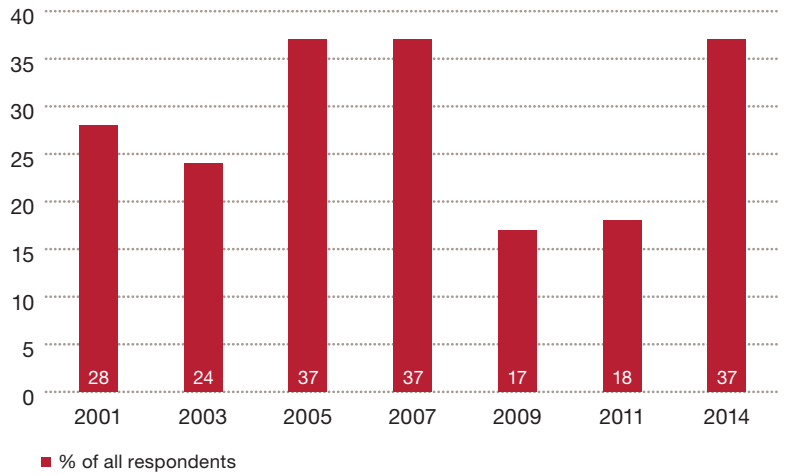
In our 2014 survey we see a significant increase in fraud where 37% of our respondents experienced incidents of economic crime in contrast to 18% in 2011 [Figure 1]. Some of this shift may be attributable to the shorter length of time surveyed in 2011 (12 months) in comparison to 2014 (24 months), which gave companies more time and, therefore, more opportunity to detect fraudulent incidents. If the perpetrator is skilful in covering his tracks, it may often take companies several months before the wrongdoing is unearthed.

**Figure 1: Economic crime suffered in 2011 and 2014**




When analysing our previous survey results in terms of the percentage of Swiss companies affected by economic crime, we noted that this year we returned to the trends evident in 2005 and 2007 [Figure 2]. Interestingly, during that period we were experiencing favourable economic conditions, so the number of reported fraud cases is what we expected to see from our surveys in 2009 and 2011 during an economic downturn.

**Figure 2: Swiss companies reporting fraud 2001–2014**




As mentioned at the time, during a period of recession the fraud rate tends to increase; however, we notice that this may not be the case in Switzerland as the opposite in fact occurred. The reason for this could be that, although there is more pressure and incentive to commit fraud in an economic downturn, there is also less opportunity to do so because of the decreased availability of assets in circulation and the tendency of companies to reduce their headcount. On one hand, the declining headcount may have affected internal functions that are traditionally responsible for fraud detection, such as internal audit, controlling or compliance, and therefore weakened their ability to effectively detect fraud incidents. On the other hand, however, this wave of layoffs may also have hit potential and actual fraudsters, thereby depriving them of the possibility to commit fraud.

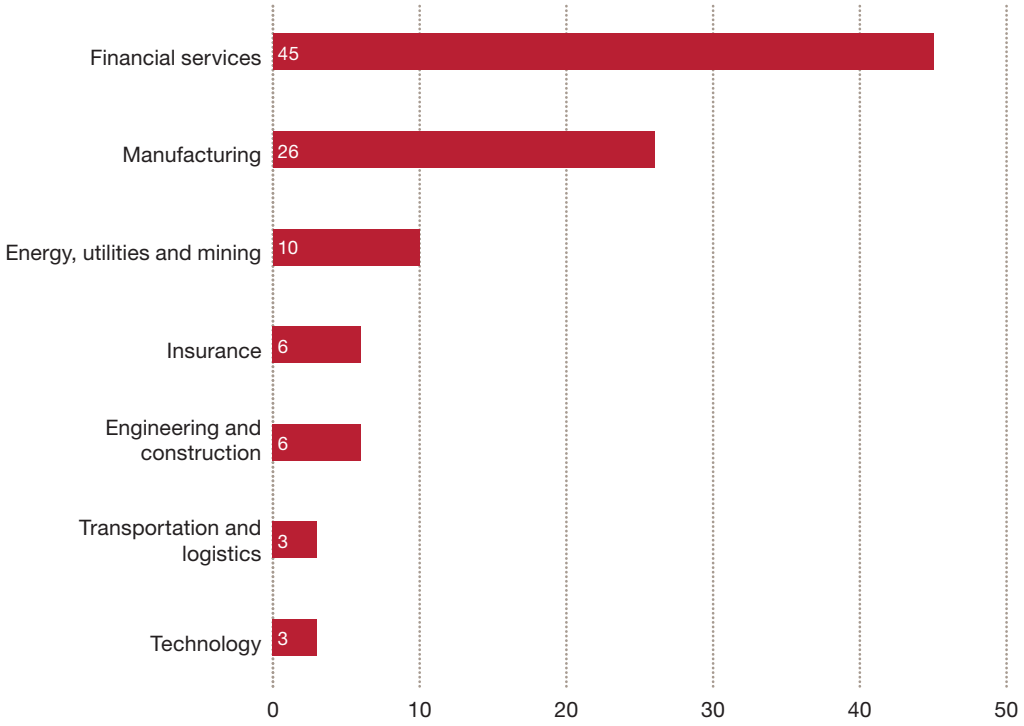
Furthermore, the 2014 results are more in line with the global trends, where 37% of respondents experienced economic crime in the past 24 months compared to 34% of respondents from Western Europe.

## The corporate landscape

Over half of the Swiss survey respondents come from three industries: financial services, manufacturing, and engineering & construction. Given the importance of these industries in Switzerland, the participant mix is in line with our expectations.

Financial services are also the leading industry in terms of survey participation in Western Europe (17%) as well as globally (19%); however, in Switzerland they contributed to almost one-third of the results with 30%. We believe that such a strong financial services contribution is endemically Swiss and the results of the survey reflect our unique corporate landscape. This is especially evident when it comes to incidents of cybercrime and money laundering, which are discussed in more detail below. It is therefore not surprising that entities in the financial services industry have experienced the highest rate of economic crime over the past 24 months (45%) [Figure 3].

**Figure 3: Top 5 Swiss industries affected by economic crime – 2014 Survey**

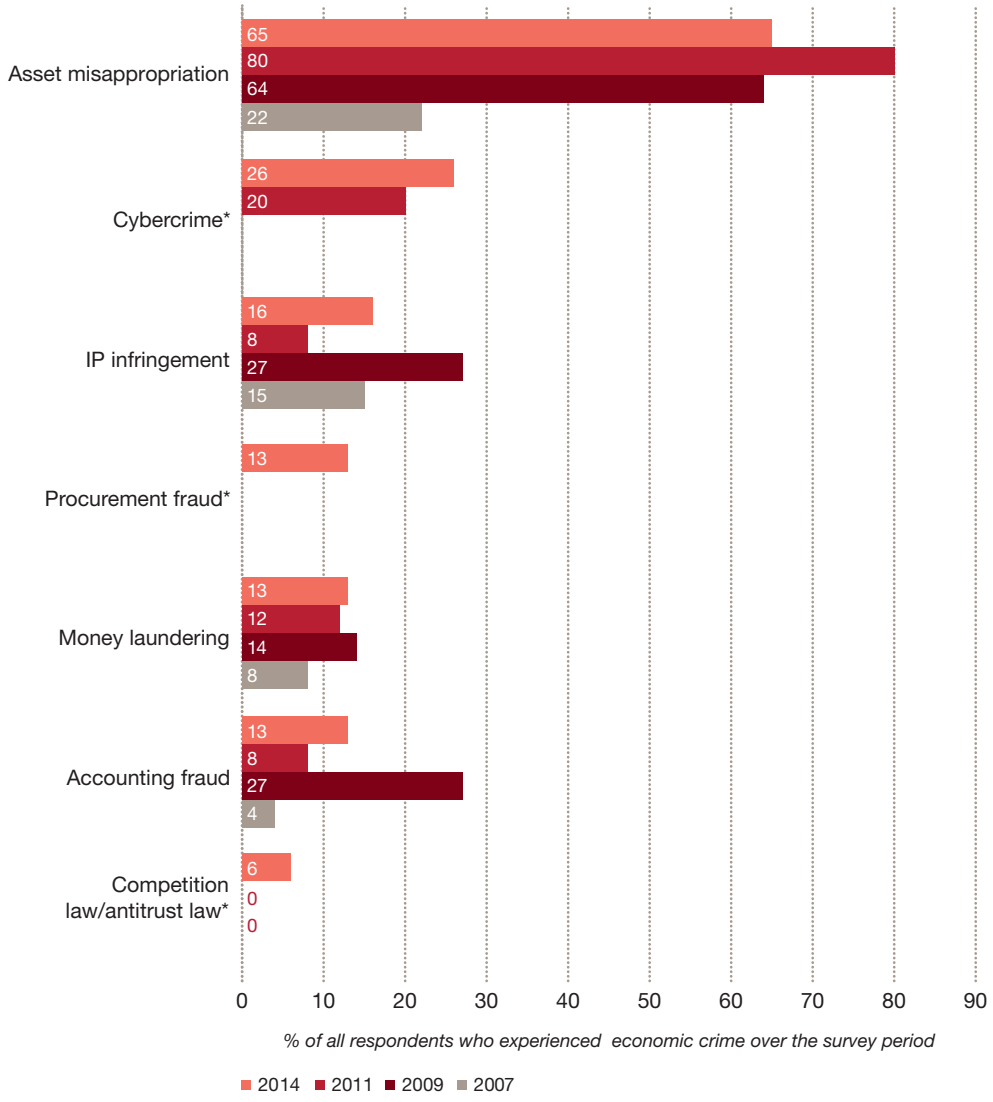



## Types of economic crime

Asset misappropriation has traditionally ranked highest in the type of fraud reported by our respondents, with 65% being affected by this particular economic crime in 2014 [Figure 4]. This is a significant drop since 2011 when a whopping 80% were affected. Despite the decline, we believe asset misappropriation will continue to be the most prevalent type of economic crime impacting Swiss organisations as it is often easily committed and detected.

The second type of fraud affecting Swiss entities is cybercrime, which was reintroduced as a separate category in our last survey in 2011. We noted an increase from 20% to 26%, as expected. This type of fraud is predominant in the financial services industry, where 75% of the reported incidents of cybercrime relate to entities from that sector. We are of the opinion that cybercrime is here to stay, given the unrelenting reliance on technology – from coping with an ever-increasing amount of data to the introduction of new devices that help us in our everyday work life.

## Figure 4: Top 5 types of economic crimes reported




* Cybercrime: reintroduced in 2011 as a separate category; Procurement: introduced as a separate category in 2014; Competition law/antitrust law introduced as a separate category in 2009

Intellectual property infringements also continue to be amongst the top economic crimes (ranking number three out of the 5 most frequent categories) and increased from only 8% in 2011 to 16% in 2014. As Switzerland is an economy that is characterised by high innovation and know-how, this emerging trend comes as no surprise.

Procurement fraud, which is a newly introduced category, ranks in the fourth place affecting 13% of respondents who experienced economic crime in the past 24 months. We believe that this time around a number of respondents might have more aptly reclassified some incidents of fraud to this category, given that it was previously equated to asset misappropriation. This may partly explain the decline in companies being affected by the latter type of fraud. Sharing places with procurement fraud are money laundering (2011: 12%) and accounting fraud (2011: 8%), with the former being a focus of further discussion later on in this report.


## *Procurement fraud and business processes*

Despite having robust controls in place fraud can occur in all stages of the procurement process – starting with the bidding phase to the post-award and administration phase which can lead to use of low-quality products. Common procurement fraud schemes include:

- Invoicing frauds (false invoicing through dummy suppliers, personal purchases)
- Conflicts of interest (overbilling, pre-payments)
- Bribery and corruption (kickbacks and suppression of rebates)

Consider an employee who has significant power within the organisation working with a legitimate supplier in order to receive kickbacks through overbilling. The key element to this scheme is collusion – a secret agreement involving fraudulent activity. Collusion is extremely difficult to detect as it mainly happens outside of the transactional cycle and therefore creative accounting entries are generally not required. Typically, such a scheme is characterised by the fact that the employee and the vendor are closely acquainted.

So what can companies do to minimise the risk of procurement fraud? A combination of robust controls and well-designed data analytic tests may do the trick. Some examples include testing for:

- Unusual number of disbursements that fall just below a threshold that requires additional approval for payment
- Unusual payments to a particular supplier over a specified period of time
- Purchase orders which have been raised at the same time or after an invoice has been entered
- Payment date on or before invoice date
- Matches between contact person in the vendor master file to employee name within the employee master file (including identical or similar addresses, phone numbers, tax identification numbers or other relevant contact details)
- Corporate expense analysis

The human element is also essential when it comes to combating purchasing fraud. Those entrusted with combating fraud within the organisation should also regularly check the company's payment authorisation matrix to ensure that it is still relevant to the existing processes. Not only will this reveal any weaknesses in the segregation of duties within the company, but it will also help detect any individuals who may be overstepping their job description boundaries.

In addition, a company should have several suppliers wherever possible, and a list of pre-approved vendors who have been subject to a strict vetting exercise should be set up and regularly reviewed. Payments should only be made to these pre-approved vendors and for their pre-approved services. Any potential related party relationships between employees and suppliers should also be scrutinised before accepting a vendor for provision of services.

## *Procurement fraud – can you spot the red flags?*

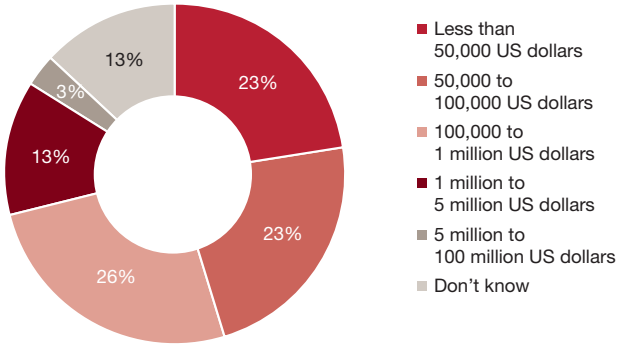
Indications that the organisation might be an easy target for a fraudster:

- Too much trust placed in key employees
- Weak internal controls
- Lack of purchasing guidelines
- Missing supplier documentation
- Use of agents/advisors/brokers to facilitate business, in particular in emerging markets

Indications that the organisation has already been affected by procurement fraud:

- Significant price changes as well as changes in orders and contracts after the award
- Suppliers' accounts with a high volume of debit and credit entries
- Large/unusual commission payments and advance payments
- Vendor complaints

## Figure 5: The cost of economic crime – 2014 Survey




*% of all respondents who experienced economic crime over the survey period*

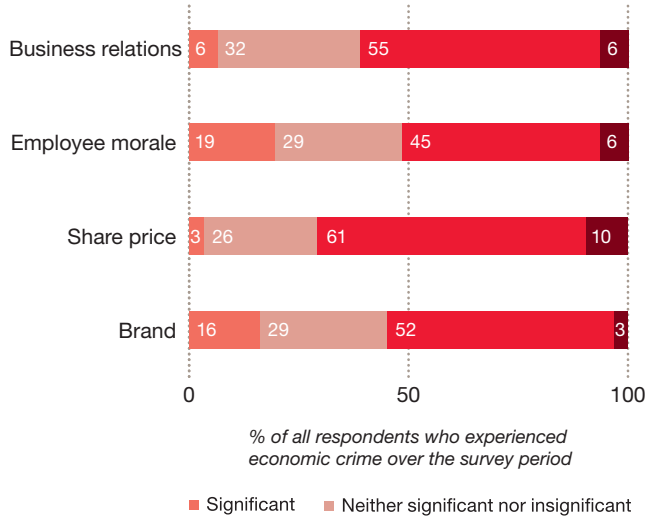
## The damage is done

When asked about the aggregate financial impact of economic crime suffered in the past 24 months, 71% of Swiss companies indicated that they had incurred losses amounting to less than USD 1 million, compared to 77% of Western European companies and 73% of companies globally. Although the trend seems to be roughly in line with other regions, 13% of the respondents do not actually know what the financial impact of fraud is on their organisation, thus the overall effect may be underestimated [Figure 5].

Unfortunately, the occurrence of economic crime is not only limited to adverse monetary effects; it may also leave a wider swath of damage on our businesses. Despite not being all too worried about the collateral effects of reported instances of fraud, Swiss businesses do confess to being slightly more concerned than they were in 2011 [Figures 6 & 7]. The most significant impact of fraud on businesses other than the financial dimension is its effect on employee morale, with 19% of respondents experiencing this type of collateral damage as well as an adverse influence on the company's brand (16%).

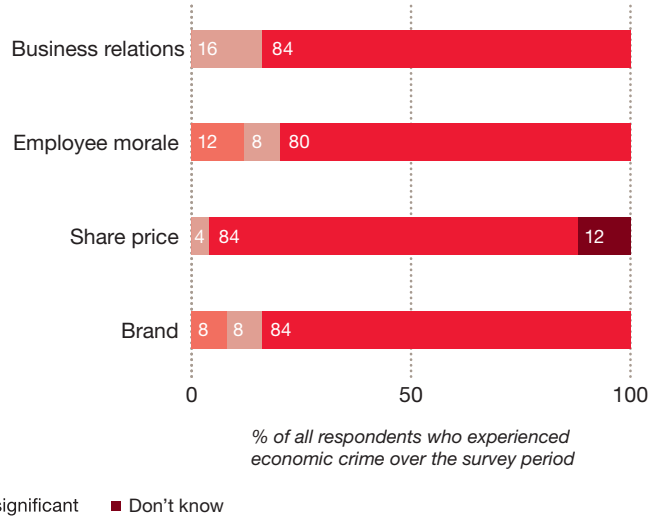
Furthermore, 6% of the organisations that experienced fraud also say that it had a detrimental impact on their business relations, whilst in 2011 there were no such cases. And only 3% of the respondents think that economic crime had a significant impact on their share price.

## Figure 6: Non-financial impact of the economic crime – 2014 Survey




*% of all respondents who experienced economic crime over the survey period*

## Figure 7: Non-financial impact of the economic crime – 2011 Survey




*% of all respondents who experienced economic crime over the survey period*

Significant | Neither significant nor insignificant | Insignificant | Don't know

*12% of all respondents believe it is likely that their organisation will experience bribery and corruption in the next 24 months.*

# Under the eye of enforcement

Some economic crimes cause not only significant harm to the company; they are also of particular concern to society. They worsen the overall corporate climate and are a source of inefficiency and waste. We believe this is the case with incidents of bribery and corruption, money laundering and anti-competitive behaviour which for the purposes of this report are referred to as government enforcement-related crimes.

Over the years, these crimes have been and continue to be under increased scrutiny by regulators and other public authorities. They are subject to stringent regulation and enforcement as well as to harsh penalties including fines and remedial expenses. Organisations convicted of having engaged in government enforcement-related crimes also suffer adverse reputational damage due to negative publicity.

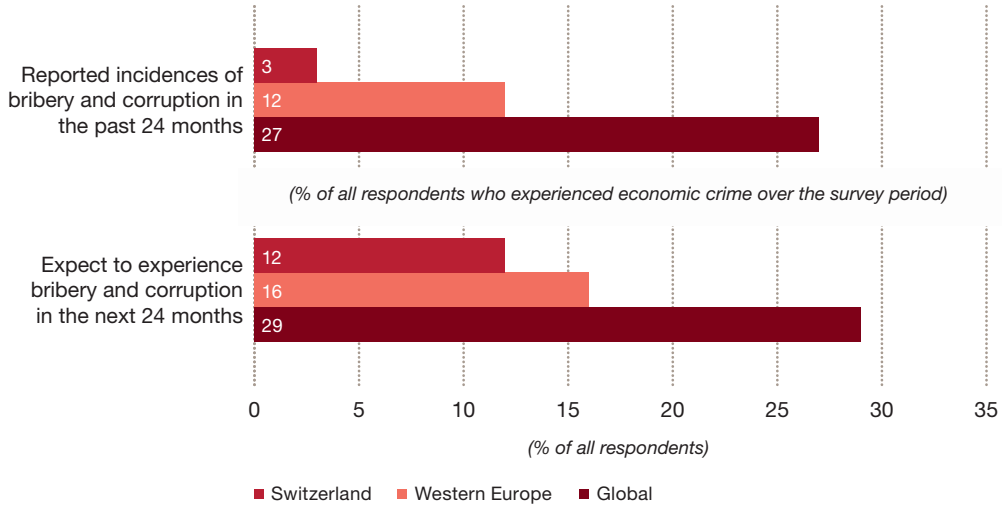
The impact of this type of crime has increased significantly in today's highly intertwined global economy. As organisations seek to gain new market shares and need to cope with intensified competition, they expand into high-risk territories where they are confronted with cultural differences and varying national customs. Therefore, they may be exposed to questionable business ethics and tempted to abide by them. In addition, organisations also have to consider the extraterritorial effects of their own national regulations in this regard.

## Swiss companies and government enforcement-related crimes

When asked what type of economic crime their organisation has experienced in the previous 24 months, only 3% of Swiss respondents mentioned bribery and corruption. Even though that number appears to be in line with the perception of Switzerland as a country with low levels of bribery and corruption, we believe the incidence of this type of crime in Switzerland has been underreported and thus may not reflect reality. The risk perception of bribery is however higher, with 12% of all respondents believing it is likely that their organisation will experience this type of crime in the next 24 months. In contrast, at the global level a striking 27% of respondents affected by economic crime reported incidents of bribery and corruption over the same period of time and almost 29% expect to experience this crime in the future [Figure 8].

This significant difference is surprising in light of the fact that our survey shows that 76% of Swiss respondents already operate or expect to operate in territories where there is a high level of corruption risk, compared to 49% of respondents in Western Europe and 57% globally.

**Figure 8: Incidences of bribery and corruption within the past 24 months and expectations for the next 24 months**




Interestingly, our survey shows that even though almost three quarters of the Swiss financial services companies operate and/or plan to operate in territories with a high level of corruption risk, no respondent from that industry reported having been asked to pay a bribe or having lost an opportunity to a competitor who paid a questionable incentive over the past 24 months. Although bribery and corruption is widespread in different industrial sectors, this particular result comes as no surprise. However, as our findings suggest, an increasing number of Swiss financial services companies are involved or plan to get involved in business operations in high-risk markets. Going forward, this may leave them exposed to the risk of bribery and corruption, indicating that no industry is immune.

In terms of money laundering (13%) and anti-competitive practices (6%), our survey indicates that Swiss companies are currently more affected by these types of fraud than by bribery and corruption. Globally, the levels of money laundering and anti-competitive behaviour appear to be quite similar, with 11% of the fraud affected respondents having experienced money laundering and 5% reporting anti-competitive behaviour in the past 24 months. When asked about their future expectations in terms of money laundering, 14% of the Swiss respondents believe it is likely that their organisation will experience this type of crime and 11% believe the same for anti-competitive behaviour, which is in line with the trend observed globally.

## The Swiss perception of government enforcement-related crimes – how risky are they?

We asked our respondents, which of the government enforcement-related crimes they perceived as posing the highest risk to their organisation in doing business on a worldwide scale. More than one-third of the Swiss respondents (37%) ranked bribery and corruption as the highest risk to their organisation, closely followed by money laundering (35%). This is considerably less compared to the global results, where more than half of the respondents (53%) consider bribery and corruption to be the highest risk [Figure 9].

This suggests that, even though Swiss respondents have been less affected by bribery and corruption in the past 24 months, they are becoming more aware of the risks that this economic crime may pose to their organisation and business activities, albeit far less so than their global counterparts.

**Figure 9: The highest risk in doing business globally in terms of government enforcement-related crimes**

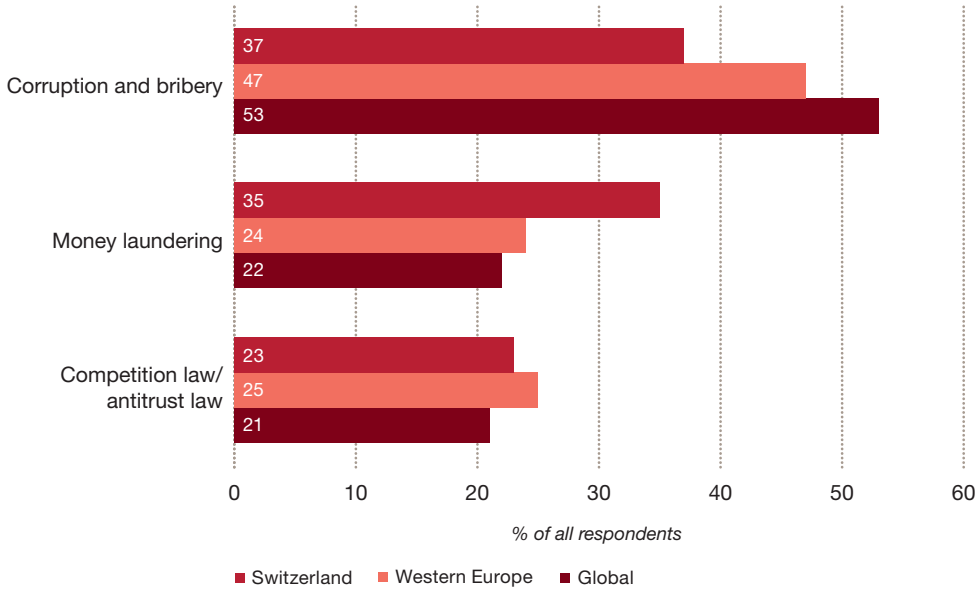
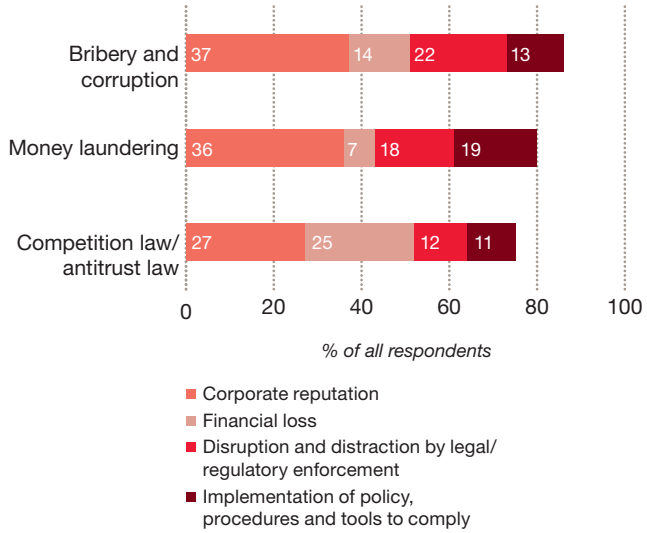



**Figure 10: Perceived most severe impact of government enforcement-related crimes**

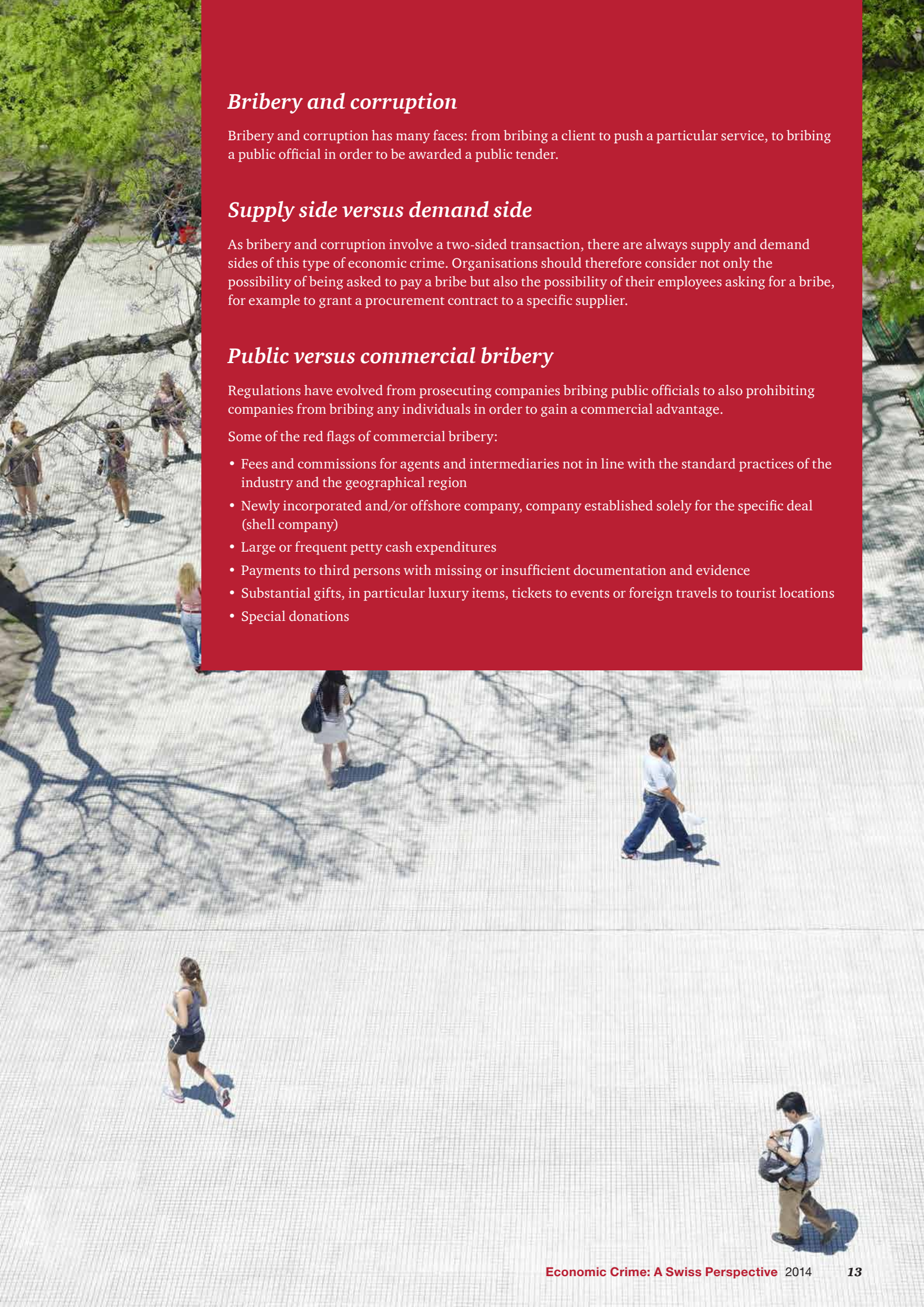



## The associated costs

We also asked Swiss companies what they perceived to be the most severe impact of government enforcement-related crimes on their organisation. More than a third of the respondents indicated that money laundering as well as bribery and corruption have the greatest negative impact on corporate reputation. About one-fifth of the participants also mentioned the disruption and distraction caused by legal/regulatory actions in connection with government enforcement-related crimes [Figure 10].

With respect to anti-competitive behaviour, 27% of the respondents also mentioned corporate reputation. However, almost as many respondents (25%) said financial loss represented the most severe impact. This is not surprising, given the number of severe penalties imposed on organisations for anti-competitive behaviour. It is interesting to note that financial loss is also worsened by a decrease in profits when anti-competitive practices are ceased as a result of antitrust investigations.

This demonstrates that economic loss is not the only concern organisations have when combating fraud. Respondents clearly pointed at the damage to corporate reputation and additional regulatory burden on their business activities that result from government enforcement-related crimes. This trend appears to be very similar on a global level.



## *Bribery and corruption*

Bribery and corruption has many faces: from bribing a client to push a particular service, to bribing a public official in order to be awarded a public tender.

## *Supply side versus demand side*

As bribery and corruption involve a two-sided transaction, there are always supply and demand sides of this type of economic crime. Organisations should therefore consider not only the possibility of being asked to pay a bribe but also the possibility of their employees asking for a bribe, for example to grant a procurement contract to a specific supplier.

## *Public versus commercial bribery*

Regulations have evolved from prosecuting companies bribing public officials to also prohibiting companies from bribing any individuals in order to gain a commercial advantage.

Some of the red flags of commercial bribery:

- Fees and commissions for agents and intermediaries not in line with the standard practices of the industry and the geographical region
- Newly incorporated and/or offshore company, company established solely for the specific deal (shell company)
- Large or frequent petty cash expenditures
- Payments to third persons with missing or insufficient documentation and evidence
- Substantial gifts, in particular luxury items, tickets to events or foreign travels to tourist locations
- Special donations

*67% of our respondents stated that their perception of cybercrime risk increased during the last 24 months.*

# Cybercrime – here to stay

## Cyber threat and Switzerland

It is generally accepted that today's ever-increasing dependency on technology has made the corporate landscape more complex and brought the threat of cybercrime progressively closer to our doorstep. Cybercrime was highlighted in our previous survey in 2011. As there are no borders in cyberspace, this allows fraudsters to use communication pathways created by the government and Internet service providers (ISPs) to exploit national infrastructure, our local businesses, and government entities. To date, there have been no disastrous cyber-attacks on Switzerland; however, our experience shows that cyber threats have reached our networks and thereby illustrate a basic truth: the precariousness of operating in a compromised digital environment.

Attacks on Swiss networks are not likely to peak in 2014 but instead will continue to evolve and increase in the years ahead – not because of any specific threat group or persistent vulnerability, but because of the unique Swiss corporate landscape mentioned earlier. Invading Swiss networks and stealing from Swiss financial institutions or corporations online is far less risky than committing the crime in person.

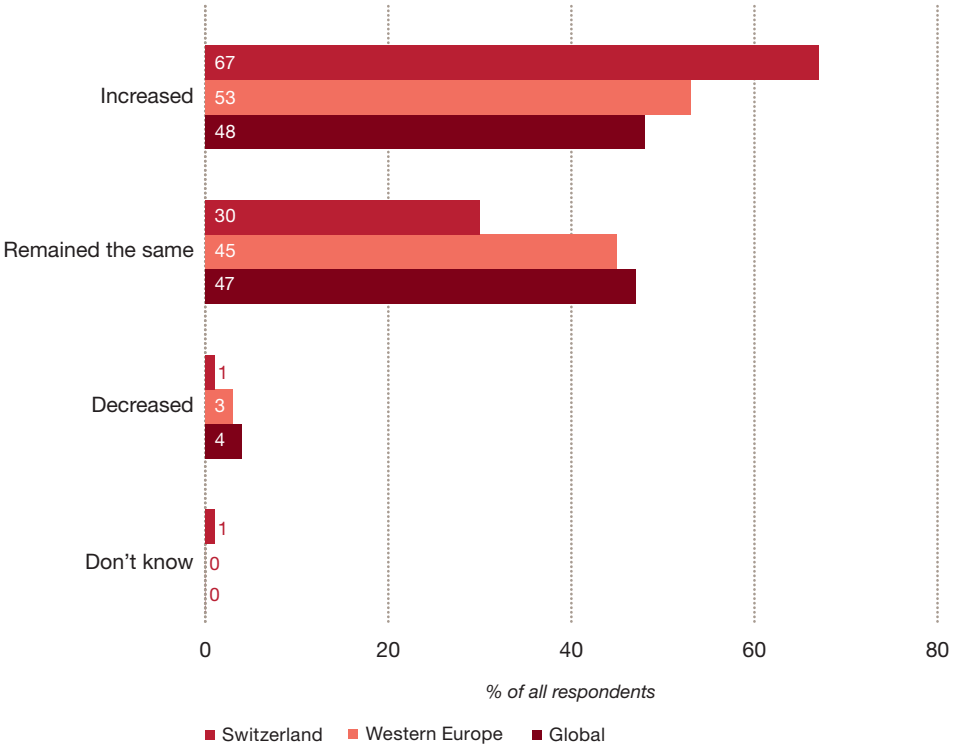
Although the risks in cyberspace can be managed, unfortunately they cannot be eliminated. Over the past 24 months, Swiss companies have started to understand that the goal is to mitigate rather than attempt to eliminate the damage and disruption that threats can do to the business. The Swiss findings of our current survey show an increase of awareness with regard to cyber risks. However, Switzerland still lags other major industrialised nations in addressing the risks cyber attacks pose to their companies.

### *Cybercrime – The costs we know of and those we don't*

The 2011 report was the first in our series to highlight cybercrime as a high-level threat to organisations. This year's survey confirms the significant, continued impact of this crime on businesses, with one in four of all respondents that were affected by fraud, reporting they have experienced cybercrime as a type of economic crime in the past 24 months. On the other hand, the results also show that almost the same percentage of respondents (23%) are not actually aware of how much cybercrime has cost them during that time frame. In our estimation, this reflects the current state of awareness of cybercrime in Switzerland. As the degree of awareness increases in the coming years, the ability to quantify the financial impact will also increase.

In a sign that Swiss organisations are taking this threat more seriously, our survey indicates that the perception of cybercrime is increasing at a faster pace than that of reported actual occurrences. This year, 67% of our respondents said their perception of cybercrime risk increased in the survey period [Figure 11], in comparison to 52% in 2011.

**Figure 11: Perception of cybercrime threats over the past 24 months**




### *The risks of not knowing*

While it is concerning enough that one-quarter of the respondents affected by economic crime reported cybercrime, we must also consider that a significant percentage of those who did not report cybercrime may have suffered such an event and not even known about it. And that is rather alarming. Further complicating the picture is that even when it is detected, cybercrime often goes unreported. Outside of breaches in regulated areas, such as identity theft, there are few regulatory conventions requiring disclosure. And often – such as in the case of theft of key intellectual property – there may be compelling competitive reasons for organisations to keep such losses confidential.

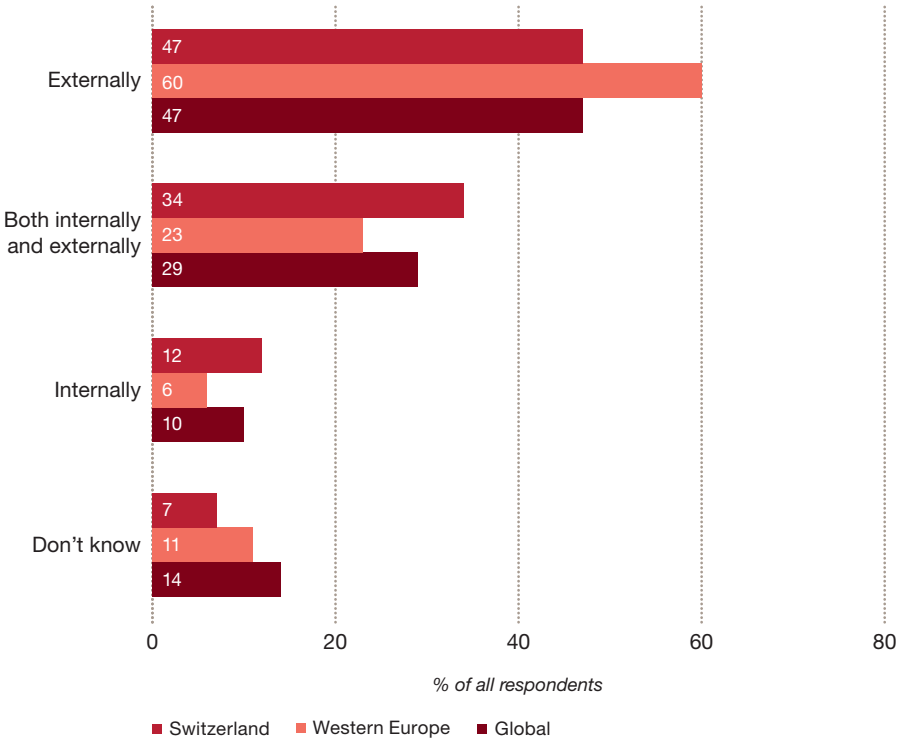
For example, if a confidential bid-planning document were accessed by cybercriminals and utilised by rivals to gain an advantage, would an organisation disclose the incident? Are organisations adequately defending themselves against such cybercrime breaches, and if they were discovered, how would they value the loss?

The bottom line is that much of the damage wrought by these types of attack is not disclosed, either because it is not known, difficult to quantify, or because it is not shared. Naturally, this kind of operational murkiness poses risks for a global business ecosystem that is increasingly reliant on both technology and intellectual property yet would benefit from such transparency.

### *Cyber threats from outside your network*

When asked where the cyber threats will come from in the next 24 months, close to half of the Swiss respondents believe that they will come from outside their organisation, which reflects the trend globally. Compared to their global and Western European counterparts, Swiss respondents are also more sceptical with regard to cyber threats that come from within their organisation. However, this is to be expected, seeing as how the risk of data theft at Swiss financial institutions by internal perpetrators has been a hot topic in the past several years [Figure 12].

**Figure 12: Source of cybercrime threat**



Similar to the global findings, Switzerland has experienced an overall increase in concern that cyber threats will affect all areas of company, including reputational loss, financial loss, legal and investigation costs, regulation risks, intellectual property theft, and service disruption. In each of these categories, more than 60% of the respondents are either concerned or very concerned. The highest level of concern at Swiss companies pertains to reputational damage, closely followed by theft or loss of personal identifiable information (PII) [Figure 13].

### *Targeting the money*

The financial services industry, with 43% of fraud-affected organisations noting cybercrime, is the clear leader in reported cybercrimes [Figure 14]. It is important to note that large, regulated financial institutions have higher levels of transparency and system safeguards, which may increase the chance of a breach being detected. Financial institutions also are an appealing target for cybercriminals because they provide large amounts of customer/financial information online that can potentially be accessed – and sold on illegal markets – by those with the right tools and skills.

**Figure 13: Concerns about the effects of cybercrime on the organisation**

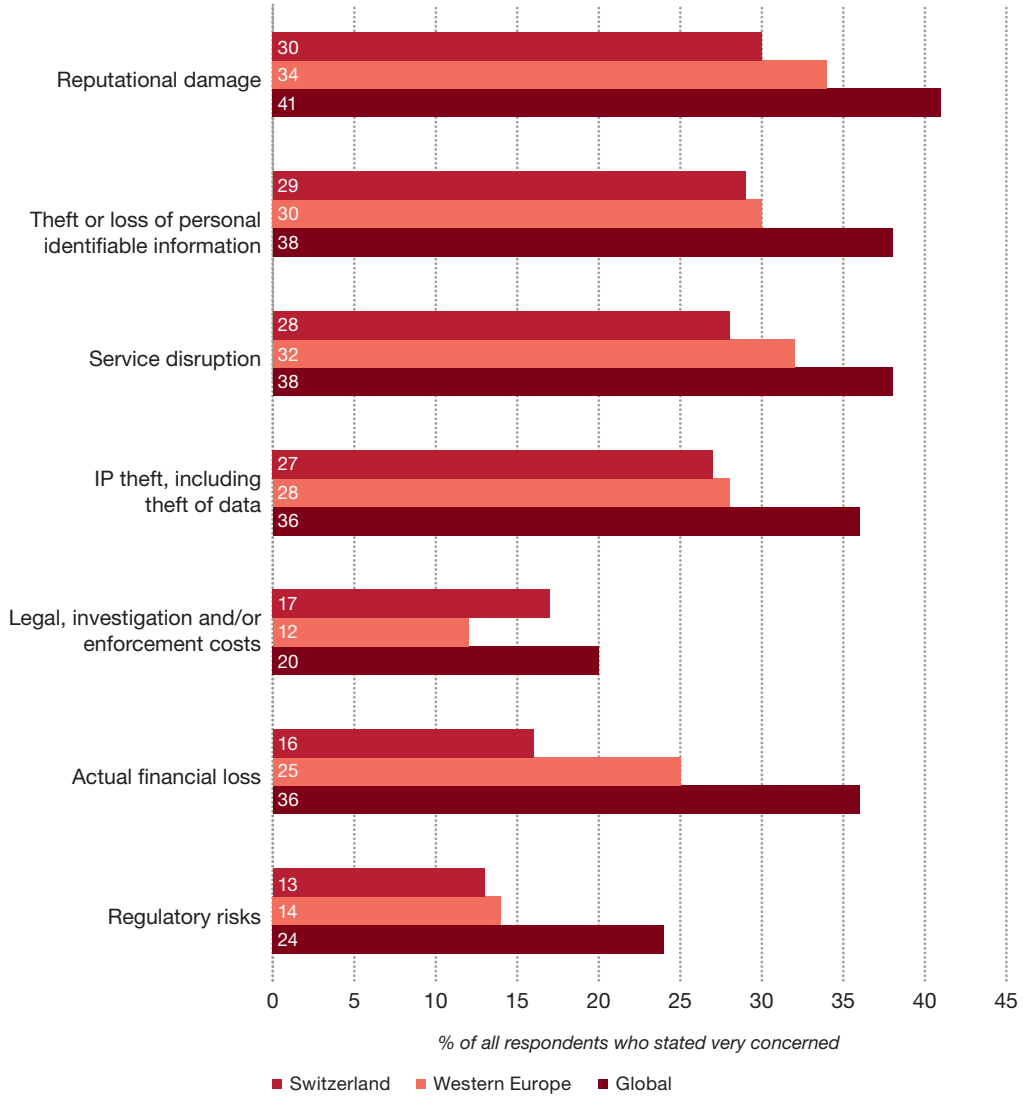
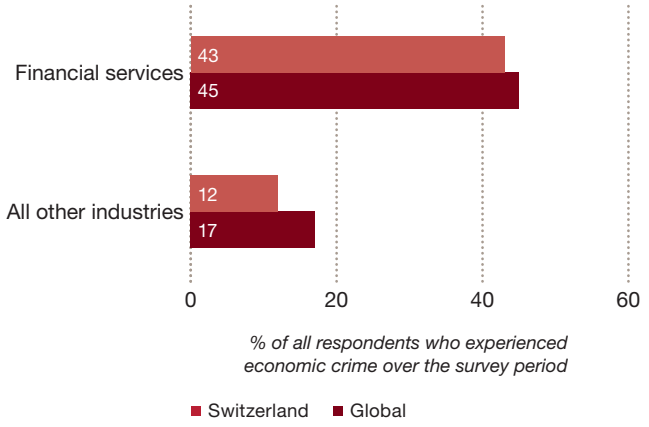


**Figure 14: Cybercrime in the financial services industry and across the corporate landscape**




### *The human element of technology problems*

Even though organisations are generally aware of the types of cyber threats they face, many do not truly understand the capabilities of cyber criminals, what their targets might be and what the value of those targets are. While our 2014 Global CEO Survey reports that nearly half of the CEOs (47%) are concerned about cyber security threats (including lack of data security), cyber security is now trending lower on the scale of CEO concerns. Yet they continue to make their critical data available to management, employees, vendors, and clients on a multitude of platforms – including high-risk ones such as mobile and cloud – because the economic and competitive benefits appear to be so compelling.

While nobody expects those benefits to go away or for organisations to shrink their digital data footprint, with ever more data more accessible on an ever-growing number of platforms, it is clear that valuable data will remain under attack and that the cost of security breaches will continue to be steep. The truth is, in today's global digital domain the landscape is constantly changing and the sophisticated adversary takes advantage by attacking new vulnerabilities – which is why it is essential that organisations at least try to keep pace with the raiders who threaten them. Ultimately cybercrime is not truly a technology problem. It is a human problem – a strategy and process problem.

### *Cybercrime outlook for Switzerland*

In every region surveyed, between a quarter and a third of the organisations told us they believe they will likely encounter cybercrime in the near future. It is interesting to contemplate whether these readings are grounded in a growing realisation on the part of organisations that they may be falling behind in detecting attacks, or whether they reflect a broader, well-founded sense of anxiety about cybercrime.

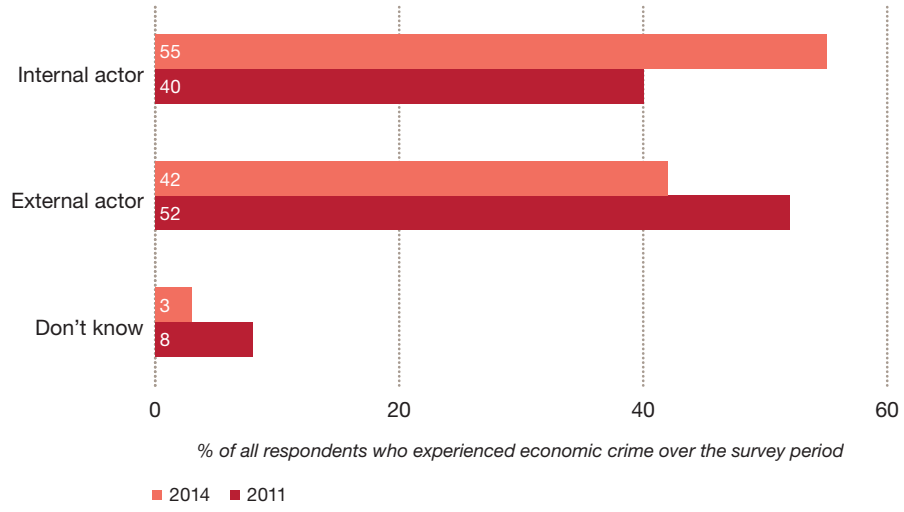
Each year Swiss organisations are becoming more aware of the cyber threat they face. Ironically, as Switzerland continues to prosper, these favourable conditions will attract cyber criminals whose intent is to exploit our domestic organisations and infrastructure.

*55% of reported fraud incidents were committed by someone within the organisation.*

# The thief in our midst

One of the steps in protecting organisations against the possibility of fraud is to gather as much information as possible about the perpetrators. Knowing who they are and where they come from is essential in pinpointing weaknesses in the organisation's processes and internal controls. Of those Swiss organisations that experienced economic crime in the past 24 months, 55% said the fraud was committed by someone within the organisation [Figure 15], an increase from 40% in 2011. On a global scale, we are observing the same trend, with 56% of economic crimes perpetrated by an internal perpetrator.

**Figure 15: The main perpetrator of the fraud**

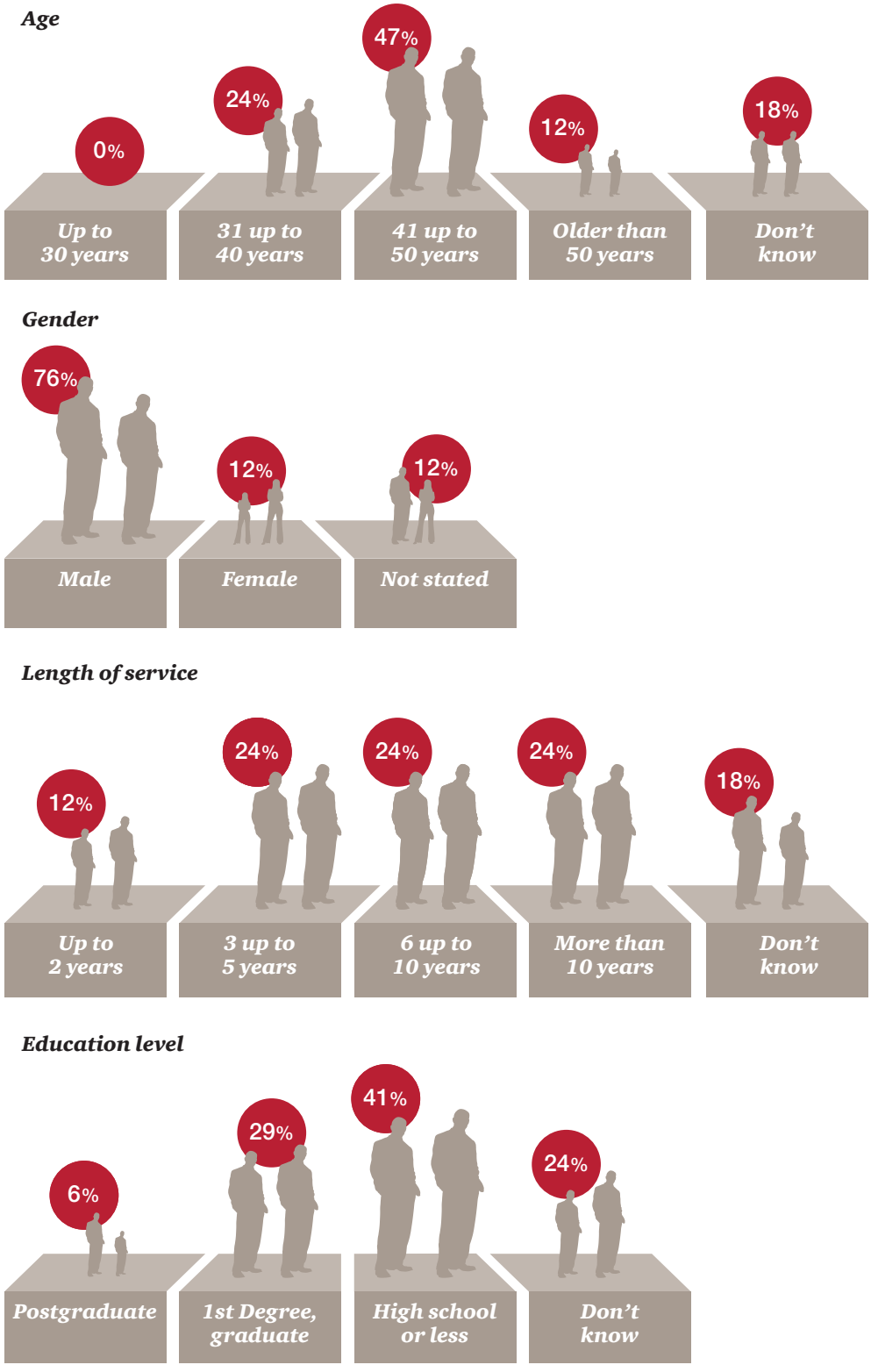



## The fraudster profile

### *The internal fraudster*

Asked about the internal perpetrator, 76% of the respondents said the culprit was a male, up from 50% in 2011. Interestingly, we note that the fraudster profile depicted by this year's survey is in line with the traditional profile encountered by anti-fraud practitioners – where the majority is male, has been with the company for several years, and is therefore familiar with the company's processes and controls [Figures 16–19].

## Figure 16–19: Age, gender, length of service and education level of internal perpetrator



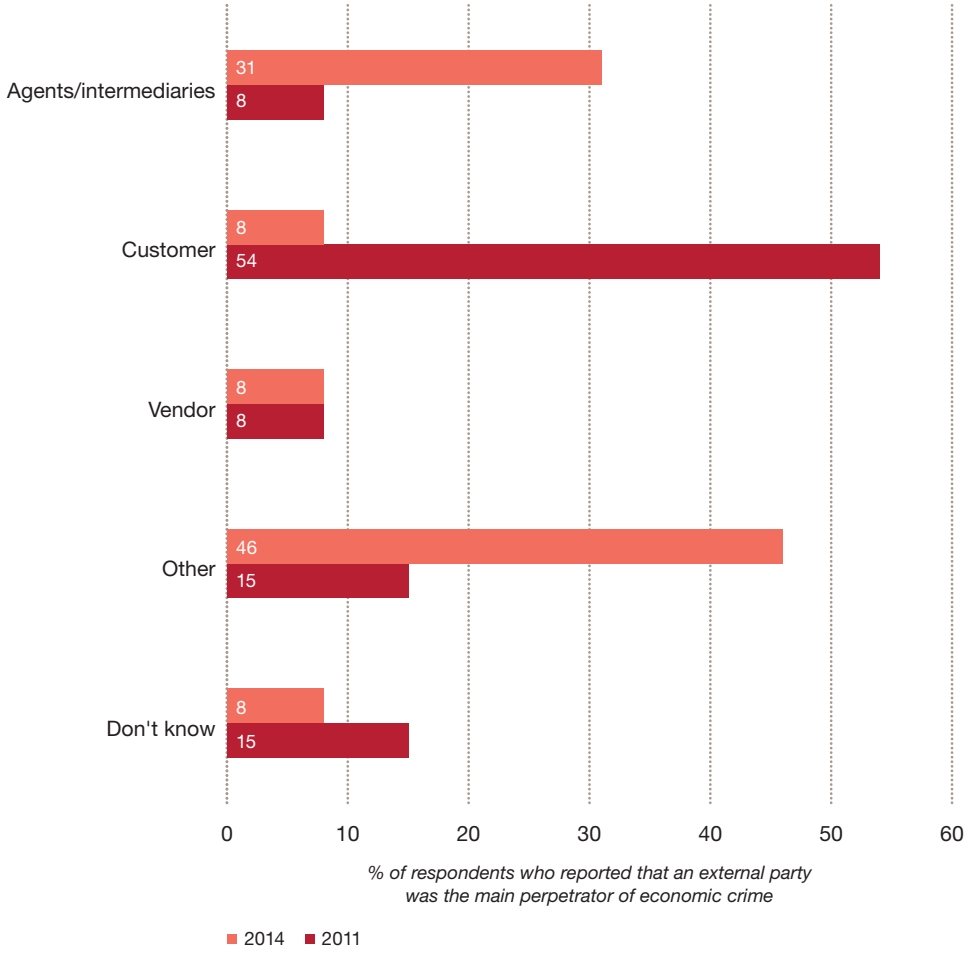

*% respondents who reported that an internal party was the main perpetrator of economic crime*

■ 2014

### *The external fraudster*

In terms of the external fraud perpetrator, there have been significant changes since our previous survey. On one hand, the amount of fraud committed by agents and intermediaries has increased from 8% as reported in 2011 to 31% in the past 24 months and, on the other, fraud committed by the customer decreased from 54% to only 8%. Although organisations have become more effective in choosing their customers, they may have not applied the same methods when selecting their agents and intermediaries, which demonstrates the importance of third-party due diligence checks.

**Figure 20: External fraudster**

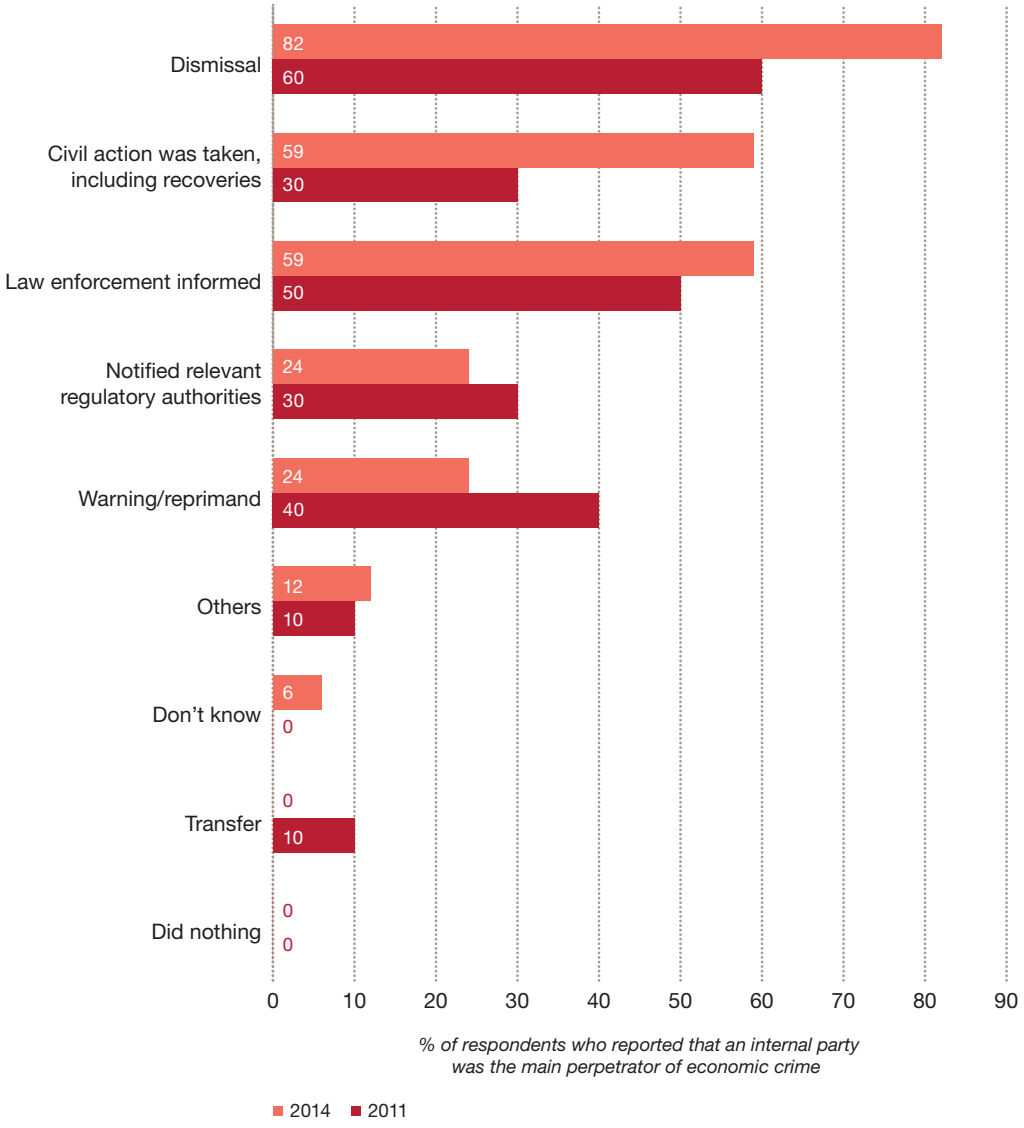



It is also interesting to note that a significant proportion of the external fraudsters in this year's survey do not fall into any of the main categories and were classified as "other" or "don't know" by our respondents. We believe that this trend may be related to the incidence of cybercrime, as 47% of respondents said the greatest risk related to this type of crime is posed by external parties.

## Did the punishment fit the crime?

Organisations have several options on how to deal with fraudsters once they have been discovered. For internal infractions, disciplinary measures may start with a warning/reprimand and can, depending on the gravity of the crime committed, extend to dismissal. For external infractions, businesses may decide to cease the business relationship. Whilst in the previous survey the Swiss organisations appeared to have taken a more lenient stance in comparison to the global average when it came to disciplinary action, this year's survey suggests that they are taking a tougher stance. An increasing number of Swiss organisations take proactive measures aimed at protecting themselves against fraud and recovering damages, thereby going beyond a simple warning/reprimand or transfer of the fraudster within the organisation.

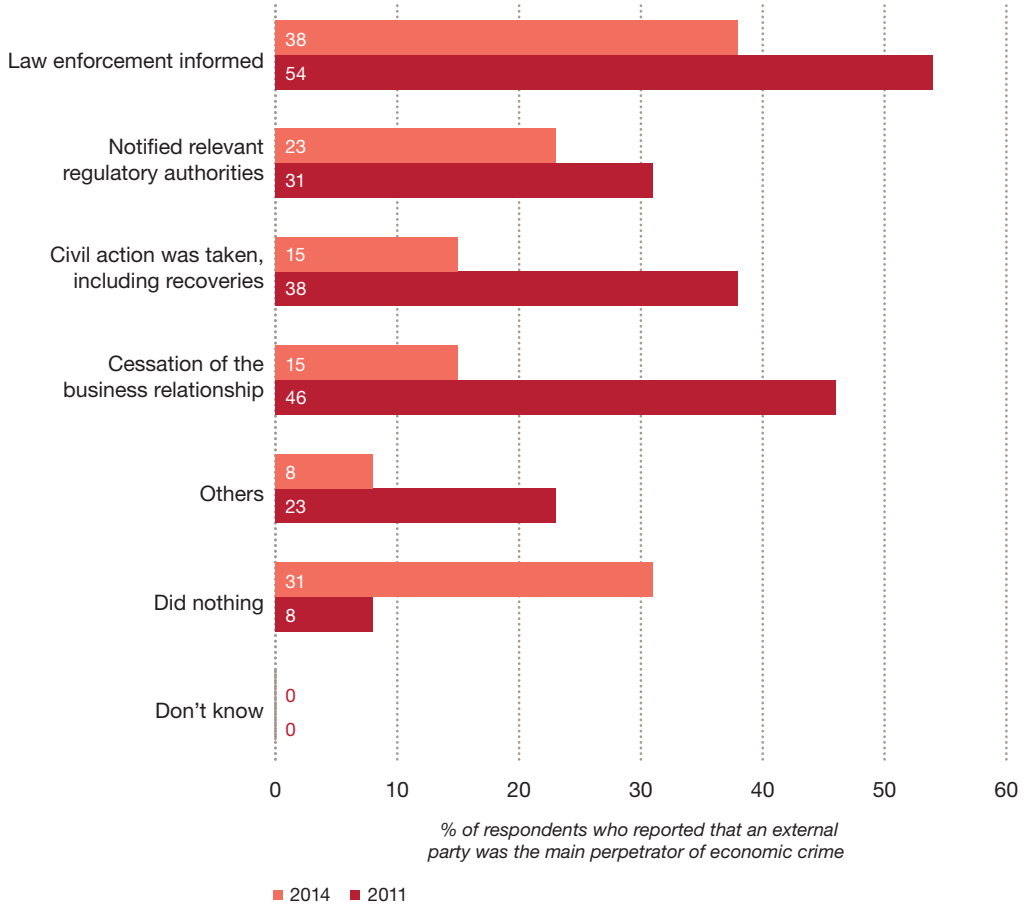
**Figure 21: Actions taken against internal fraudsters**




In fact 82% of the Swiss respondents chose to dismiss the individual involved in internal fraud and a further 59% took civil action against the perpetrator as well as sought to recover damages. This is more than a 20% increase for both of these measures compared to the 2011 readings. Furthermore, Swiss organisations are tougher on their perpetrators in comparison to respondents globally, where 79% of the companies dismissed the internal perpetrator and 44% initiated a civil action.

Surprisingly, this year's survey shows that Swiss organisations are less consistent when dealing with external perpetrators. Even though they appear to have improved their ability to identify external fraudsters, a striking 31% of the Swiss respondents who had been affected by external fraud took no action against the fraud perpetrator [Figure 22]. This is a significant increase in comparison to 2011, which may be explained by the recent rise of cybercrime in Switzerland where this type of fraud usually involves an unknown external party. Even though organisations are able to classify the type of perpetrator (for example a hacker), it would be difficult to uncover their identity, which makes taking specific measures against them rather challenging.

**Figure 22: Actions taken against external fraudsters**




Moreover, only 15% of the Swiss participants chose to cease the business relationship and a further 15% took civil action against the external perpetrator, a rate that is lower than the global average. In addition, 38% of the Swiss respondents reported having informed law enforcement authorities, which is also the measure most commonly taken by respondents globally (61%).

## To catch a thief – methods of detection

There are many different ways to detect that an economic crime has occurred. The most straightforward method is to implement well-designed internal control mechanisms. The next step is to bolster the procedural detection system with a corporate environment that fosters zero fraud tolerance, given that a human element is essential in detecting fraud. However, we also recognise that fraud can be discovered by accident, perhaps by parties outside the realm of the organisation itself and beyond the influence of management.

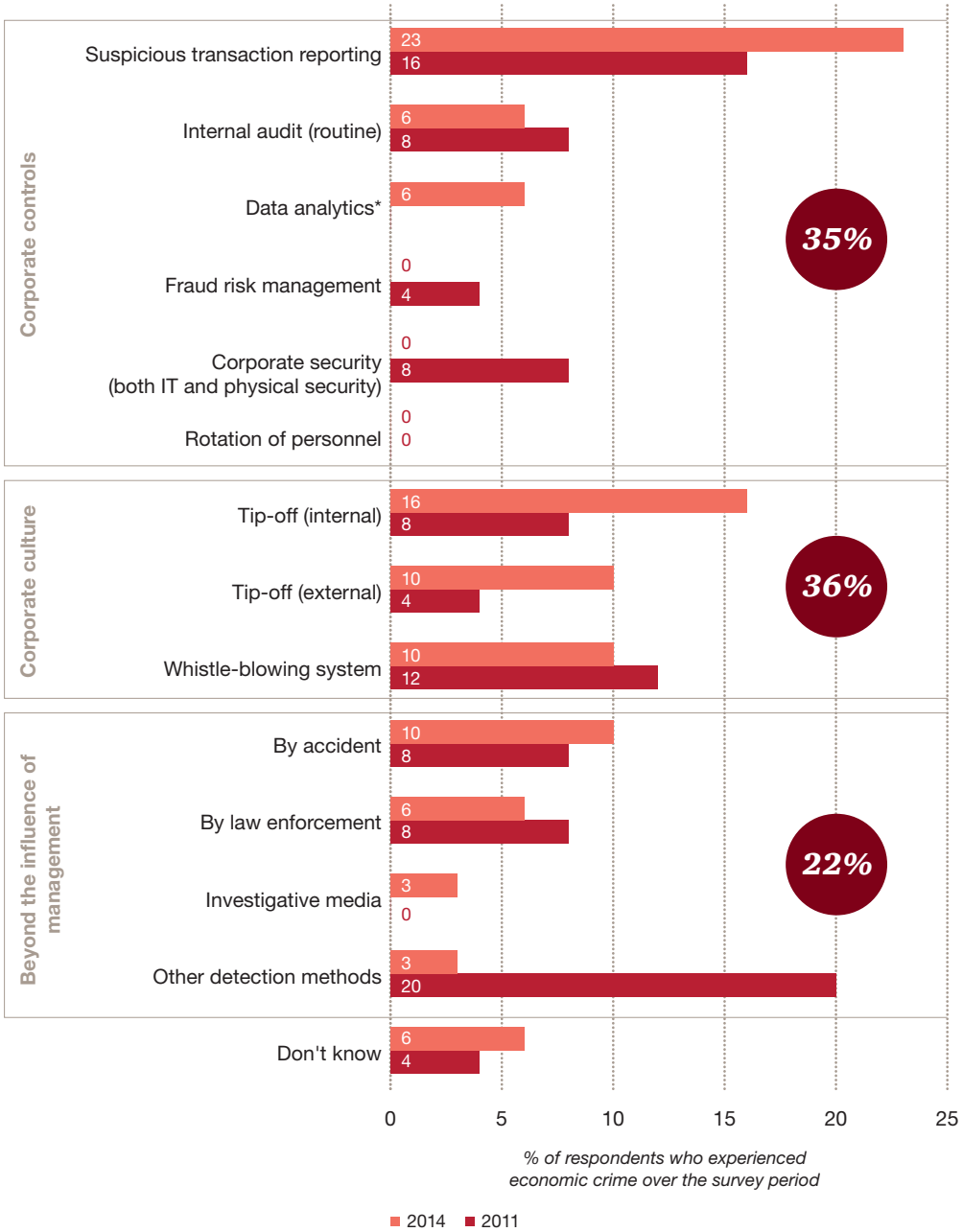
This year's survey shows that corporate controls as well as culture were more or less on a par in terms of their effectiveness, whereby more than one in three of the reported fraud incidents were detected by both of these methods independently. It is interesting to note that, whilst the overall effectiveness of corporate controls remained relatively unchanged during the survey period, we have observed an increase in fraud detected by corporate culture, i.e. from 24% in 2011 to 36% in the past 24 months [Figure 23].

In particular, there has been a significant rise in detection through data-driven fraud discovery methods and through tip-offs. In fact, 29% of the Swiss organisations affected by economic crime stated that the fraud was initially detected by suspicious transaction reporting or data analytics (data-driven fraud detection methods), compared to only 16% in 2011. A further 26% of the respondents mentioned external and internal tip-offs, a 14% increase over the 2011 figures.

The third key detection method in Switzerland is attributable to the whistle-blowing system with 10% of the respondents affected by fraud reported that it was initially detected through this method, compared to only 5% globally. Furthermore, over half of all Swiss respondents (52%) reported having a whistleblowing mechanism in their organisation, which is lower than then the global average (62%) and may suggest that Swiss companies have more sophisticated whistleblowing processes. Interestingly, our respondents' perception of the effectiveness of this process does not actually reflect reality as 51% of them rate their company's whistleblowing mechanism as only slightly effective or not effective at all.

Overall, the survey reveals that participating Swiss organisations may have increased the quality of their corporate controls and/or introduced new, more effective fraud-detection methods since the last survey. In particular, this year's survey demonstrates the progress made by Swiss companies in developing an anti-fraud corporate culture. This highlights the increased awareness of organisations of the need to improve the environment where anti-fraud controls operate, which starts by setting an appropriate tone at the top, fostering a "no tolerance for fraud" corporate culture, and heightening transparency within the company.

**Figure 23: Methods of detection**




* Data analytics was added as a new category in the 2014 Survey.

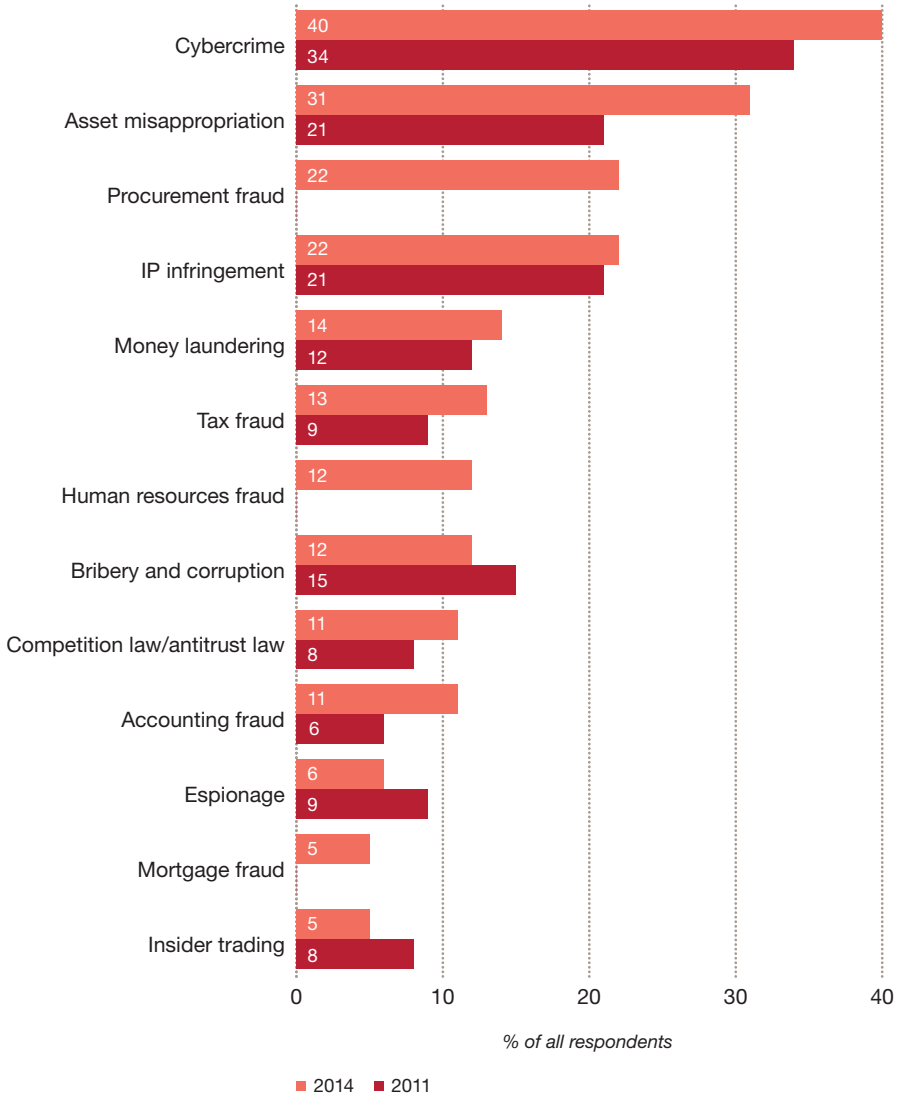
*Swiss respondents expect cybercrime, asset misappropriation and procurement fraud to be the top three types of fraud affecting their organisation in the next 24 months.*

# The outlook – perception versus reality

It is quite clear that over half of the Swiss respondents are rather confident and believe that they will not fall victim to economic crime in the next 24 months. We do, however, note growing concern compared to 2011 especially with regard to cybercrime, where 40% of the respondents believe they will experience this type of crime in the future, a reading that exceeds even the easiest fraud to commit, i.e. asset misappropriation. We also note that respondents are concerned about procurement fraud. This type of fraud can be expected to remain amongst the top five economic crimes in the years to come [Figure 24].

In addition, due to growing concerns and despite the strengthening of corporate controls and corporate culture, it appears that Swiss companies took a less complaisant stance in terms of fighting fraud over the past 24 months.

## Figure 24: Perception of future likelihood of economic crime



# About the survey

The 2014 Global Economic Crime Survey was completed by 5,128 respondents (compared to 3,877 respondents in 2011) from 95 countries (compared to 78 countries in 2011). Of the total number of respondents, 50% were senior executives of their respective organisations, 35% represented listed companies and 54% represented organisations with more than 1,000 employees.

The Swiss survey was completed by 83 organisations, of which 42% are listed companies. Of the total number of respondents more than half were board members or senior executives within their organisations.

Terms and definitions can be found in the Global Economic Crime Survey.

Please note that due to rounding, the results as presented in this report may not add up to a 100% where applicable.

*www.pwc.ch/crimesurvey*

# Contacts and contributors


### *Forensic Services in Switzerland*

**Gianfranco Mautone**
Partner
Forensic Services
+41 58 792 17 60
gianfranco.mautone@ch.pwc.com

**Ralf Baumberger**
Director
Forensic Services
+41 58 792 17 63
ralf.baumberger@ch.pwc.com

**Roman Gauch**
Director
Forensic Services
+41 58 792 17 66
roman.gauch@ch.pwc.com

**Thomas Koch**
Director
OneSecurity
+41 58 792 29 54
thomas.koch@ch.pwc.com

**Sebastian Ahrens**
Senior Manager
Forensic Technology Services
+41 58 792 16 28
sebastian.ahrens@ch.pwc.com

### *Swiss survey team*

**Selma Krkić**
Manager
Forensic Services
+41 58 792 20 86
selma.krkic@ch.pwc.com

**Kevin Kirst**
Manager
OneSecurity
+41 58 792 28 77
kevin.kirst@ch.pwc.com

**Silvia Svihrová**
Assistant Manager
Forensic Services
+41 58 792 46 82
silvia.svihrova@ch.pwc.com



**PwC Switzerland** helps organisations and individuals create the value they are looking for – serving them with over 2,600 employees and partners working in 15 different offices throughout Switzerland. We are part of a network of firms in 158 countries with more than 180,000 people who are committed to delivering quality in assurance, tax & legal and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.ch.

**"PwC"** refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. For further details, go to www.pwc.com/structure.

© 2014 PwC. All rights reserved. "PwC" refers to PricewaterhouseCoopers AG, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.

*PwC's 2014 Global Economic Crime Survey*
**February 2014**

# *Confronting the changing face of economic crime*

***4th***
South African edition

***134***
respondents from organisations in 17 industry sectors provide insights into economic crime in South Africa.

pwc

*www.pwc.co.za/crimesurvey*

*The PwC Global Economic Crime Survey continues to be the world's leading research programme into economic crime*

# Contents

*Economic crime remains a serious issue affecting South African organisations*

# *Foreword*

PwC conducts a Global Economic Crime Survey every two years. Separate reports are published by various countries in addition to the overall global results report. I am pleased to present the South African edition of the Global Economic Crime Survey Survey, in which we achieved a record 134 responses across 17 industry sectors. The diversity of responses provides a more representative data set, which in turn produces a more complete picture of economic crime in South Africa.

As in previous years, the purpose of our survey is to inform South African business leaders about developments in the continuously changing landscape of economic crime in our country and to encourage debate around strategic and emerging issues in this sphere.

Our 2014 survey shows that economic crime remains a serious issue affecting South African organisations. We hope that the information contained in this survey will assist readers in their ongoing endeavours to curb economic crime.

We would like to express our sincere appreciation to all those that participated in the survey as well as the partners and staff who contributed their time and insights to this report.

**Louis Strydom**
National Forensic Services Leader

# *Key findings*

- 69% of South African respondents indicated that they had experienced economic crime, which is nine percentage points higher than in 2011.
- The percentage of South African respondents reporting fraud has increased from the previous survey (2011) for the first time since the inception of the survey.
- There has been an alarming shift in the perpetrator profile in South Africa. Senior management is now the main perpetrator of economic crimes committed by insiders.
- The typical perpetrator of insider fraud in South Africa is:
  - Male;
  - Aged between 31 and 40;
  - Has obtained a university degree; and
  - Has been with his employer for more than 10 years.
- Bribery & corruption has been the fastest growing economic crime category in South Africa since 2011.
- Globally, the construction, energy and mining sectors experience the most bribery.
- South African organisations suffer significantly more procurement fraud, human resources fraud, bribery and financial statement fraud than organisations globally.
- Competition law infringement is poorly understood by South African organisations. A significant percentage of respondents were unsure whether their organisations had experienced such a contravention and did not know what the potential consequences of an infringement would be.
- Formal fraud risk management programmes have become the most effective fraud detection method. Despite this, a significant portion of South African organisations do not carry out fraud risk assessments.

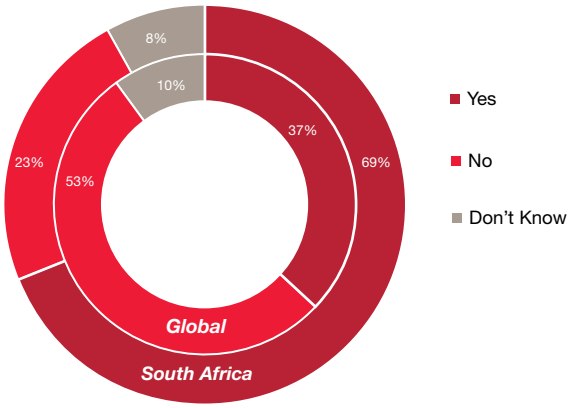
*Economic crime remains a serious challenge to business leaders, government officials and private individuals in South Africa with 69% experiencing some form of economic crime in the last 24 months.*

# Introduction

The PwC Global Economic Crime Survey continues to be the world's leading research programme into economic crime. In this edition of the survey, 5 128 senior businessmen and women from 93 countries participated in an online survey during the fourth quarter of 2013.

The latest results show that economic crime remains a serious challenge to business leaders, government officials and private individuals in South Africa – 69% of South African respondents indicated that they had been subjected to some form of economic crime in the 24 months preceding the survey, compared to 37% of global respondents.

**Figure 1: Respondents subjected to economic crime over the past 24 months**



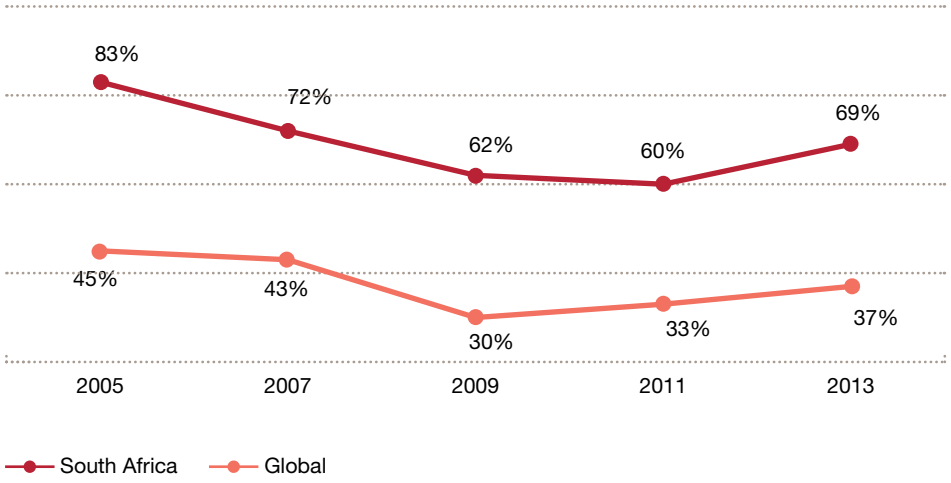

***Q: Has your organisation experienced any economic crime within the last 24 months?***

This is the first time since 2005 that the prevalence of economic crime has increased in South Africa. Prior to the current survey, South Africa had shown a diminishing trend in the incidence of economic crime.

Figure 2 shows that there was an increase in the overall incidence of fraud from 2009 to 2011 globally, while South Africa showed a decrease over the same period.

South Africa was affected less by the global economic slowdown of 2008 and this may have delayed the uptick in the overall incidence of economic crime in South Africa compared to the trend witnessed globally .

**Figure 2: Prevalence of economic crime since 2005**




***Q: Has your organisation experienced any economic crime within the last 24 months?***

*South Africa has experienced a higher incidence of every category of economic crime except intellectual property infringement and mortgage fraud.*

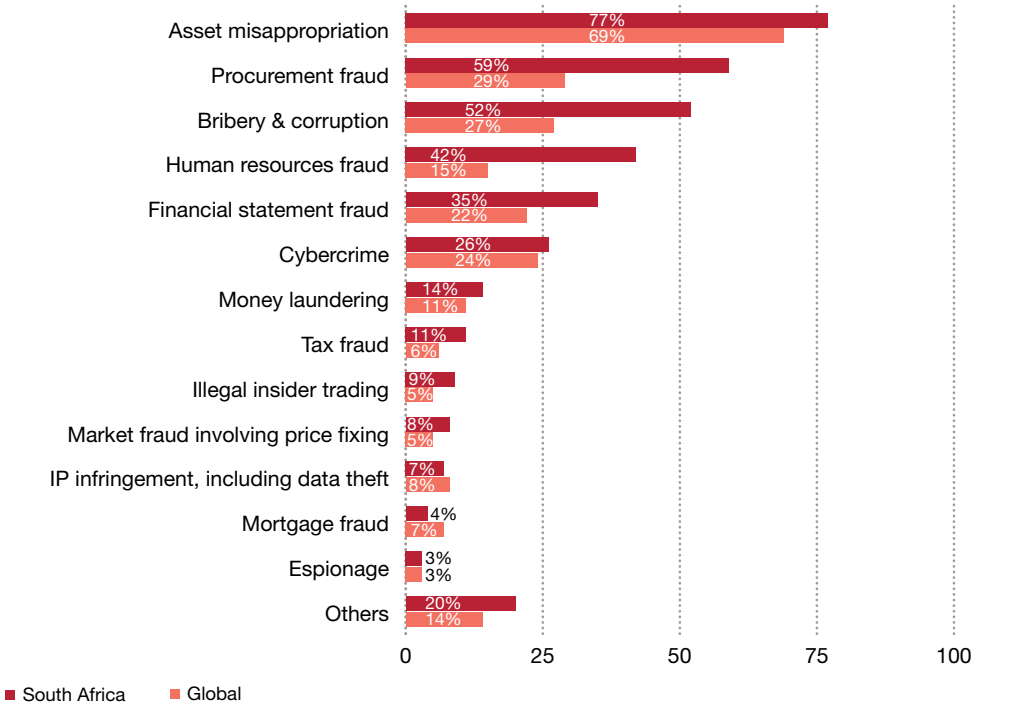
# *Profile of economic crime in South Africa*

Figure 3 depicts the incidence of different types of economic crime globally and in South Africa. We introduced three new categories for the first time in this survey: procurement fraud, human resources fraud and mortgage fraud.

In our last survey, asset misappropriation, bribery & corruption and financial statement fraud were the top three crime categories in South Africa.

This time, procurement fraud and human resources fraud were reported on separately and have come in as the second and fourth most prevalent among the former 'big three' crime categories.

**Figure 3: Types of economic crimes experienced in the past 24 months**




***Q: What types of economic crime has your organisation experienced within the last 24 months?***

South Africa has experienced a higher incidence of every category of economic crime except intellectual property infringement and mortgage fraud.

South African respondents report significantly more instances of procurement fraud, bribery & corruption, financial statement fraud and human resources fraud than their global counterparts. In the remaining categories, the distribution of economic crime in South Africa mirrors the global picture.

Two fraud categories that showed significant increases since our previous survey are bribery & corruption (up from 42% to 59%) and insider trading (up from 4% to 9%).

Despite the recent publicity surrounding collusion in the South African construction industry, market fraud decreased the most when compared to the 2011 survey results. Market fraud is difficult to detect and may be underreported.

### *Government-enforced crime categories: Bribery & corruption, money laundering, competition law infringements*

Some types of economic crime carry a greater degree of risk than others. Asset misappropriation has been the most common type of economic crime in South Africa since the inception of our survey.

The fallout from asset misappropriation is usually relatively small-loss of funds or assets impact the bottom line of the affected organisation. Other fraud types, especially those carried out by or on behalf of the organisation, and which attract enforcement actions from regulators in South Africa or elsewhere, create far greater problems for the affected organisations.

Bribery, money laundering and competition law infringements can trigger fines and criminal charges, but also invite a long trail of corrosive fallout.

### *Consequences of businesses perpetrating economic crime*

| | |
|---|---|
| Reputational damage | • Public disfavour<br>• Product/service boycotts<br>• Negative media attention<br>• Civil litigation<br>• Falling share prices |
| Financial damage | • Loss of future business<br>• Legal costs defending civil litigation/claims |
| Operational damage | • Disruptions caused by criminal/regulatory investigations<br>• Loss of critical talent pool and employee morale |

Organisations often fail to grasp the full financial impact of economic crime until after it has occurred – sometimes well after. This is especially true of crimes ostensibly committed on behalf of the organisation, as can be seen in our survey results. A large percentage of respondents stated 'I don't know' when asked to quantify the financial losses related to each of these three economic crimes.

### *Percentage of 'I don't know' responses*

| | |
|---|---|
| Bribery & corruption | 30% |
| Money laundering | 40% |
| Competition law infringements | 41% |

Occurrences of economic crimes perpetrated by businesses are often indicative of larger organisational problems such as failure of key internal controls or lack of appropriate tone from the top.

Fortunately, top management appears to understand this: in our 17th Global CEO Survey, South African CEOs mentioned bribery & corruption among the risks they were most concerned about.

### *Bribery & corruption*

Just over half of South African respondents (52%) who experienced economic crime during the survey period, suffered bribery (an increase of ten percentage points since our 2011 Survey).

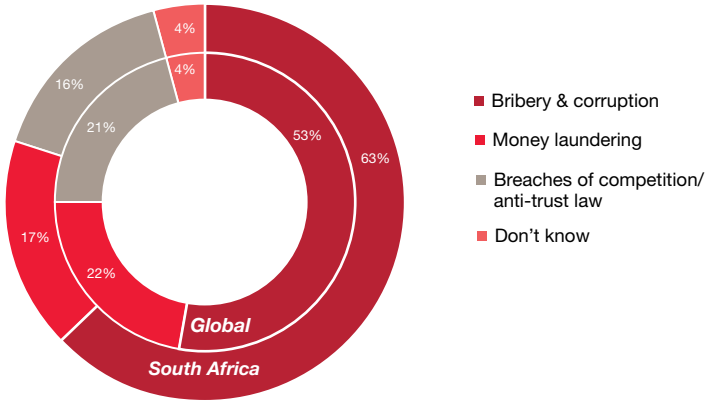
*Bribery & corruption is a major problem in Southern Africa*

This is the third most prevalent economic crime type in South Africa.

PwC's 17th Global CEO Survey released in January 2014 found that 86% of South African CEOs are either 'somewhat' or 'extremely' concerned about corruption.

We asked respondents to indicate which regulatory enforcement-related risk they were most concerned about. Figure 4 shows that bribery & corruption was by far their greatest worry.

**Figure 4: Regulatory enforcement-related risks respondents rank as greatest concern**




***Q: In doing business globally, which of the following three issues do you perceive to be the highest risk to your organisation?***

These results indicate that bribery & corruption is a major problem, despite high levels of awareness of this form of economic crime in Southern Africa.

This is further highlighted by the fact that more than a quarter of South African respondents reported that their organisations had been asked to pay a bribe in the last 24 months.

In addition, one fifth of South African respondents believe they lost a business opportunity because a competitor had paid a bribe.

While not the most prevalent economic crime in South Africa, bribery & corruption may pose the greatest risk to organisations doing business across borders, especially if they are affiliated with the USA or the UK. This is because offences are often pursued by regulators across borders and laws such as the US Foreign Corrupt Practices Act and the UK Bribery Act have far-reaching ambits.

The results of our 17th Global CEO survey indicate that South African CEOs have significant existing operations in the rest of Africa or ambitions to expand into Africa: 94% of CEOs stated that they expected to grow their operations into the rest of Africa in the next 12 months.

Senior management should therefore ensure that robust preventative and detective controls are implemented for operations in other countries, especially those where the local practices and customs may be more accepting of bribery.

Globally, the engineering & construction and energy, utilities & mining sectors reported the highest levels of corruption across all industries (50% and 20% respectively).

It is, however, important to note that the increased likelihood of these industries reporting bribery & corruption may, in part, be attributable to their heightened awareness of this risk and the implementation of more stringent controls.

We asked respondents what consequences concern their organisations most with regard to bribery & corruption. The top two concerns for South African respondents were financial loss (46%) and corporate reputation (30%).

### *Confronting the risk of bribery & corruption*

| **Regardless of industry or region of operation, we believe organisations should focus on these four areas to diminish the risk of bribery & corruption.** | |
|---|---|
| **Management and tone at the top**<br><br>While compliance is everyone's responsibility, setting the right tone must start at the top. Senior management should have an understanding of anti-corruption statutes and give a clear and consistent message that bribery will not be tolerated and adequate resources will be allocated to combat the threat. | **Control environment**<br><br>Staying on top of corruption risk requires a robust communication plan and vigilant internal enforcement procedures. A formal code of conduct, employee training (including on compliance-sensitive issues such as gifts and entertainment) and a system of controls monitoring suspicious transactions should be in place. Organisations are only as compliant as their weakest link so business partners, vendors and other third parties must be vetted and monitored. |
| **Risk assessment**<br><br>Both the business and compliance environment are constantly evolving. That's why it is essential that periodic risk assessments are conducted and that any previously identified risks have been addressed. | **Evaluating effectiveness**<br><br>Risk assessment and control plans, of course, do not of themselves lead to compliance. Due diligence reviews, periodic visits from management to high-risk locations, compliance reporting to the board, hotline follow-ups, business-partner audits should all be maintained and re-evaluated on an ongoing basis as part of an effective internal compliance programme. |

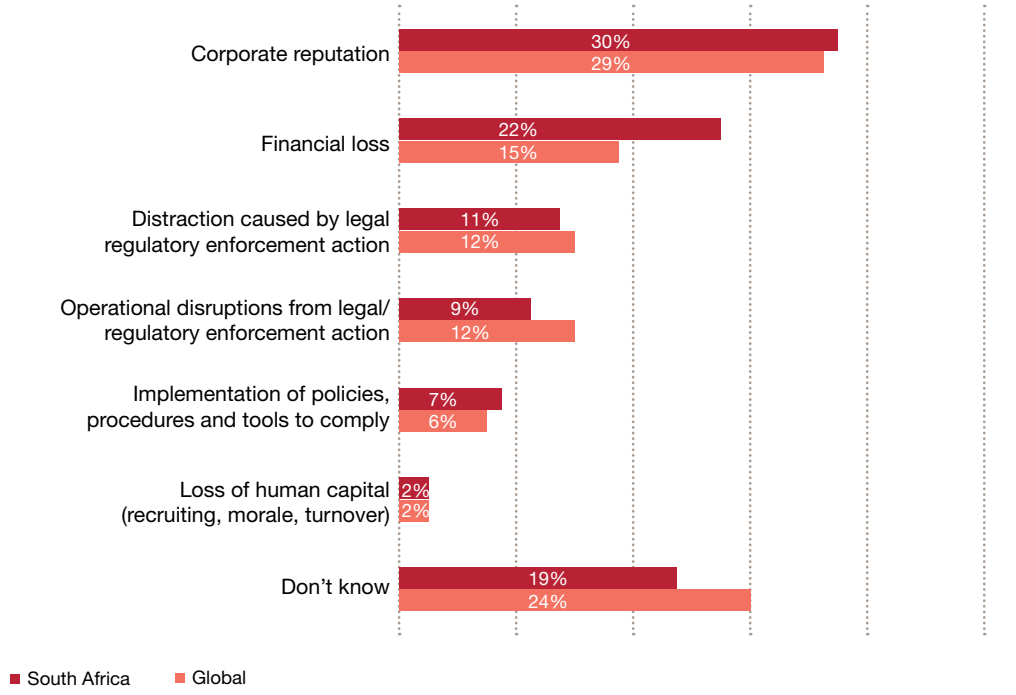
### *Money laundering*

Money laundering affects the financial services industry most. Defined in our survey as 'actions intended to legitimise the proceeds of crime by disguising their true origin', the crime of money laundering exposes financial institutions in two ways – through the access to laundered money provided to potential criminals and through the banking functions (bank accounts, loans, etc.) which fraudsters use to disguise the funds.

Over one quarter (27%) of global and South African respondents in the financial services industry reported having experienced money laundering in the last 24 months.

All respondents considered damage to corporate reputation as the most serious consequence of money laundering. South African respondents were significantly more concerned about financial loss than their global counterparts.

**Figure 5: Greatest concerns regarding money laundering**




***Q: With respect to money laundering, what do you perceive to be the most severe impact on your organisation?***

### *Competition law infringement*

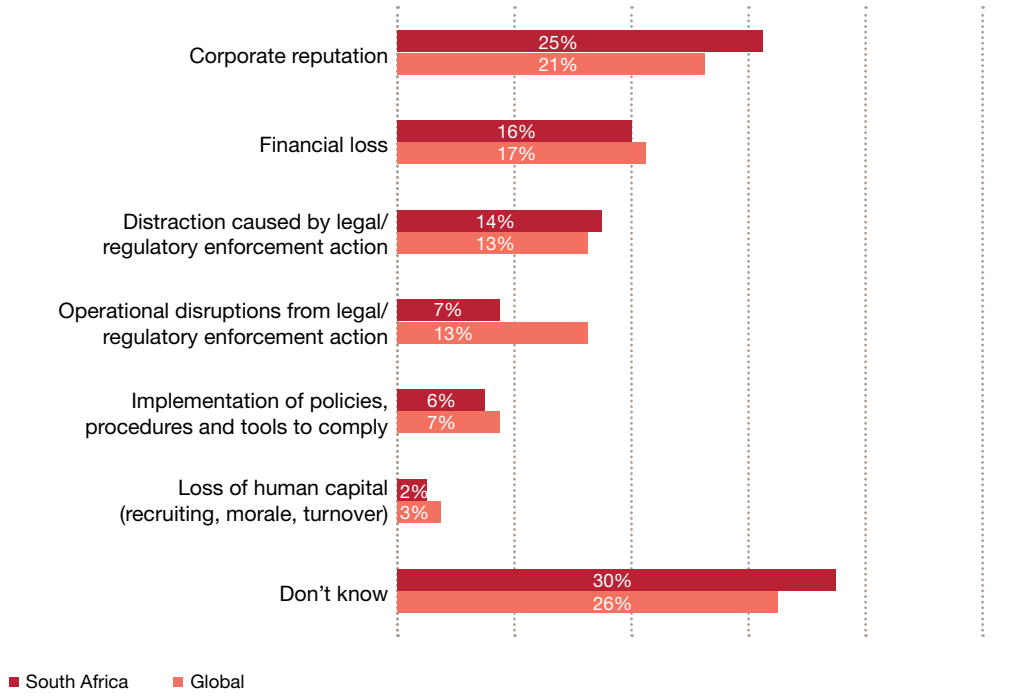
Figure 3 shows that 8% of South African respondents reported having experienced a competition law infringement during the survey period, compared to 5% globally.

Figure 4 in turn depicts that 16% of South African respondents were most concerned about competition law infringement when asked to choose between the three enforcement-related crimes.

In terms of what consequences concern organisations most with regard to competition law infringement, Figure 6 shows that corporate reputation and financial loss are the two most serious potential consequences of infringements.

Financial losses related to competition law infringements are not limited to statutory fines. Such acts also open the door for significant civil claims from parties that are disadvantaged by the prohibited market practices and these can run into millions of rand. Three percent of South African respondents indicated that they had lost between USD1-100 million as a result of competition infractions in the 24 months preceding our survey.

**Figure 6: Greatest concerns with regard to competition law infringement**




***Q: With respect to competition law infringement, what do you perceive to be the most severe impact on your organisation?***

Competition law infringement is a complex economic crime that is poorly understood by respondents. When we asked South African respondents to quantify how much they had lost as a result of competition law infringements, 40% responded with 'I don't know'. Figure 6 also shows that 30% of local respondents did not know which consequences they were most concerned about.

Education and awareness regarding the competition law framework in South Africa should therefore be a priority for companies in South Africa.

## Other high-impact frauds

The survey results also highlight the contribution of procurement fraud and human resources fraud to losses in South Africa. This is a clear indication that more attention needs to be paid to these two processes by organisations.

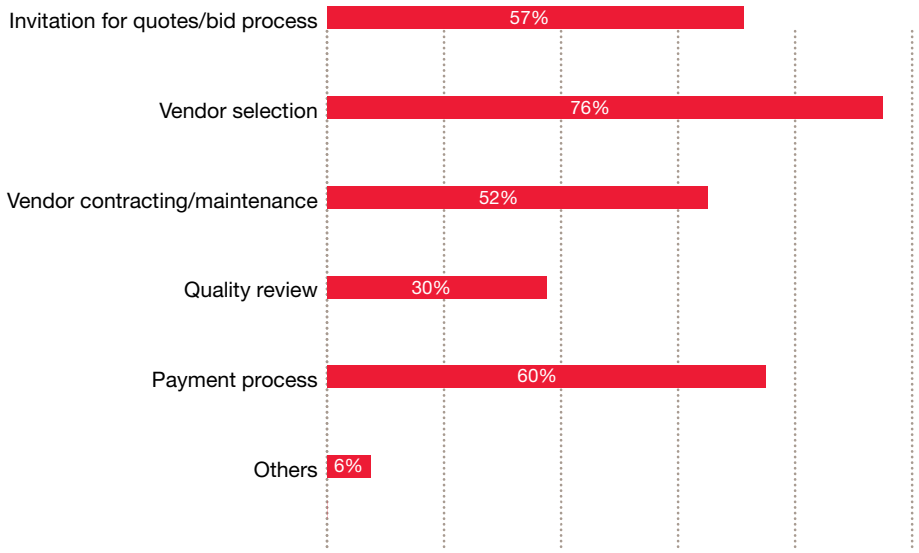
### *Procurement fraud*

Procurement fraud affected 59% of South African respondents during the past 24 months, compared to only 29% of global respondents.

In South Africa, vendor selection was the step in the procurement process that was targeted most by fraudsters, although all steps appear to be vulnerable to fraud.

South African organisations should pay attention to safeguarding each step in the procurement process.

**Figure 7: Steps in the procurement process where fraud occurred**



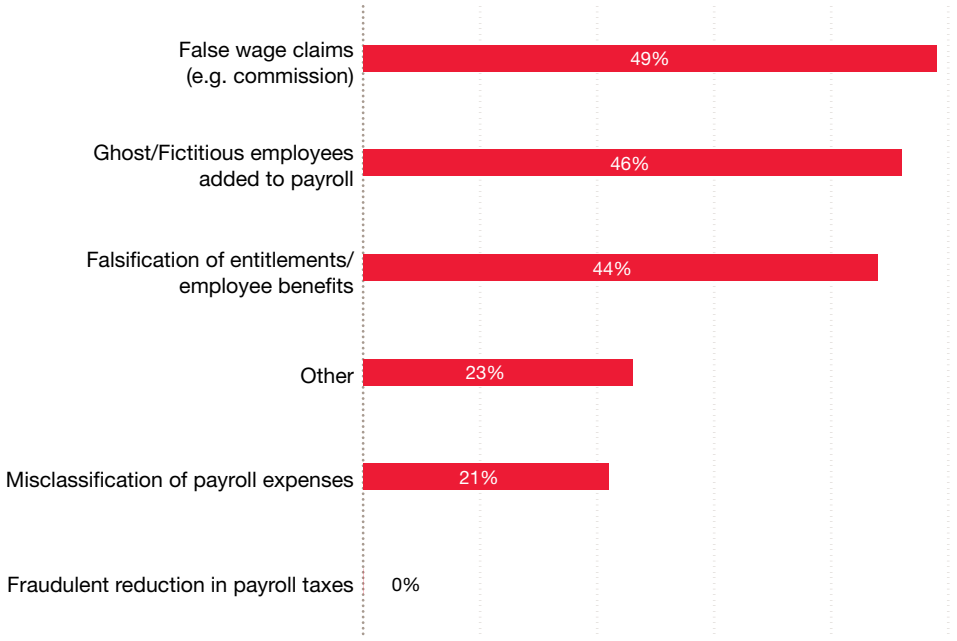

*Q: Where did the procurement fraud primarily occur?*

### *Human resources fraud*

Forty-two percent of South African respondents reported that they experienced some form of human resources fraud during the past 24 months. This is almost three times the prevalence reported by global respondents.

Figure 8 shows false wage claims and fictitious employees as the most prevalent problem.

**Figure 8: Types of human resource fraud detected**

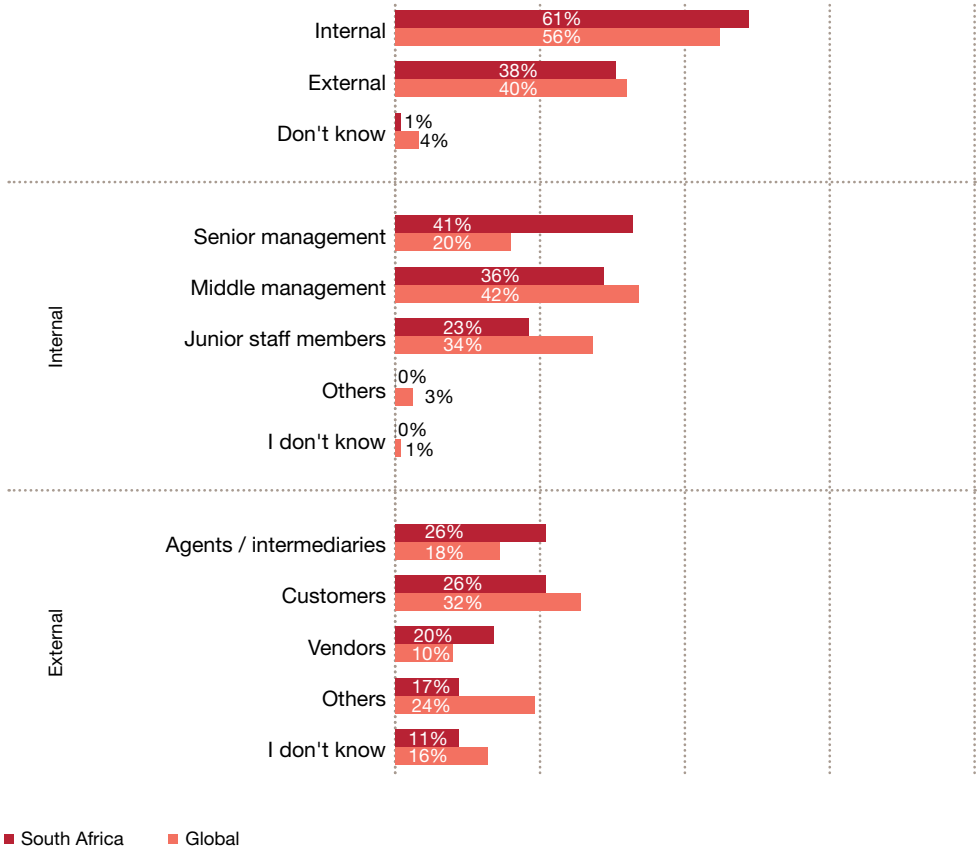



*Q: What was the type of Human Resources fraud suffered?*

*Globally, most economic crime is committed by internal parties, with senior and middle management being the main perpetrators.*

# Perpetrators of economic crime

**Figure 9: Perpetrators of economic crime**

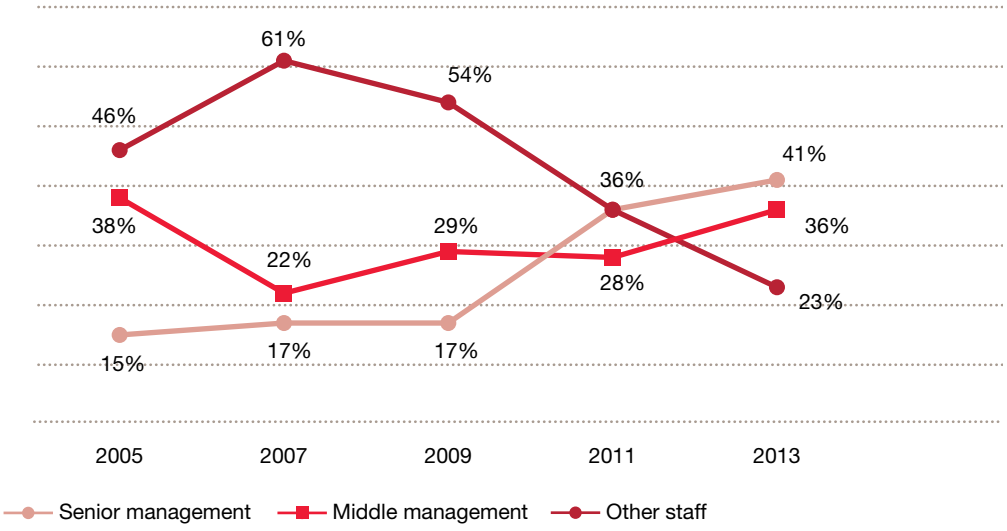



***Q: Thinking about the most serious economic crime your organisation experienced in the last 24 months, who was the main perpetrator ?***

Most economic crime is committed by internal parties, both in South Africa and globally. Internally, we have seen an alarming shift in the perpetrator profile in South Africa since our 2009 survey and our latest results confirm that this trend is continuing, with 41% of all internal fraud being committed by senior management.

Figure 9 shows that employees in senior and middle management have become the main perpetrators of internal fraud.

**Figure 10: The changing face of internal fraud South Africa**




***Q: Thinking about the most serious economic crime your organisation experienced in the last 24 months, at what level was the main perpetrator of internal fraud within your organisation?***

When looking at external perpetrators of economic crimes against companies, South African organisations are targeted more by external vendors and less by their customers than their global counterparts. Since our last survey, agents and intermediaries have become significantly more involved in committing fraud against their principals.

## The profile of a perpetrator

Our survey results indicate that the typical internal fraudster is male, aged between 31 and 40, has worked for his employer for more than 10 years and has acquired a first university degree. This profile is consistent with South African organisations reporting that senior and middle management commit 77% of all internal fraud.

***Perpetrator profile***

*With no 'silver bullet' in the fraud detection arsenal, multiple channels are required to detect fraud effectively.*

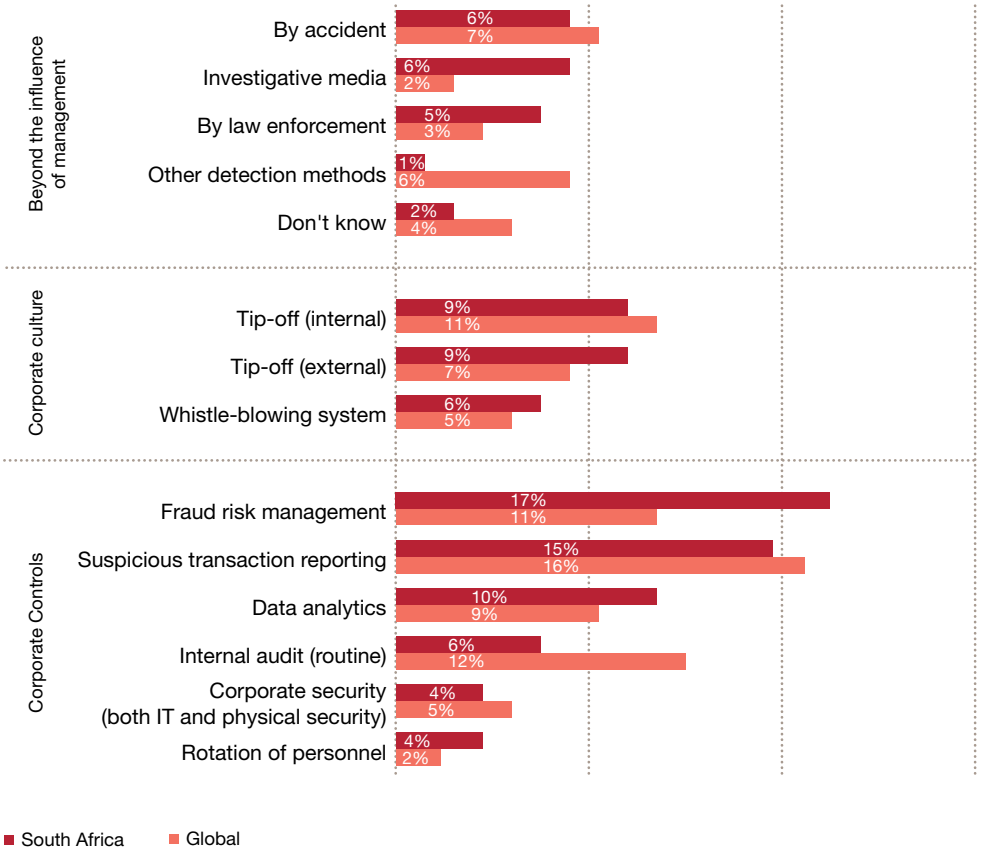
# Detecting fraud

Detecting fraud is a key step in managing fraud risk. Figure 11 depicts the effectiveness of different detection methods, which fall into three categories: corporate controls, corporate culture and events beyond the control of management.

Our survey results suggest that while some methods are more effective than others, there is no 'silver bullet' and that multiple channels are needed to detect fraud effectively. While a number of key detection methods (like formal whistle-blowing mechanisms) have shown decreased effectiveness over the last few years, one encouraging aspect is that the number of frauds detected 'by accident' has decreased significantly since our last survey.

It is encouraging to note that methods that are within management's control accounted for 80% of detections. This justifies management investment in anti-fraud controls and in developing a risk-based fraud risk management framework that combines preventative and detective controls.

**Figure 11: Most common means of detection**



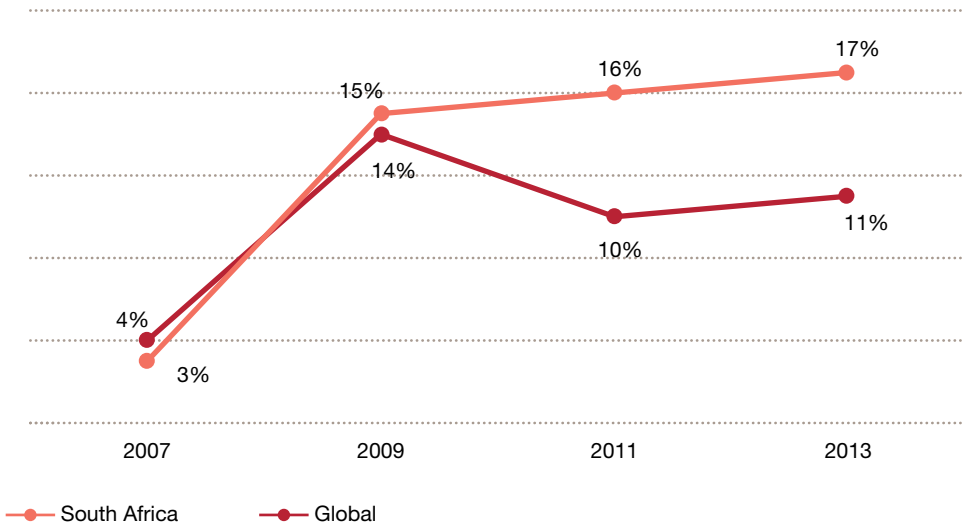

***Q: Thinking about the most serious economic crime your organisation experienced in the last 24 months, how was the crime initially detected?***

We introduced data analytics as a separate category in this edition of the survey and noted that it contributed significantly to detections with South African respondents reporting 10% (global: 9%) of fraud detections came about in this way.

## Fraud risk management coming into its own

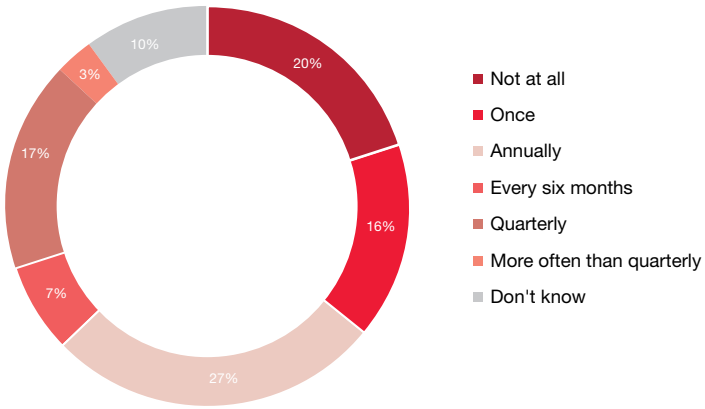
Figure 12 shows how formal fraud risk management (including formal fraud risk assessments) has established a sustainable trend in effectively detecting fraud globally, and to an even greater extent, in South Africa. Accounting for 17% of fraud detections in this survey (2011: 16%), it has been the most effective detection method in our last two surveys.

**Figure 12: Fraud risk management growing in effectiveness**




***Q: Thinking about the most serious economic crime your organisation experienced in the last 24 months, how was the crime initially detected?***

**Figure 13: Frequency of fraud risk assessments in South Africa**




***Q: In the last 24 months, how often has your organisation performed a fraud risk assessment?***

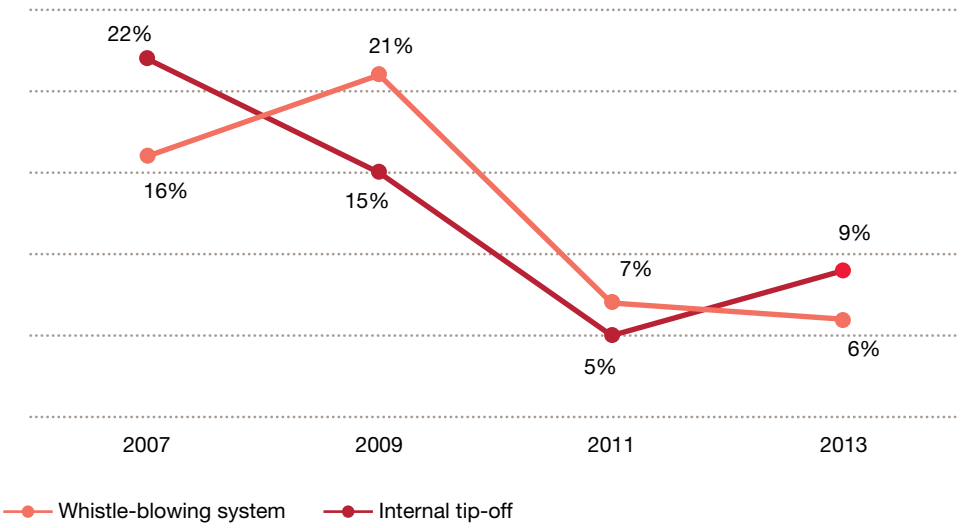
Despite being the most effective detection method, not all organisations seem to realise the value of a formal fraud risk management mechanism. Figure 14 shows that one fifth of organisations in South Africa have never carried out a formal fraud risk assessment. However, it is encouraging to note that 51% of companies in South Africa carry out formal risk assessments at least annually and are reaping the benefits of a pro-active approach to fraud risk. It appears that awareness and education play some role in the disconnect between these two extremes as the most common reason given by South African respondents for not performing fraud risk assessments is that they do not know what they entail.

## Whistle-blowing may be under threat in South Africa

Figure 14 shows a consistent decline in the effectiveness of formal whistle-blowing systems and internal tip-offs in detecting fraud over the course of the last four surveys.

This trend is worrying and may be related to senior management committing more fraud. Employees are less willing to blow the whistle if the fraudster is more senior than the whistle-blower.

**Figure 14: Declining effectiveness of whistleblowing and internal tip-offs**




***Q: Thinking about the most serious economic crime your organisation experienced in the last 24 months, how was the crime initially detected?***

Nevertheless, 82% of South African respondents (global: 62%) indicated that their organisations had implemented a formal whistle-blowing system.

So, the decline in effectiveness is not attributable to a lack of access to this mechanism in South Africa.

Only 6% of South African respondents (global: 26%) indicated that their organisation's whistle-blowing mechanism had not been utilised in the 24 months preceding the survey.

South African employees are aware of whistle-blowing lines and are generally willing to use them. Fifty percent of respondents rated their organisation's reporting mechanism as being either 'effective' or 'very effective', which raises concerns about why the other half rated it to be ineffective.

If the problem relates to processes followed after a fraud is reported, this will undermine employees' confidence in the mechanism. Figure 15 in the next section shows that the most common response once a fraud has been detected is to utilise internal resources to perform an internal investigation.

Organisations should therefore ensure that the internal resources are properly trained to appropriately carry out such investigations and not jeopardise the right to anonymity of the whistle-blower.

Given the high level of availability of whistle-blowing mechanisms, South African organisations would benefit from investing in improving the design of their mechanism, as existing whistle-blower lines will be costing organisations money each month, but not providing the envisaged benefits.

*South African organisations would benefit from investing in improving the design of their whistle-blowing mechanism.*

*Once fraud has been detected, it is critical that appropriate action is taken.*

# Responses to fraud events

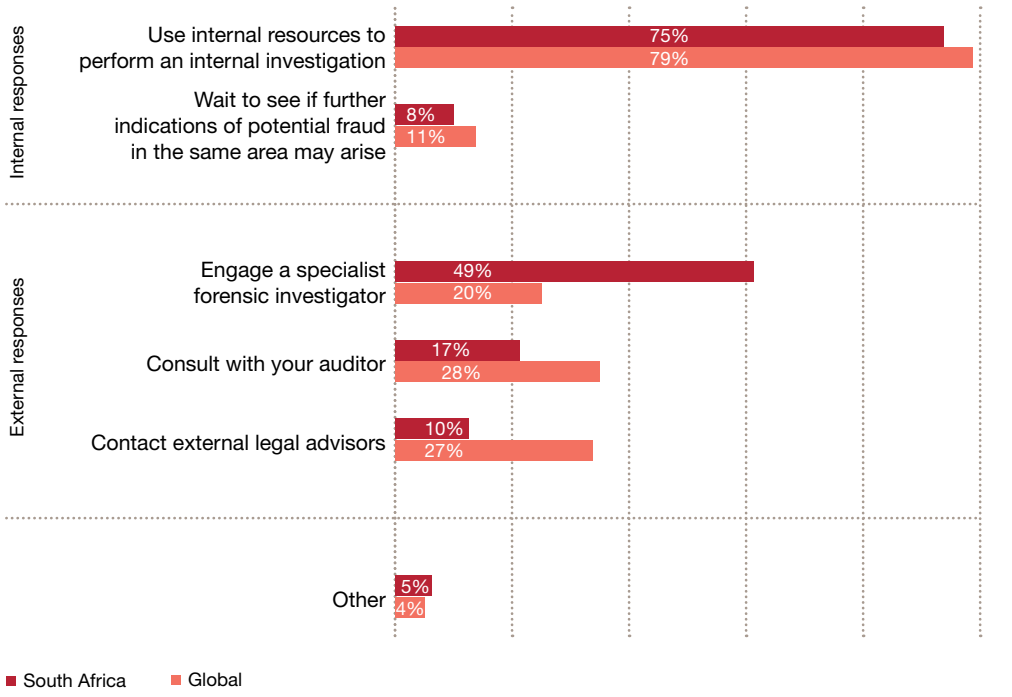
Once fraud has been detected, it is critical that an organisation takes, and is seen to take, appropriate action. Less than one in ten South African respondents (8%) and 11% of those globally confirmed their organisation would 'wait and see if further indications of potential fraud in the same area may arise'. This is worrying as decisive action such as investigating in cases where the event and/or perpetrator are known should be taken immediately.

Figure 15 indicates that most organisations opt for a combination of internal and external responses, with three-quarters of South African respondents deploying internal resources to investigate incidents.

South African organisations are more than twice as likely as their global counterparts to engage a specialist forensic investigator when involving outsiders.

Global respondents are more likely to involve their attorneys or auditors than their South African counterparts.

**Figure 15: Responses to fraud events**

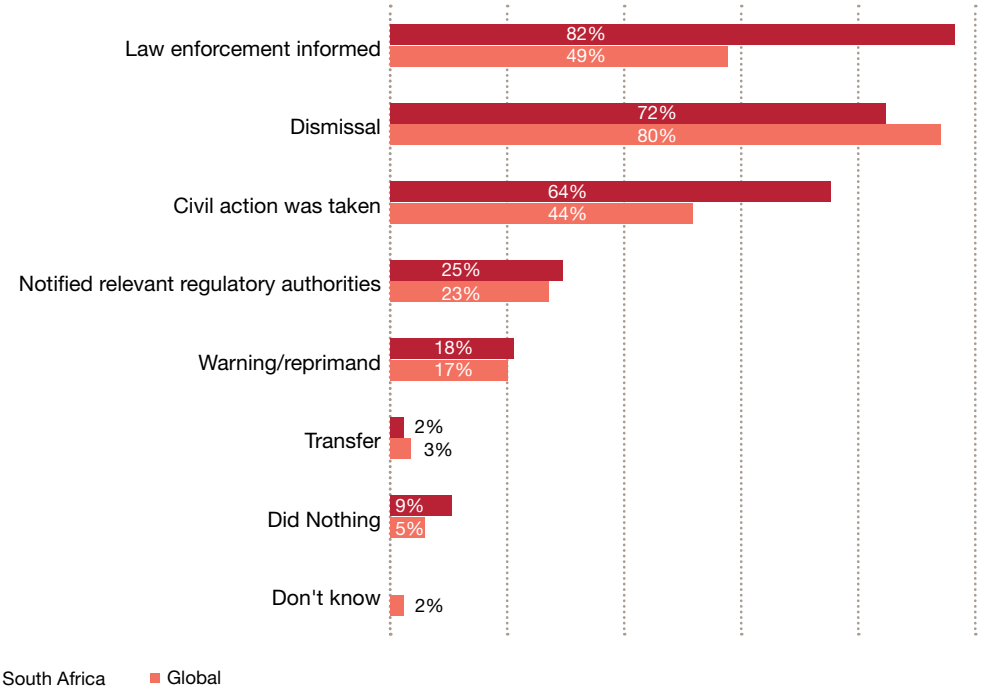



***Q: When you identify an incident of potential fraud, which action(s) are you likely to take?***

Since our last survey there has been a significant increase in the percentage of cases in which South African organisations have informed law enforcement or initiated civil litigation processes.

Overall, South African organisations resorted to more stringent measures when dealing with internal perpetrators (civil or criminal actions, notifying regulatory authorities) than their global counterparts, but opted for dismissal in fewer instances than those globally.

**Figure 16: Action taken against internal perpetrators**




***Q: Thinking about the most serious economic crime your organisation experienced in the last 12 months, what actions, if any, did your organisation take against the main internal perpetrator?***

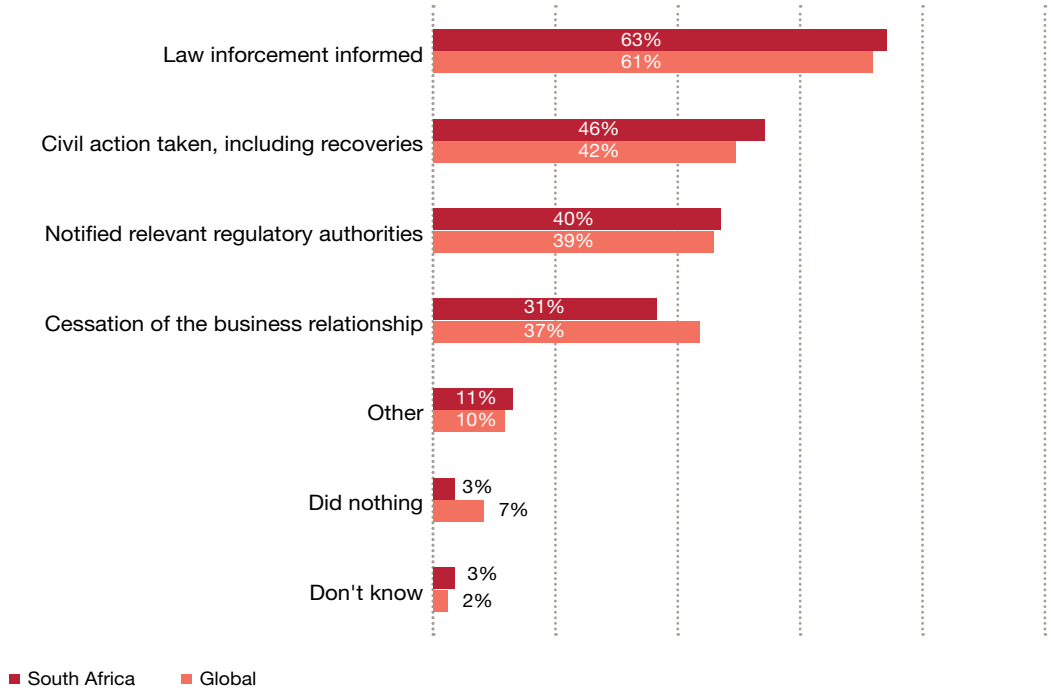
Interestingly, when it came to the most serious economic crime committed by insiders, South African entities took no action in 9% of cases, opted for transfers in 2% or warnings in 18% of cases.

This is worrying as it suggests that the perpetrators remain within the organisations, where they may commit further transgressions. It is important for organisations to adopt a zero-tolerance approach by dealing with fraudsters in an official and transparent manner, rather than sweeping the problem under the carpet internally.

The actions taken by South African organisations against external perpetrators mirror those of respondents globally. It is noteworthy that South African respondents are not as likely as their global counterparts to stop doing business with organisations whose employees were responsible for fraudulent events.

***Q: Thinking about the most serious economic crime your organisation experienced in the last 12 months, what actions, if any, did your organisation take against the main external perpetrator?***

**Figure 17: Action taken against external perpetrators**



# Contacts

## Gauteng

*Johannesburg*

**Louis Strydom**
+27 11 797 5465
louis.strydom@za.pwc.com

**Colm Tonge**
+ 27 11 797 4007
colm.tonge@za.pwc.com

*Pretoria*

**Lionel Van Tonder**
+27 12 429 0400
lionel.vantonder@za.pwc.com

**Trevor Hills**
+ 27 11 797 5526
trevor.hills@za.pwc.com

## Western Cape

*Cape Town*

**Malcolm Campbell**
+27 21 529 2676
malcolm.campbell@za.pwc.com

## Eastern Cape

*Port Elizabeth*

**Jacques Eybers**
+ 27 43 707 9802
jacques.eybers@za.pwc.com

## KwaZulu-Natal

*Durban*

**Trevor White**
+27 31 271 2020
trevor.white@za.pwc.com

## Free State, North-West & Northern Cape

*Mafikeng*

**Gerhard Geldenhuys**
+27 18 386 4720
gerhard.geldenhuys@za.pwc.com

## Namibia

*Windhoek*

**Gerrit Jordaan**
+ 264 81 22 4246
gerrit.jordaan@na.pwc.com

*www.pwc.com/crimesurvey*

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2014 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.

Designed by PwC Design Studio (JB 14-14493)

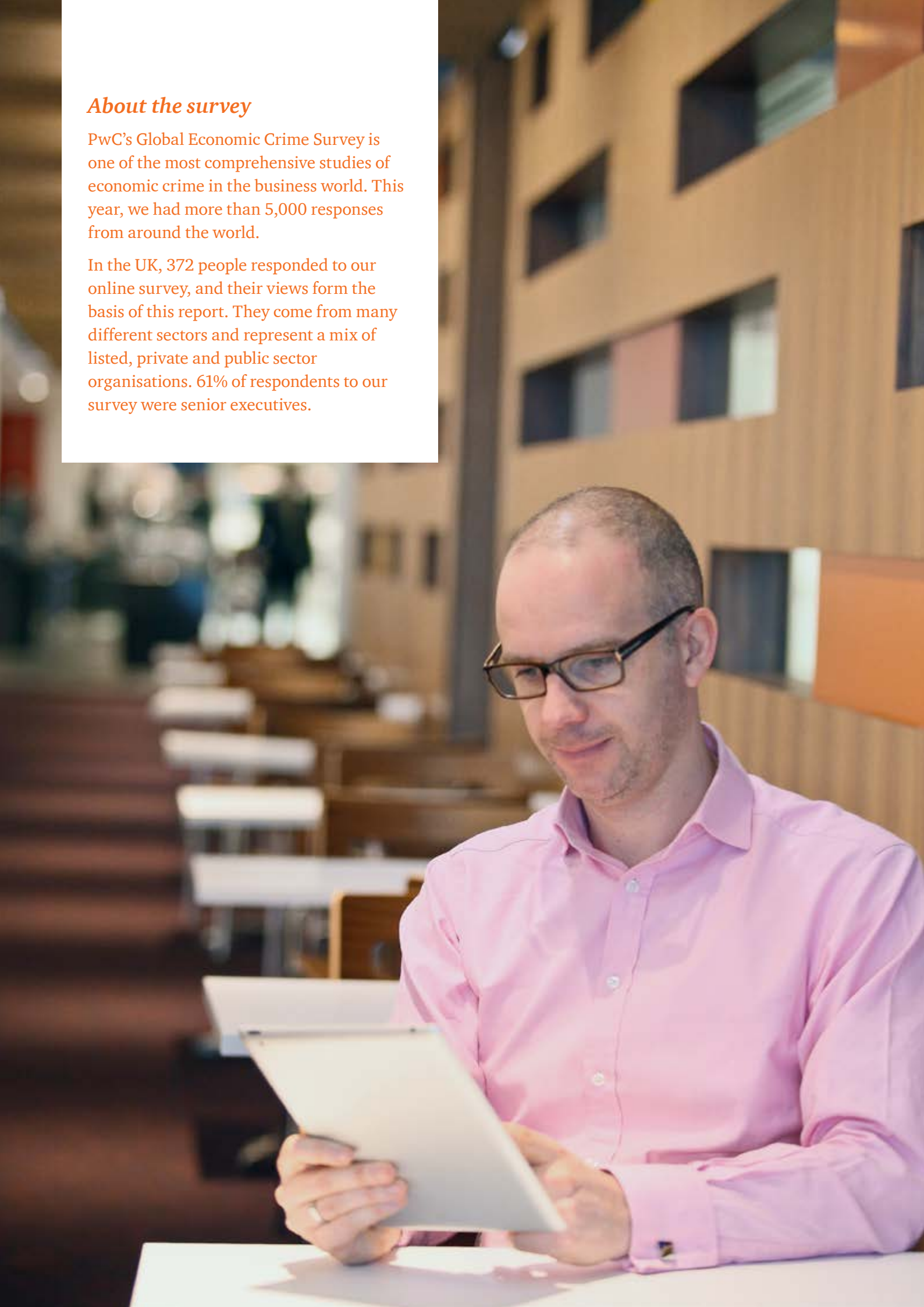
# *The changing face of fraud*
# How economic crime can impact your business

**44%**
was the rate of fraud reported in the UK in the 2014 survey, less than two years ago.

**41%**
of economic crimes are committed by employees within an organisation.

**54%**
of respondents felt the number of instances of economic crime had increased in the last two years.

pwc



## *About the survey*

PwC's Global Economic Crime Survey is one of the most comprehensive studies of economic crime in the business world. This year, we had more than 5,000 responses from around the world.

In the UK, 372 people responded to our online survey, and their views form the basis of this report. They come from many different sectors and represent a mix of listed, private and public sector organisations. 61% of respondents to our survey were senior executives.

# Contents

# *Key highlights from the UK*


The **more senior** the respondent, the less fraud they reported in their organisation.

51% 2011
44% 2014

51% of organisations experienced economic crime in 2011. In 2014, it's dropped to 44%.

UK 44%
Global 37%

44% of organisations in the UK reported some type of fraud, above the global average of 37%.

The majority of respondents felt that the number of instances and financial impact of economic crime had increased in the last two years.

## *Types of fraud*

**35%** of organisations who experienced fraud, experienced **accounting fraud** in 2011. In 2014, this has fallen to **14%**

**22%** said that they suffered a **procurement fraud**, a new category in 2014.

## *Perpetrator*

**41%** 2014
**34%** 2011

There's been a big rise in the proportion of economic crime committed by employees.

**45%** Junior staff

Most frauds committed by staff are now committed by junior staff.

## *Bribery:* A threat to expansion?

**12%** UK
**27%** Global

UK organisations report **less than half** the amount of bribery as the global average.

**9%** UK
**41%**

**9%** of UK organisations have reported that they've been asked to pay a bribe in the last year despite **41%** having operations in high risk territories.

**87%**

87% of organisations in the UK have made changes to their policies and procedures because of the UK Bribery Act.

## *Cybercrime:* A growing risk?

Nearly **two-thirds** of respondents felt their awareness of cybercrime was greater than it was two years ago despite the UK reporting a fall in the percentage of organisations reporting cybercrime.

**93%**

A lot of cybercrime may be going unreported and/or undetected. A recent PwC/BIS survey showed that **93%** of large organisations had experienced a cyber breach in the last year.

## *Detecting fraud:* What works best?

The most effective methods of detecting fraud are **suspicious transaction monitoring** and **fraud risk management**.

**83%** of organisations in the UK have whistleblowing mechanisms but nearly **40%** hadn't been used in the last two years.

# Introduction

Economic crime is pervasive and affects our lives in more ways than we may care to think about. It might be through steeper insurance premiums, higher taxes or a series of transactions on our bank statement that we know nothing about.

Economic crime also shapes the way we do business and it creates risks for UK businesses operating overseas. So how can organisations protect themselves against it? Here we look at the results of our seventh Global Economic Crime Survey and assess how fraud in the UK has changed over the last few years.

Whilst we've seen a fall in the number of UK organisations reporting economic crime in the last two years, the overall picture is far more complicated. We've seen a rise in the number of frauds committed by staff since 2011 and it's harder than ever to predict where the threat may come from. As rises in the cost of living have hit, the number of junior staff engaged in frauds has also risen.

We've also found that senior executives tend to report less economic crime than middle management. While fraud and bribery risks are higher than ever on the board's agenda, this suggests that people at the top of an organisation may not be aware of everything that's going on below them.

With little or no growth in the UK over the last couple of years, companies are increasingly turning to overseas markets. But high-risk territories have been labelled high-risk for a reason: businesses face bigger risks when they operate there. Bribery may be part of the business culture, and UK organisations need to ensure that they are fully compliant with the UK Bribery Act or face substantial penalties and reputational damage. And as UK businesses expand overseas, it becomes even more crucial to embed ethical behaviour throughout your organisation.

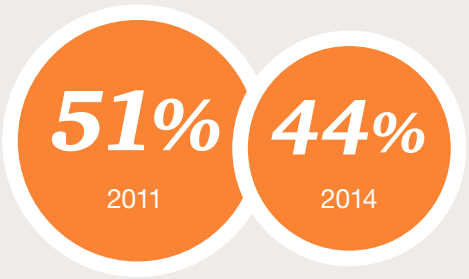
Our survey revealed that most frauds are detected by suspicious transaction monitoring and data analytics – "clever" ways of using the data that you have to identify anomalies. In contrast, we found that whistleblowing mechanisms are rarely used by organisations in the UK, despite most companies having some sort of procedure or hotline.

Having a fraud risk management programme has also proved to be an effective way of identifying economic crime. Regular fraud risk assessments, as well as setting a tone from the top that creates a culture of doing the right thing, can also help to mitigate the risk to your organisation.

*The rate of fraud in the UK is still higher than the global average and the rate across the rest of Western Europe*

# ***Comparisons***
# What's changed?

**Figure 1**
The percentage of organisations experiencing economic crime has fallen from 2011




## UK economic crime is falling – but is still higher than the global average

The number of organisations that reported experiencing some sort of economic crime in the past two years fell from 51% in 2011 to 44% in 2014[1]. Despite this, the rate of fraud in the UK is still higher than the global average (37%) and the rate across the rest of Western Europe (35%).

Why do we report more economic crime in the UK than in the rest of the world? One factor might be the increasing use of, and investment in, 'intelligent' ways of detecting it, including suspicious-transaction monitoring and data analytics. As we'll see, the UK may simply be better at detecting fraud than other countries.

1. The 2014 survey period was the 24 months prior to the respondent completing the survey. The 2011 survey period was the 12 months prior to the respondent completing the survey.

### *What is 'economic crime'?*

We define economic crime as 'the intentional use of deceit to deprive another of money, property or a legal right'. An economic crime often results in a financial loss, but not always. In this report, we have used the terms 'fraud' and 'economic crime' interchangeably for ease of understanding.

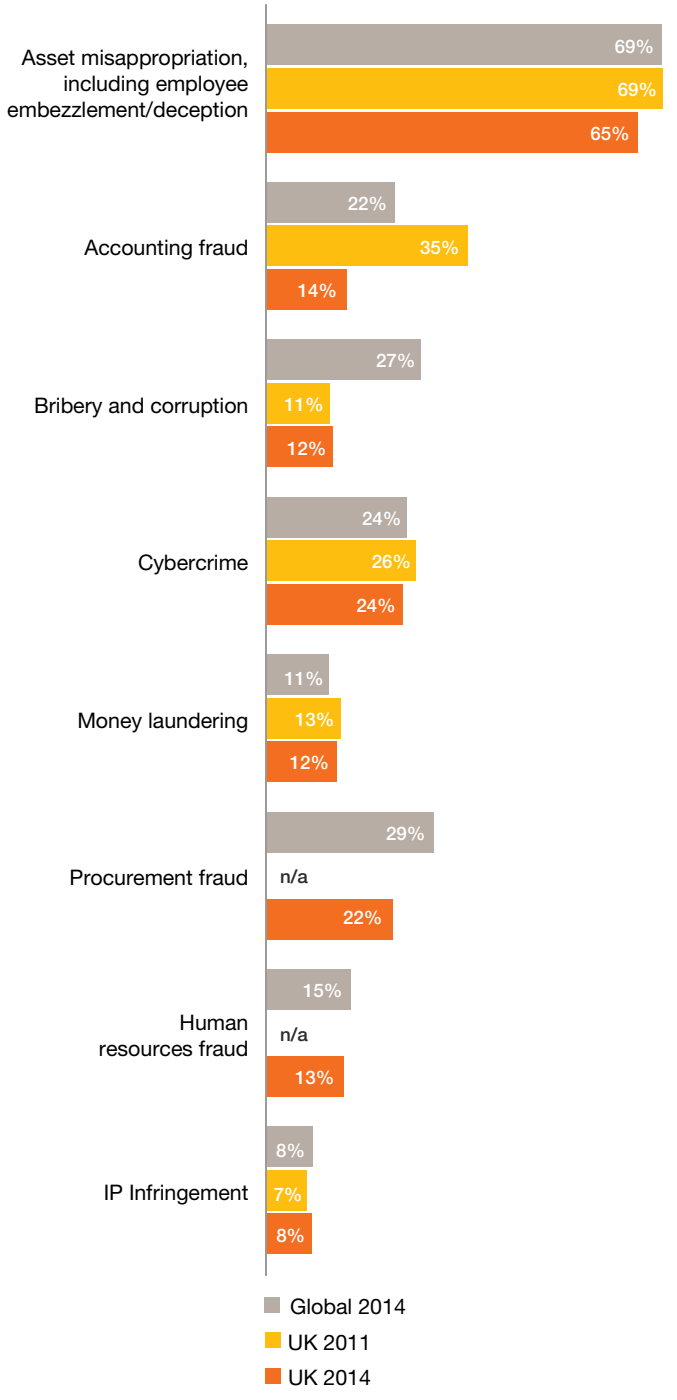
## The type of fraud is changing

There are many different types of economic crime, each with its own characteristics and risk factors. Since 2011, we've seen a significant fall in accounting fraud – the deliberate misstatement of financial information in financial statements or other documents intended to inform users about the performance or financial condition of an organisation.

This year, we've introduced two new categories into our survey: procurement fraud and HR fraud, which includes payroll fraud, recruitment fraud or the creation of ghost employees. These two new types of economic crime may explain some of the fall in accounting fraud as respondents may have re-classified a crime that they previously would have considered an accounting fraud. But we've also seen the level of accounting fraud in the UK fall well below the global average. Over the past five years, we've seen a general trend of a falling number of accounting frauds in the UK as fraudsters turn to high-tech methods of committing economic crime. At the same time, companies have improved their internal controls, making it harder for fraudsters to find an opportunity to commit fraud.

The level of bribery and corruption in the UK is still low compared to the global average. Bribery has been an area of increasing focus for regulators over the last few years, and with the introduction of the UK Bribery Act in 2011, the UK now has some of the world's most far-reaching anti-corruption legislation. Later in this report, we explore the risks that UK-based organisations face in doing business overseas, and the impact of the Bribery Act.

**Figure 2**
Those who reported experiencing economic crime suffered less accounting fraud than 2011 and lower levels of bribery and corruption than the global average



## *What is 'procurement fraud'?*

Our survey defines procurement fraud as 'illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to their organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation'. We consider procurement fraud at all stages of the process, from the bid process to contract maintenance and payment.

### Procurement fraud

This is the first year that we've asked survey respondents about their experiences of procurement fraud. Procurement fraud can be very hard to spot as it often involves collusion between staff and external contractors. Identifying procurement fraud depends on the quality of management information and the tools businesses use to monitor and assess performance.

Our respondents reported a significant amount of procurement fraud, and one reason for this could be the move towards outsourcing services and/or functions. These kinds of contractual relationships can generate savings, but they're also inherently risky.

Most procurement frauds in the UK – nearly two-thirds – happened during the payment process. A significant number also occurred during the contract maintenance process. Compared to the global results, fewer UK procurement frauds happened at the invitation to bid/tender phase of the process, which may be due in part to the strict European regulations governing the tendering process for public-sector contracts.

### The view from the top

The more senior the respondent to our survey, the less fraud they reported. Only 32% of board members reported that their organisation had suffered a fraud in the last two years; below the executive level this climbed to 63%. Whilst fraud might figure increasingly on the board's agenda, there's a clear disconnect between what is being seen at board level and what is happening in the business.

## Perceptions of fraud

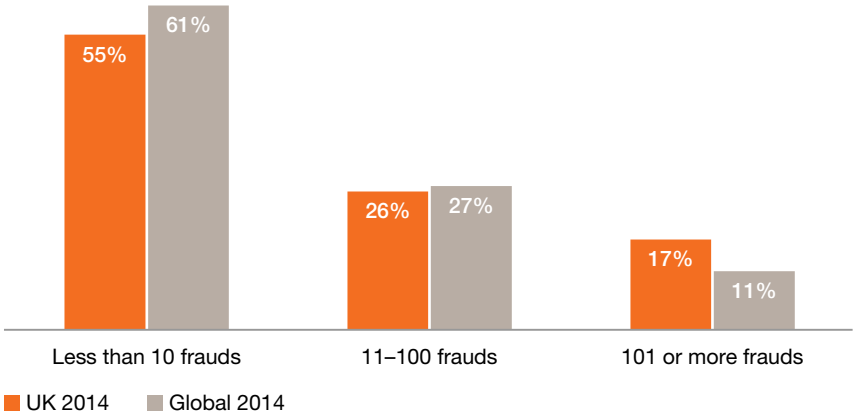
Despite the falling rate of fraud in the UK and the disconnect between the level of economic crime reported by senior executives and those below board level, it seems businesses are more aware of the risks than ever. Fifty-four per cent of respondents felt the number of instances of economic crime had increased in the last two years, compared with 45% globally. A number of high-profile fraud cases in the media in 2013 may well have helped keep fraud in respondents' minds. UK-based organisations are also more likely to suffer multiple instances of fraud than those in other countries. Of the businesses we spoke to, 18% had experienced more than 100 frauds in the past two years, compared to just 11% globally. As a result, it may feel like UK businesses are under attack more than ever before.

Of those who had experienced fraud in the UK, 52% felt the financial impact had increased in the last two years, compared to 42% globally, although it is interesting to note that the UK had far fewer high-value frauds than the global average.

**Figure 3**
More people in the UK think that the rate of fraud has increased in the last two years

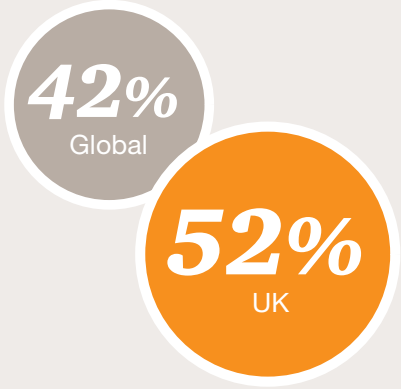

% respondents who reported either a slight increase or a significant increase

**Figure 4**
More UK organisations reported experiencing 100 or more frauds in the last two years than the global average



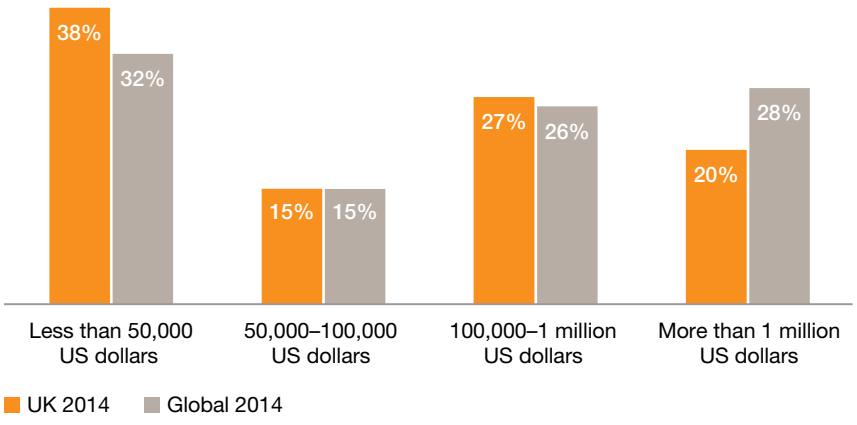

Together, these findings show that UK organisations are more likely to suffer from multiple instances of low-level economic crime than be hit by one multi-million-pound fraud. Whether a business suffers one or a hundred frauds in a year, it makes a significant impact on finances and in other ways: 18% of those who'd experienced fraud in the past two years said it had had a very significant impact on employee morale. There is also the cost of investigation/remediation to consider, as well as the damaging impact to an organisation's reputation which may have long-lasting consequences.

**Figure 5**
Fraud's financial impact is growing




% respondents who reported either a slight increase or a significant increase

**Figure 6**
UK organisations reported less £1m+ frauds over the last two years than the global average



*We've seen a significant rise in the number of frauds committed by employees – from 34% in 2011 to 41% in 2014.*

# ***Fraudsters***
# Who are they?

*When employees just get a warning or are simply transferred to another department, as happens more frequently outside the UK, it sends a message that the business tolerates fraud.*

## The rising threat of employee fraud

As we found in 2011, most UK fraudsters come from outside an organisation. But we've seen a significant rise in the number of frauds committed by employees – from 34% of the total in 2011 to 41% in 2014. In 2009, the UK reported more internal fraud than external fraud, so it appears that the dip in the proportion of frauds committed by employees in 2011 was something of a one-off.

In 2011, we questioned whether a reduction in corporate resources, like internal audit, during the recession had led to internal frauds going undetected. Our 2014 survey found that there is more employee fraud being reported, perhaps because businesses are making more use of automated systems like suspicious-transaction monitoring and data analytics that make fraud easier to detect.

Although the level of employee fraud has gone up in the UK over the last couple of years, it is still lower than the global average of 56%. One of the reasons for this might be the firm stance that UK companies take against fraudsters: fraud leads to dismissal in 88% of cases in the UK compared to 79% across the globe; firms called in the police in 63% of cases, compared to just 49% of frauds globally. When employees just get a warning or are simply transferred to another department, as happens more frequently outside the UK, it sends a message that the business tolerates fraud.

**Figure 7**
Rate of internal fraud rises but remains below the global average

## Is there such a thing as a 'typical fraudster'?

For years, the profile of a typical fraudster hasn't changed. The most likely fraudster in any organisation has usually been male and relatively senior, and will have been employed there for years, if not decades.

Whilst this remains true at a global level, our survey shows this model is changing in the UK:

- Most economic crimes are committed by junior members of staff as opposed to middle management.
- Fraudsters are most likely to have been with a company less than five years.
- The percentage of economic crime committed by women has doubled in the last two years and is higher than the global average.

Nearly 80% of the respondents to our survey felt that the main factor behind staff fraud was still the opportunity or ability for employees to commit the crime. This is important when it comes to preventing fraud, as it's the one factor that most organisations can control. If management identifies gaps in the control environment and/or policies that might allow employees to commit fraud, their organisation will be better placed to stop it happening.

**Figure 8**
UK firms are more likely to inform the police and dismiss employees for fraud

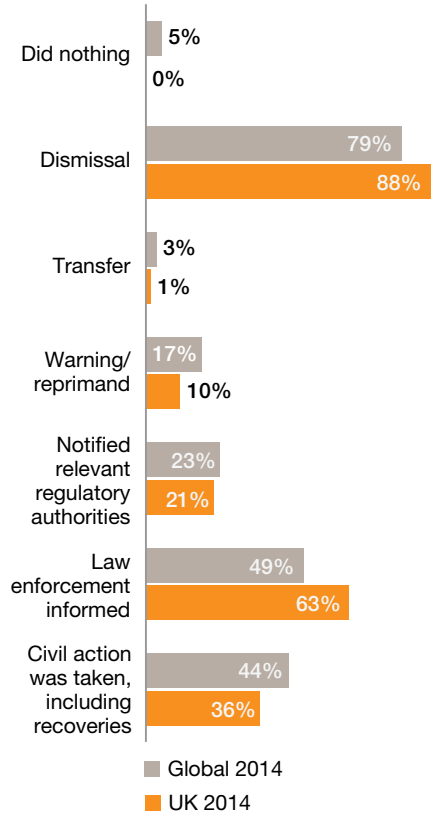
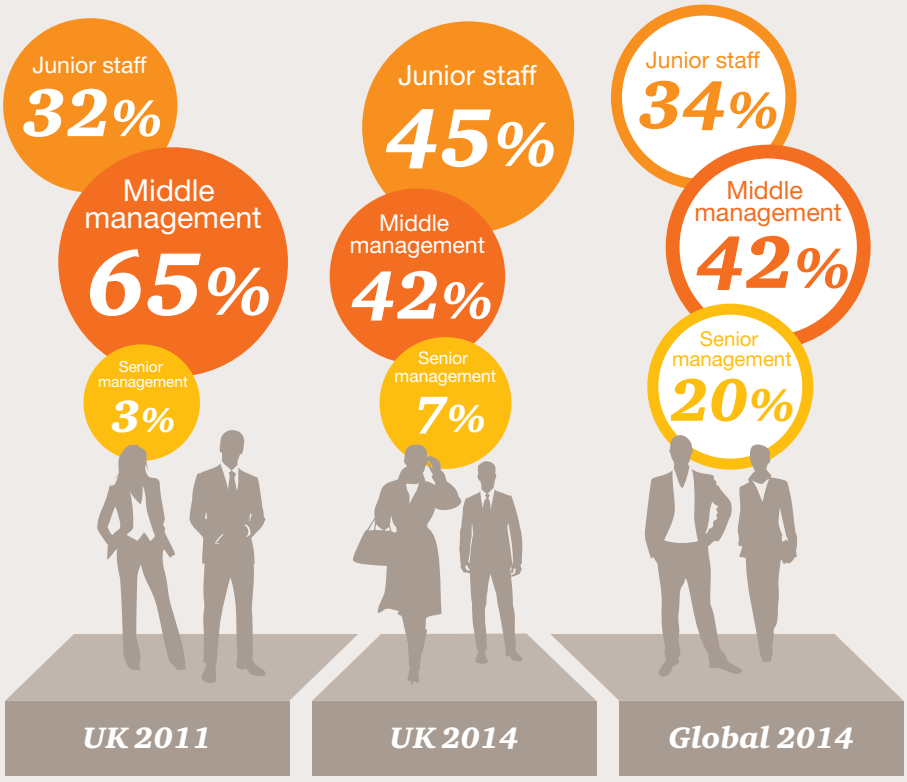
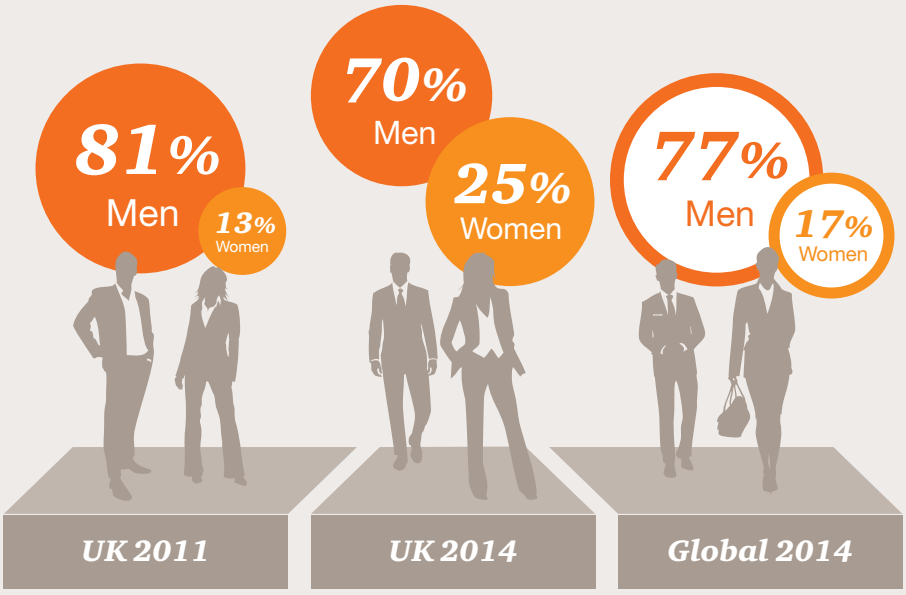


**Figure 9**
Is there such a thing as a typical 'fraudster'?

## Seniority




## Gender




Practitioners commonly refer to a "Fraud Triangle" — the three elements that are often present when a perpetrator commits fraud: opportunity, incentive and pressure. Any increases in the cost of living, whether food, electricity or housing, have a disproportionate effect on lower earners. This could create more incentive to commit fraud, or put pressure on more junior members of staff to do so. This may well be one of the reasons why we've seen an increase in the proportion of economic crimes committed by junior employees.

While the proportion of economic crime committed by senior executives remains relatively low in the UK, it has more than doubled over the last two years. And, after a dramatic increase over the past decade, the proportion of fraud committed by middle management has fallen by 35% since 2011.

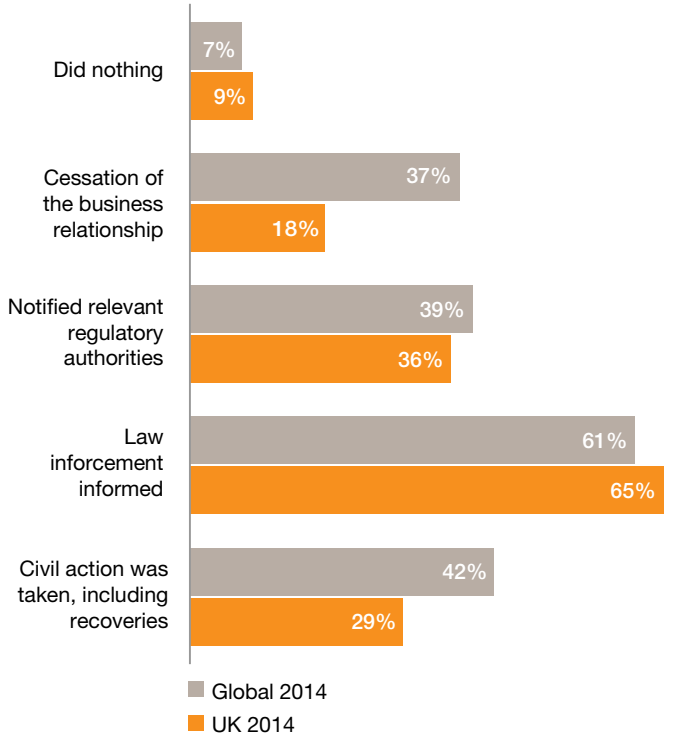
The clearest message from these changes is that it's very difficult, and potentially even dangerous, to try to identify the 'most likely' fraudster within your organisation. It could well be the person you least expect. If they have the opportunity, incentive and pressure, a fraud could be committed by anyone.

## Dealing with external fraudsters

While UK organisations take a firm stance on employee fraud, they seem to be much more reluctant to deal with external fraudsters in the same way. A fraudulent act led to the end of a business relationship in just 18% of cases, compared to a global average of 37%. Respondents in the UK were also much less likely to take civil action, including attempting to recover stolen money or goods, though 65% did contact the police.

Identifying and knowing how to deal with an external perpetrator is difficult. Organisations often have to involve a third party, like a regulator or the police. The desire to keep matters like this 'in-house' might make organisations less likely to take action, but this can mean a fraudster is free to strike again.

**Figure 10**
UK organisations are less likely to end a business relationship after a fraud



*When the UK Bribery Act came into force, nearly two-thirds of respondents said they didn't see any need to update their existing policies. Our 2014 responses show a shift in this thinking.*

# ***Bribery***
# A threat to expansion?

Short-term forecasts for the UK economy are still uncertain, so UK firms are increasingly turning to potentially more lucrative overseas markets, with higher growth rates, for expansion. But doing business on the global stage comes with its own risks.

41% of survey respondents said their organisation had pursued an opportunity in a high-risk market in the past two years

**41%**

## In the shadow of the UK Bribery Act

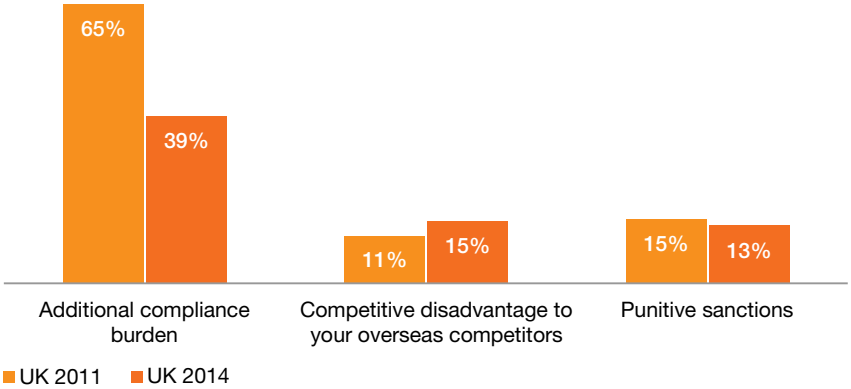
When the UK Bribery Act came into force in July 2011, nearly two-thirds of survey respondents that year said they didn't see any need to update their organisation's existing policies. But our 2014 responses show a shift in this thinking, and the Bribery Act appears to have had more impact than firms initially expected. Eighty-seven per cent of respondents said their organisation had made at least some changes to policies and procedures, with 37% saying that their organisation had performed a major overhaul of their anti-bribery policies.

Whilst the Bribery Act may have had results in changes of policy for many organisations, it appears that the compliance burden associated with the Act isn't as great as was expected. In 2011, when the Act was introduced, 65% of respondents were concerned about this – in 2014, the figure had fallen to 39%.

## A competitive disadvantage?

The Bribery Act makes organisations in the UK responsible for the actions of anyone doing business on their behalf, anywhere in the world. Fifteen per cent of respondents felt the Act put them at a competitive disadvantage compared to other countries. This is an increase of just over a third from 2011 but it still remains relatively low.

**Figure 11**
The factors which our survey respondents were concerned about in relation to the UK Bribery Act have changed since 2011



This is perhaps a reflection of that fact that only 10% of respondents in the UK felt their organisation had lost a business opportunity in the last two years to a competitor who was willing to pay a bribe, compared to a global average of 22%.

## Bribery affects the UK less than you might expect

Overall, organisations in the UK reported less than half as much bribery as their global counterparts. Only 9% of organisations said they'd been asked to pay a bribe in the last two years; half the global average.

UK businesses don't expect bribery either. Only 15% of people felt that they would face an incidence of bribery in the next two years, compared to the global average of 29%. These figures are reflected in PwC's recent *Global CEO Survey*[1], published in January 2014. Over half of global CEOs were somewhat or very concerned about the threat of bribery and corruption to their growth prospects; in the UK, just 21% of CEOs were concerned.

1. www.pwc.co.uk/ceo-survey

### *Is it a bribe?*

Our survey defines bribery as 'the unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, or the use of intimidation or blackmail. It can also refer to the acceptance of such inducements. Specific examples include kickbacks, gifts (with strings attached), facilitation payments, etc'.

Bribery doesn't always have to involve the exchange of money or goods.

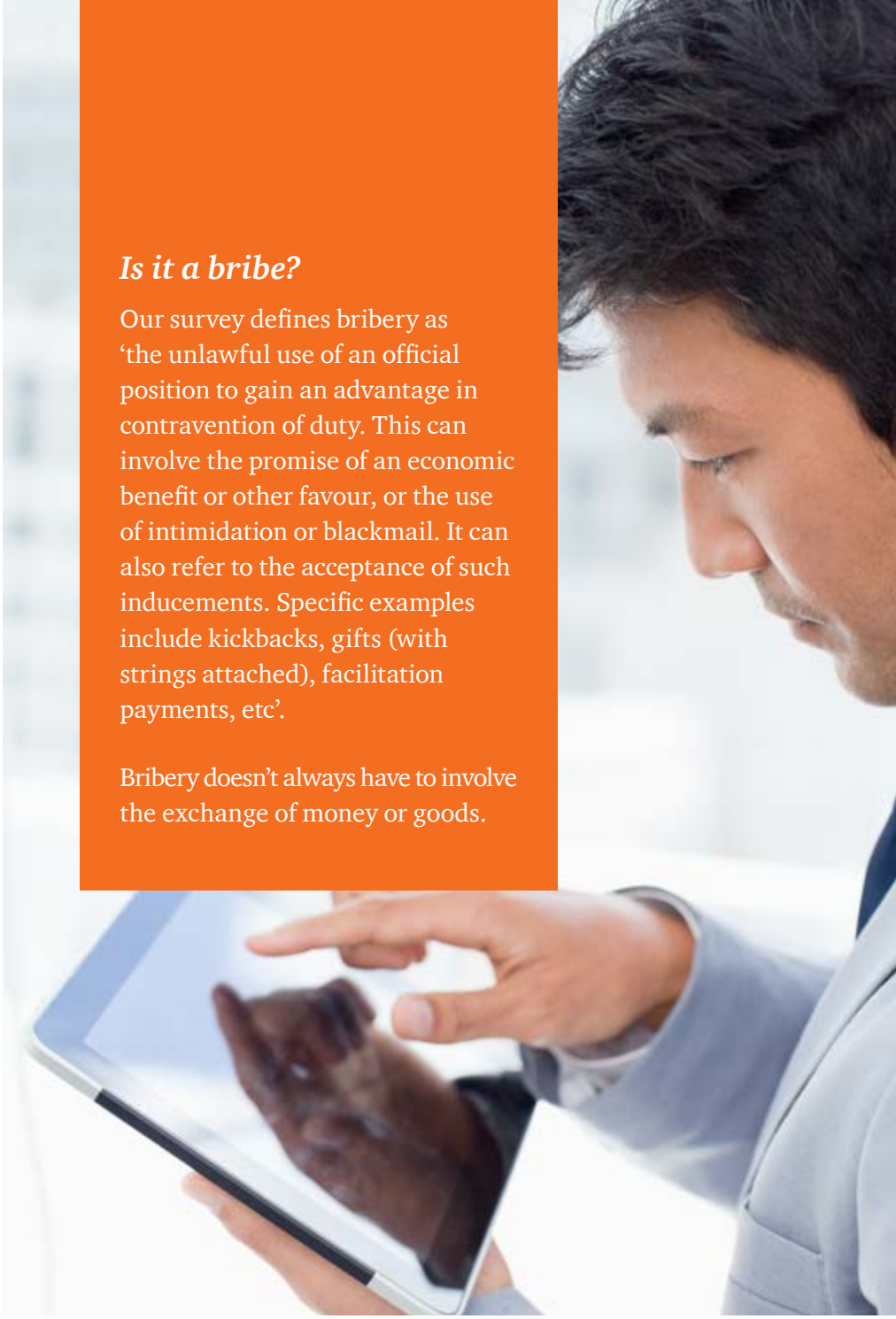


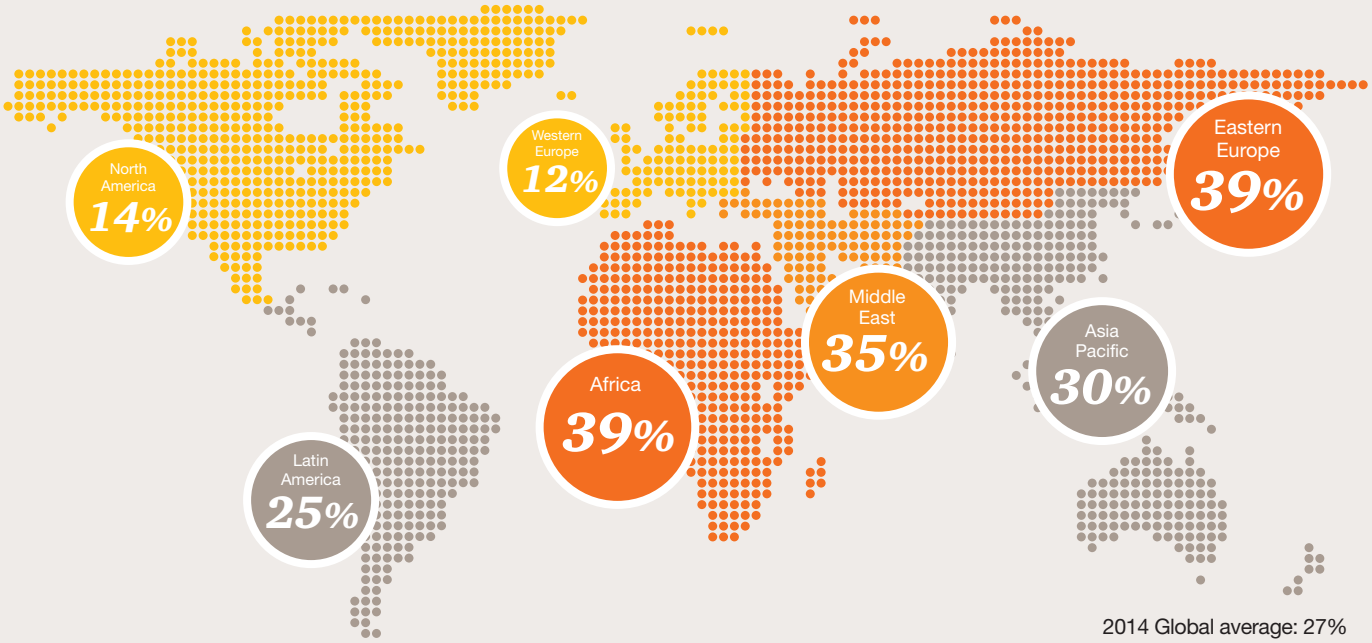
**Figure 12**
The UK experiences less bribery than the global average

## Doing business overseas

UK companies are increasingly targeting overseas growth – 41% of survey respondents said their organisation had pursued an opportunity in a high-risk market in the past two years, 21% higher than the global average.

The level of bribery reported by organisations in the UK is in line with the results across Western Europe and North America, the two regions with the most stringent anti-bribery legislation. Other regions – Africa, Eastern Europe and the Middle East – reported far higher levels of corruption. The challenge is that these high-risk territories are ones that UK businesses are expanding into.

**Figure 13**
Regions reporting experiencing bribery and corruption in the last two years




2014 Global average: 27%

It's interesting to compare UK results with North America, which operates under a similar regulatory regime and reported a similar level of bribery over the past two years. Forty-eight per cent of organisations in North America said they'd pursued an opportunity in a high-risk market in the past two years, nearly 20% more than the UK. As a result, nearly double the proportion of North American organisations had been asked to pay a bribe. The lesson here is clear: the more you do business in high-risk countries, the higher the risk of being asked to pay a bribe, or being offered one. This really brings home the importance of creating a culture of 'doing the right thing'. Businesses also need to make sure that everyone working internally, and representing the company externally, understands these values.

## *What can you do to diminish the risk of bribery and corruption, wherever you operate?*

1. **Setting the tone from the top and then doing it:** Everyone's responsible for compliance, but if senior management doesn't set the right tone – stating that bribery is not tolerated – then that message could be lost. When management do take that line, they've got to have a clear understanding of the regulatory environment and make sure their organisation has the resources to fight the threat. And if senior management don't follow up their words with action, then it will not be believed.

2. **Assess risks; address risks:** Businesses and the compliance environment are constantly evolving. Business leaders have to keep on top of these changes with periodic risk assessments. It's also important, of course, to address all risks that are identified, including the risk of unethical business conduct and the risk of a lack of integrity in business decision-making.

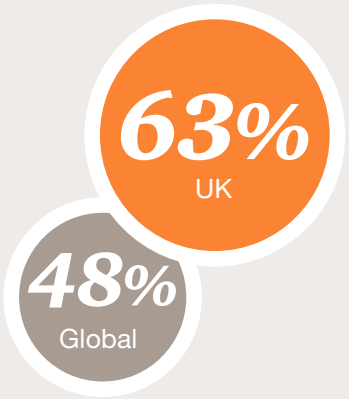
3. **Keep control:** A robust control environment needs a written code of conduct and values-based employee engagement and training (including on compliance-sensitive issues such as gifts and entertainment), as well as a system of controls that monitor suspicious transactions. Organisations are only as compliant as their weakest link, so it's important to vet and monitor anyone you do business with or who does business on your behalf.

4. **Follow up for effectiveness:** Risk assessment and control plans don't lead to compliance on their own. There's ongoing work too, such as due diligence, periodic visits from management to high-risk locations, compliance reporting to the board, hotline follow-ups, effectiveness testing, behaviours-based key performance indicators and business-partner audits.

*Only one respondent to our survey in the UK felt that they were less aware of the risks of cybercrime now than in 2011.*

# *Cybercrime*
# How real is the risk?

**Figure 14**
A higher proportion of respondents in the UK felt that the risks of cybercrime had increased over the last two years compared to the global average




Our survey shows a small drop in the percentage of organisations reporting cybercrime since 2011, however businesses are taking the threat of an attack more seriously than ever. This is particularly true in the UK, where 63% of respondents felt their awareness of the risks of cybercrime had increased over the past two years, compared to 48% globally. Only one UK respondent felt they were less aware of the risks in 2013 than in 2011. Awareness has also grown more over the last two years than in previous years – in 2011, only 47% of respondents felt their awareness of the risks had increased over the previous year.

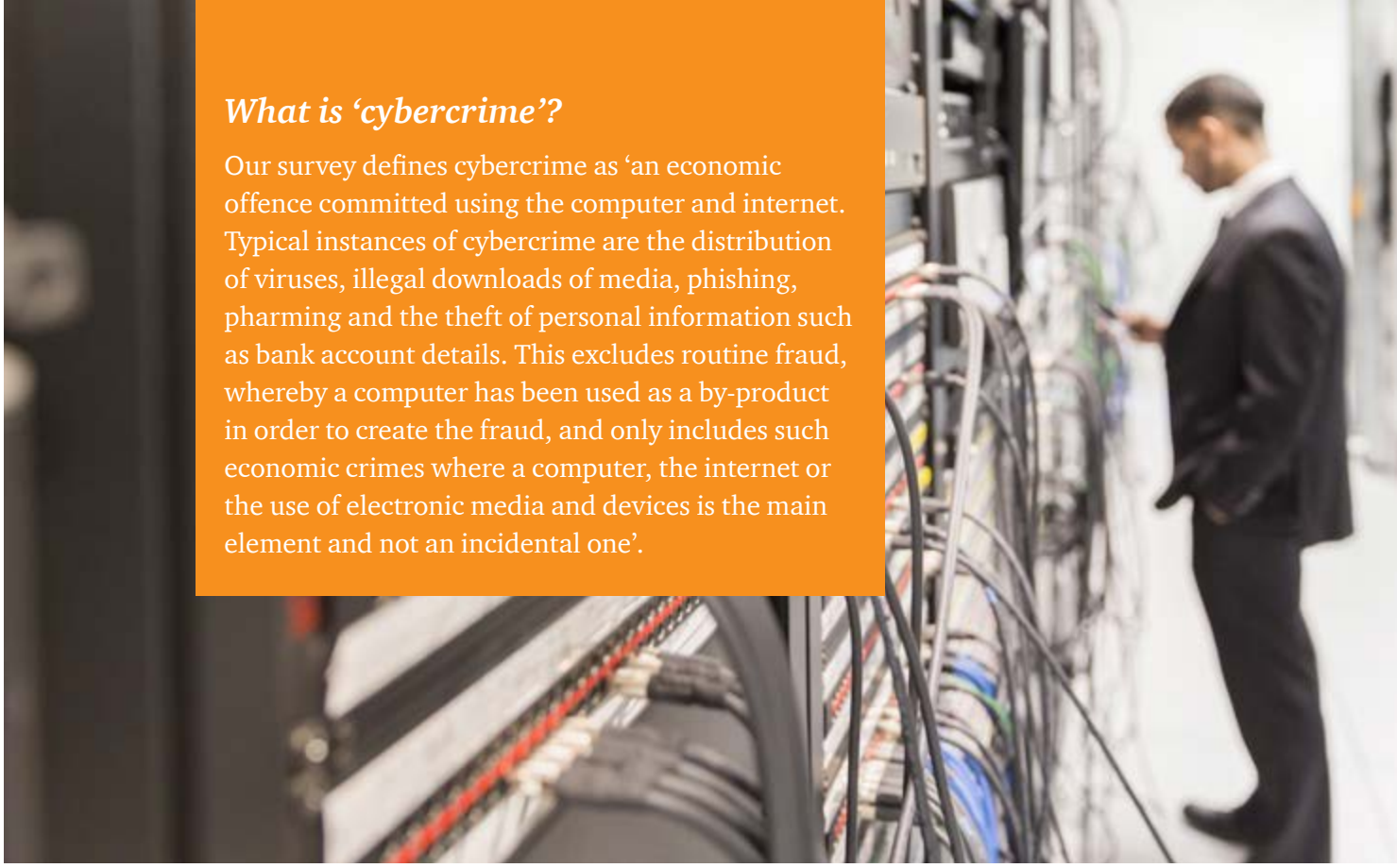
## Businesses might not be spotting cybercrime

Given this, the reported level of cybercrime in the UK – 24% of all reported frauds – seems low. That's particularly true when compared to the results of a recent survey of FTSE 350 companies by PwC and the Department for Business, Industry and Skills, which revealed that 93% of large organisations and 87% of small organisations had suffered a cyber-breach in the last year. Either the increased perception of the risk has helped organisations to keep cybercrime under control or, more likely, organisations are failing to detect cybercrime.

One problem with assessing the scope of cybercrime is the lack of a common definition – cybercrime means different things to different people. Using our survey's definition, a fraud where a computer was used to create and email a fictitious invoice to an accounts department isn't a cybercrime. Another factor to bear in mind is that not all cyber-security breaches have an immediate economic effect, so it can be difficult to quantify the financial impact.

It's also probable that, in many cases, people didn't report a cybercrime for the simple reason that they didn't know it had happened. And even when they do detect an attack, organisations might want to keep it confidential for competitive reasons, for example, if key intellectual property was stolen.

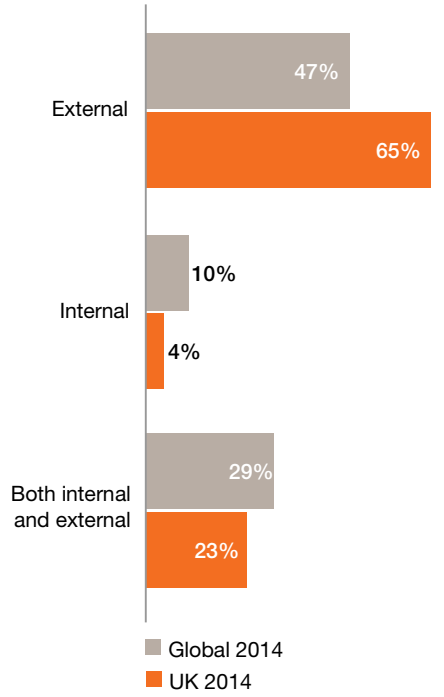
Unsurprisingly, people are most concerned about the impact that a cybercrime would have on their organisation's reputation and the subsequent service disruption. Interestingly, only 58% of our respondents said they were concerned or very concerned about the legal or enforcement costs. This is down from 78% in 2011 – most likely because of a relative lack of horror stories over the last few years.



## *What is 'cybercrime'?*

Our survey defines cybercrime as 'an economic offence committed using the computer and internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing, pharming and the theft of personal information such as bank account details. This excludes routine fraud, whereby a computer has been used as a by-product in order to create the fraud, and only includes such economic crimes where a computer, the internet or the use of electronic media and devices is the main element and not an incidental one'.

Figure 15
The threat of cybercrime is mainly seen as external




### *A management blind spot?*

Respondents to our survey said they expected cybercrime to be one of the most common types of fraud affecting their business in the next two years: 31% felt that an attack was likely, a proportion second only to asset misappropriation.

But this expectation of cybercrime varies depending on the respondents' seniority. Only 26% of board members expect to suffer a cyber-fraud in the next two years, compared to 38% of more junior management. As the responsibility for managing cyber risks sits outside or below the board – they may consider it to be an operational issue, rather than a strategic one – board members may be less concerned.

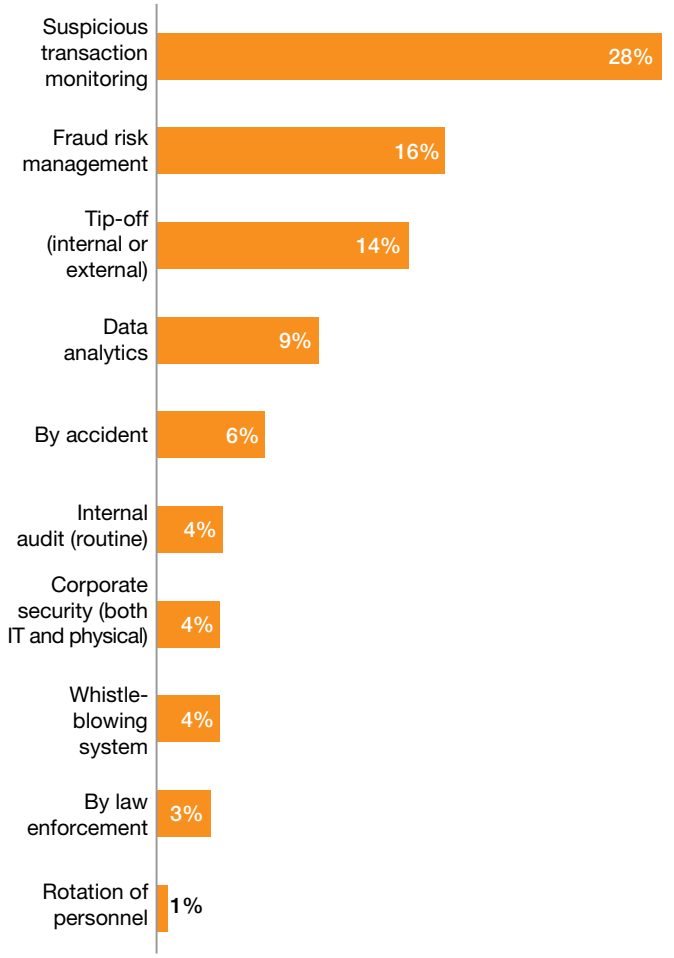
Unsurprisingly, businesses view cybercrime as mainly an external threat, with 65% of respondents feeling that the main source of danger lies outside their organisation. Far fewer respondents in the UK feel the threat is internal, or both internal and external, than the global average and the percentage of respondents in the UK who feel the threat is internal has halved in the last two years. This decline could be because of the media focus on such attacks, but there's a danger of complacency if businesses ignore the risk that comes from inside. Like procurement frauds, cybercrime can often be a result of internal and external collaboration, with an employee providing access to systems or databases to aid the criminal. A cybercrime or cyber-security issue may also result from human error, such as losing confidential data.

Whilst cyber risks are often bundled up with wider IT issues, it's important to remember that cybercrime is not wholly, or even mainly, a technology problem – it's a human problem.

*As in 2011, our 2014 survey shows that suspicious-transaction monitoring was the single most successful method of detection in the UK.*

# *Detecting Fraud*
## What works best?

**Figure 16**
Firms used suspicious transaction monitoring to detect over a quarter of frauds in the UK




### Suspicious transaction monitoring

The most successful methods of fraud detection are corporate controls and, in particular, suspicious-transaction monitoring (using a company's financial data to automatically detect irregularities and suspicious transactions). As in 2011, our 2014 survey shows that suspicious-transaction monitoring was the single most successful method of detection in the UK. Firms used it to detect 28% of frauds in the UK compared to 16% globally. Data analytics – historically reviewing a company's data to identify unusual patterns – also scored highly, detecting 9% of frauds in the UK.

As the number of frauds detected electronically has increased, we've seen 'human' detection methods like internal audit reviews and rotation of personnel become less effective. Whilst this could be down to resources being shifted to fraud-detection technology, these newer techniques aren't flawless. The ability of these programs to spot unusual transactions depends on the quality of the underlying information, plus human intelligence to review the results, spot any anomalies and investigate further.

As in 2011, our 2014 survey shows that suspicious-transaction monitoring was the single most successful method of detection in the UK. Firms used it to detect 28% of frauds in the UK compared to 16% globally.

**28%**

## *Using data to detect procurement fraud*

Nearly a quarter of respondents to our survey who had experienced fraud in the last two years had suffered a procurement fraud. Procurement fraud is a very real threat, both in terms of the potential financial loss and the reputational damage. Clients often say "it couldn't happen to us". But in the last year we've worked with clients who discovered significant losses including one who almost lost a sizeable sum as a result of a falsified change of supplier bank account details. Procurement fraud is on the rise.

However, there are genuinely new and innovative approaches to detecting procurement fraud, combining knowledge of procurement fraud with advanced data analytics techniques. This approach can detect fraud more quickly and accurately than ever before.

One good way to detect a potential procurement fraud is to perform cluster analysis on your Accounts Payable data to identify vendors who consistently demonstrate similar behaviour which may be considered normal. Using an algorithm, you can then identify a small number of clusters which exhibit subtly different behavioural characteristics to the wider population.

From hundreds of thousands of transactions and vendors, you may be able to identify just a handful of vendors that can be considered to be "outliers". Within these small "outlier" populations, you may find false-invoicing frauds, conflicts of interest and evidence of kick-backs.

## A whistle that doesn't get blown often enough?

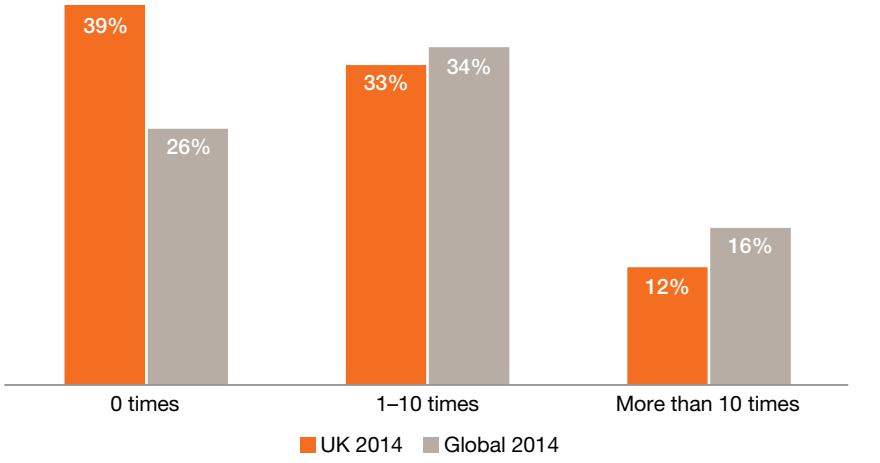
The vast majority of organisations in the UK have invested in whistleblowing mechanisms: 83% of our survey respondents said their company had one, much higher than the global average of 62%. But they're underused. We found that nearly 40% of our respondents reported that their organisation's whistleblowing hotline hadn't been used in the last two years and whistleblowing hotlines identified only 4% of reported frauds (although, obviously, whistleblowing hotlines can be used to report issues other than economic crime, like malpractice or health and safety concerns).

Media reports suggest the UK government is considering implementing a US-style system of financial incentives for whistleblowing in cases of fraud, bribery and corruption. The data from our survey suggests this could see whistleblowing being used more – only 9% of organisations in the US reported that their whistleblowing line hadn't been used in the last two years. (The global average of 26% was somewhere in between.)

Firms rarely report successful cases of whistleblowing. It's more common to see a story about someone who has lost their job as a result of blowing the whistle. This may explain the relatively low use of whistleblowing hotlines in the UK.

**Figure 17**
UK organisations are more likely to have whistleblower mechanisms


**Figure 18**
Nearly 40% of whistleblowing hotlines had not been used by UK organisations in the last two years




## The benefits of fraud risk assessments

Our survey shows a higher rate of fraud in the UK than elsewhere and we've wondered whether that is simply because the UK is better at detecting fraud. One survey finding that supports this conclusion is the fact that 75% of organisations in the UK performed at least one fraud risk assessment in the last two years, nearly 20% more than the global average. As in 2011, our survey shows that businesses that had carried out a fraud risk assessment identified more fraud in their organisations than those who didn't. The businesses we surveyed told us that fraud risk assessment identified 16% of frauds in the UK. Those who didn't run an assessment – normally because of a perceived lack of value – may be unaware of what's hiding in their books.

## *What is a fraud risk assessment?*

A robust fraud risk assessment:

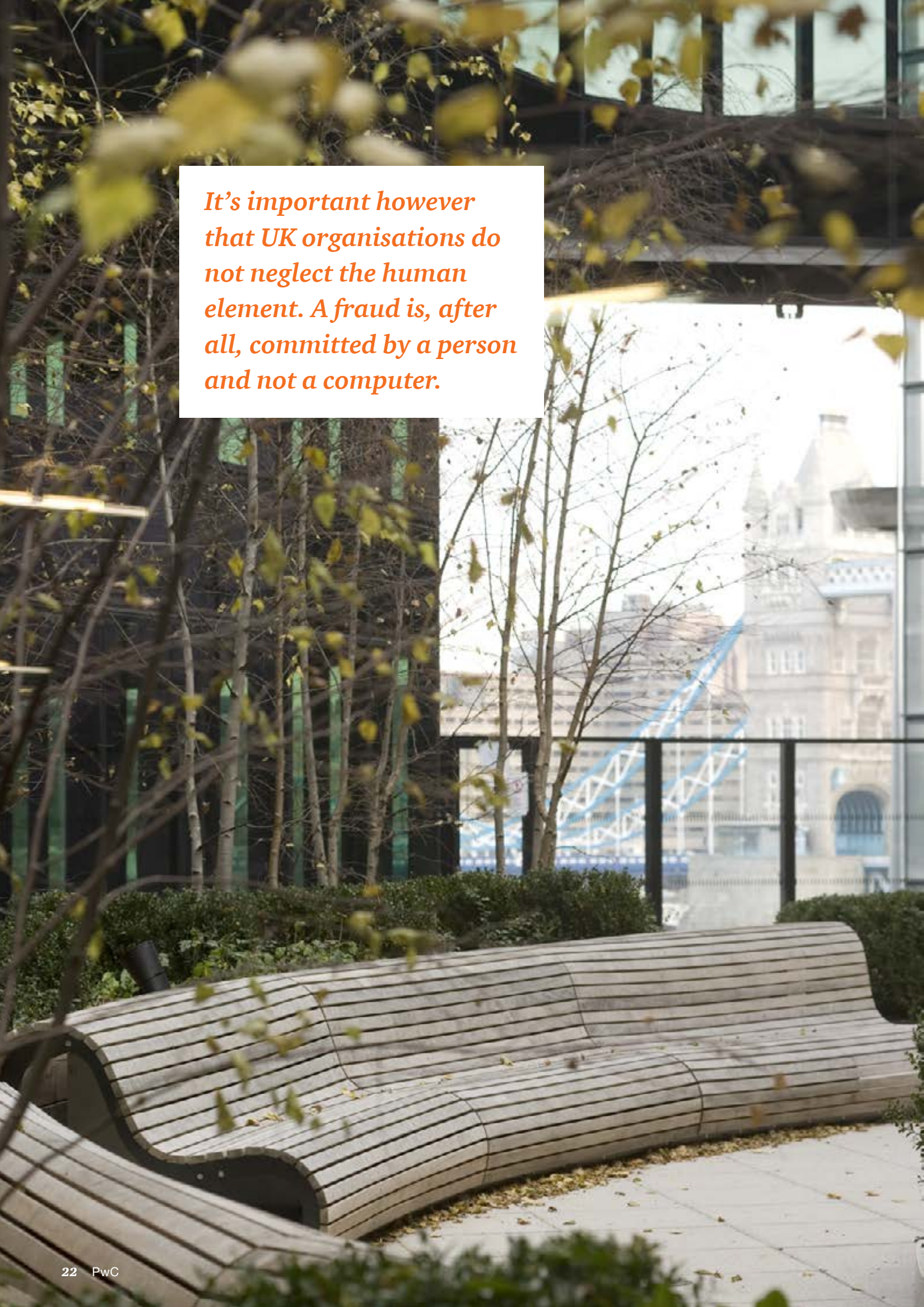
**Considers** the fraud risks that each business unit faces

**Assesses** the most threatening risks (i.e. how significant they are and how likely they are)

**Identifies** and evaluates the controls that are in place (if any) to mitigate the key risks

**Assesses** the general anti-fraud programmes and controls in an organisation

**Calls for action** to plug any gaps in the controls

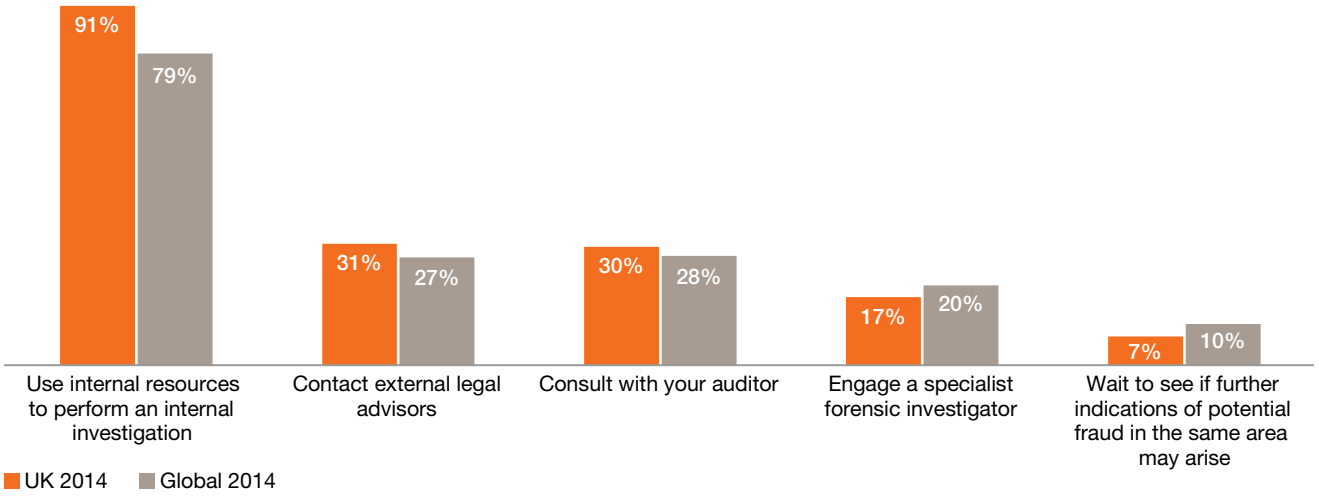


*It's important however that UK organisations do not neglect the human element. A fraud is, after all, committed by a person and not a computer.*

## What happens when an organisation detects fraud?

When someone discovers a potential fraud, nearly all respondents – 91% – use their internal resources to investigate. Respondents in the UK are more likely than the global average to contact their external auditors or legal advisors. There are signs that UK firms have lower tolerance when it comes to fraud: respondents in the UK are much less likely to do nothing than the average business globally. Investigating potential frauds can be costly and time-consuming, but doing nothing shouldn't ever be an option. Ignoring a potential fraud may allow this behaviour to continue, suggesting that the business tolerates unethical behaviour.

**Figure 19**
UK organisations are most likely to perform an internal investigation if they discover a potential fraud



*Managing the risk of economic crime isn't just about mitigating financial losses and reputational damage. It's also a chance to gain competitive advantage.*

# How to cut back on fraud

The most efficient and cost-effective way to deal with economic crime is to be proactive, focus your resources on prevention, and let intelligent automated systems shoulder the burden of detection. Our survey shows that businesses are increasingly using suspicious-transaction monitoring to detect frauds, and having less success with conventional methods, like whistleblowing hotlines and internal audit reviews.

It's important that UK organisations don't forget the human side of fraud. Fraud is, after all, committed by a person and not a computer. This year, we've seen a change to the profile of the typical fraudster, with more junior employees committing crimes than in previous years. We've also seen a rise in the number of frauds committed by staff, rather than external parties. So it's important to keep an eye out – fraud may come from a place or a person that you least expect.

As UK companies expand overseas, there's an increased risk of bribery and corruption. Breaching the UK Bribery Act comes with severe consequences – unlimited fines and up to ten years in prison – so organisations need to make sure that everyone who works for them, or on their behalf, understands how they need to behave, wherever in the world they're working. Setting and embedding the standard of ethical behaviour you expect from all your people, wherever they are, is a critical step in mitigating the risk to your business.

Managing the risk of economic crime isn't just about mitigating financial losses and reputational damage. It's also a chance to gain competitive advantage.

# Contacts


**Ian Elliott**
Partner, Head of Investigations
+44 (0) 20 7213 1640
ian.elliott@uk.pwc.com

**Andrew Gordon**
Partner, Forensic Services UK Leader
+44 (0) 20 7804 4187
andrew.gordon@uk.pwc.com

**Keith McCarthy**
UK Survey Project Lead
+44 (0) 20 7804 3914
keith.v.mccarthy@uk.pwc.com

**Ketan Vaghjiani**
UK Survey Marketing Manager
+44 (0) 20 7212 2359
ketan.vaghjiani@uk.pwc.com

**Kathryn Westmore**
UK Survey Project Manager
+44 (0) 20 7213 2941
kathryn.m.westmore@uk.pwc.com


## *PwC Forensic Services*

Our team of specialists, based all around the world, can tackle any crisis or anxiety costing you sleep: corruption, fraud, cybercrime, contract disputes, litigation, intellectual property and licensing compliance, insurance claims, regulatory investigations, and so on. We're your trusted advisor, your expert witness, your investigator and your representative in mediation and arbitration. We fight threats to your brand and bottom line – anywhere and everywhere, at a moment's notice.

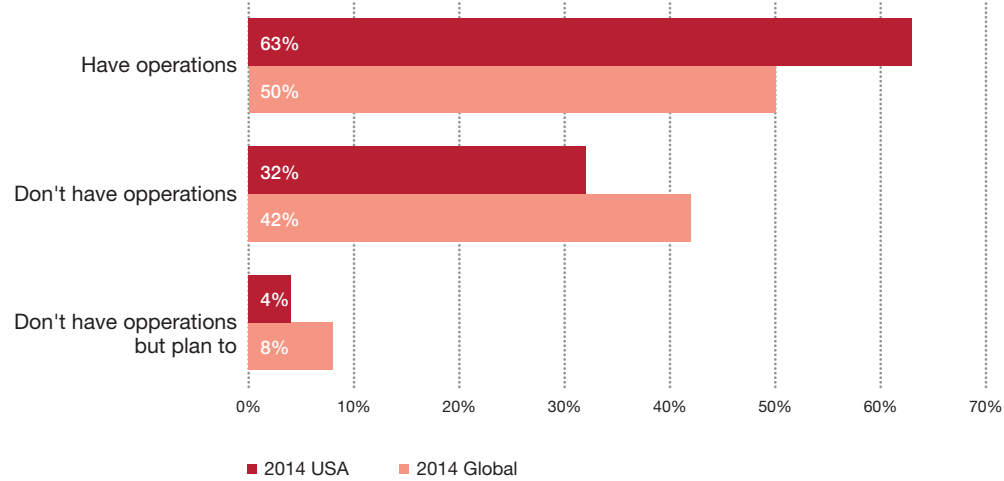
www.pwc.co.uk/forensics

*www.pwc.co.uk/crimesurvey*

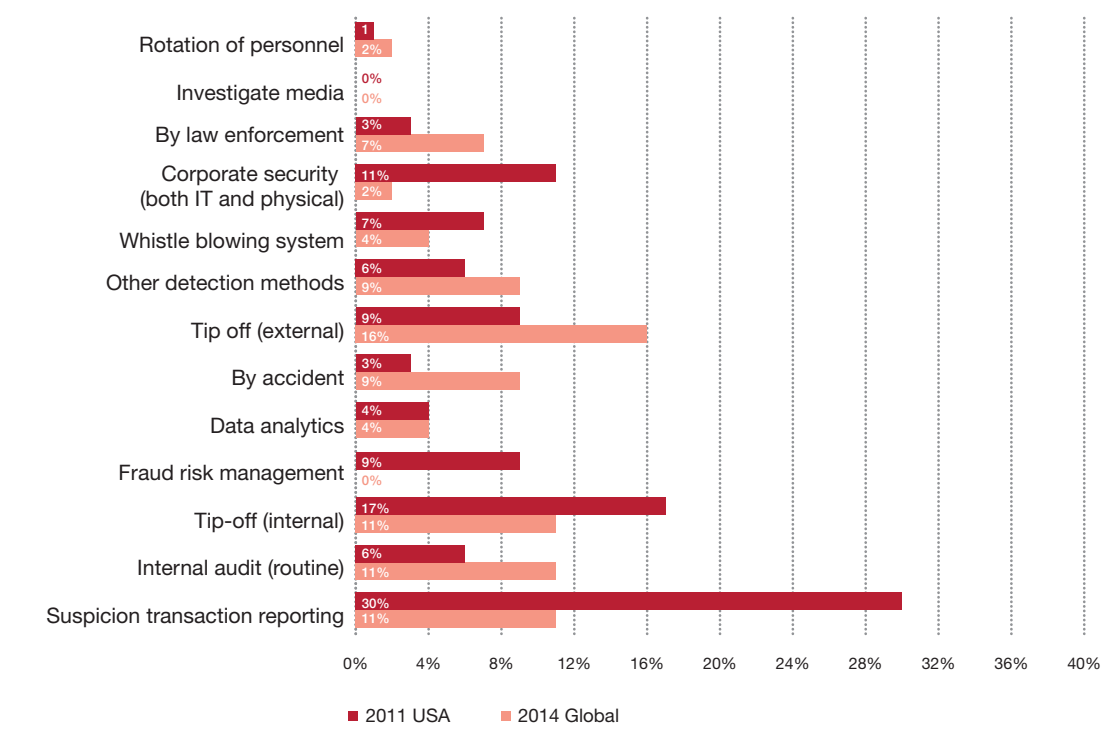
PwC UK helps organisations and individuals create the value they're looking for. We're a member of the PwC network of firms in 157 countries with more than 184,000 people committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com/uk.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it. © 2014 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

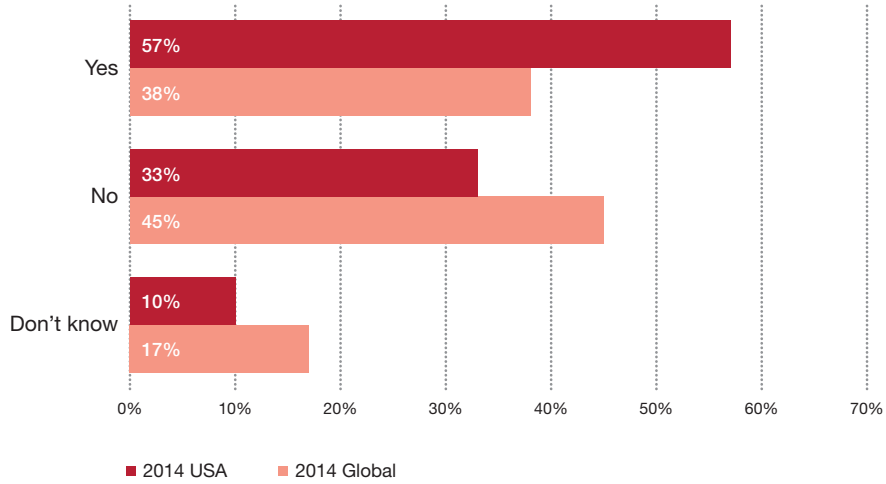
The Design Group 21634 (02/14)



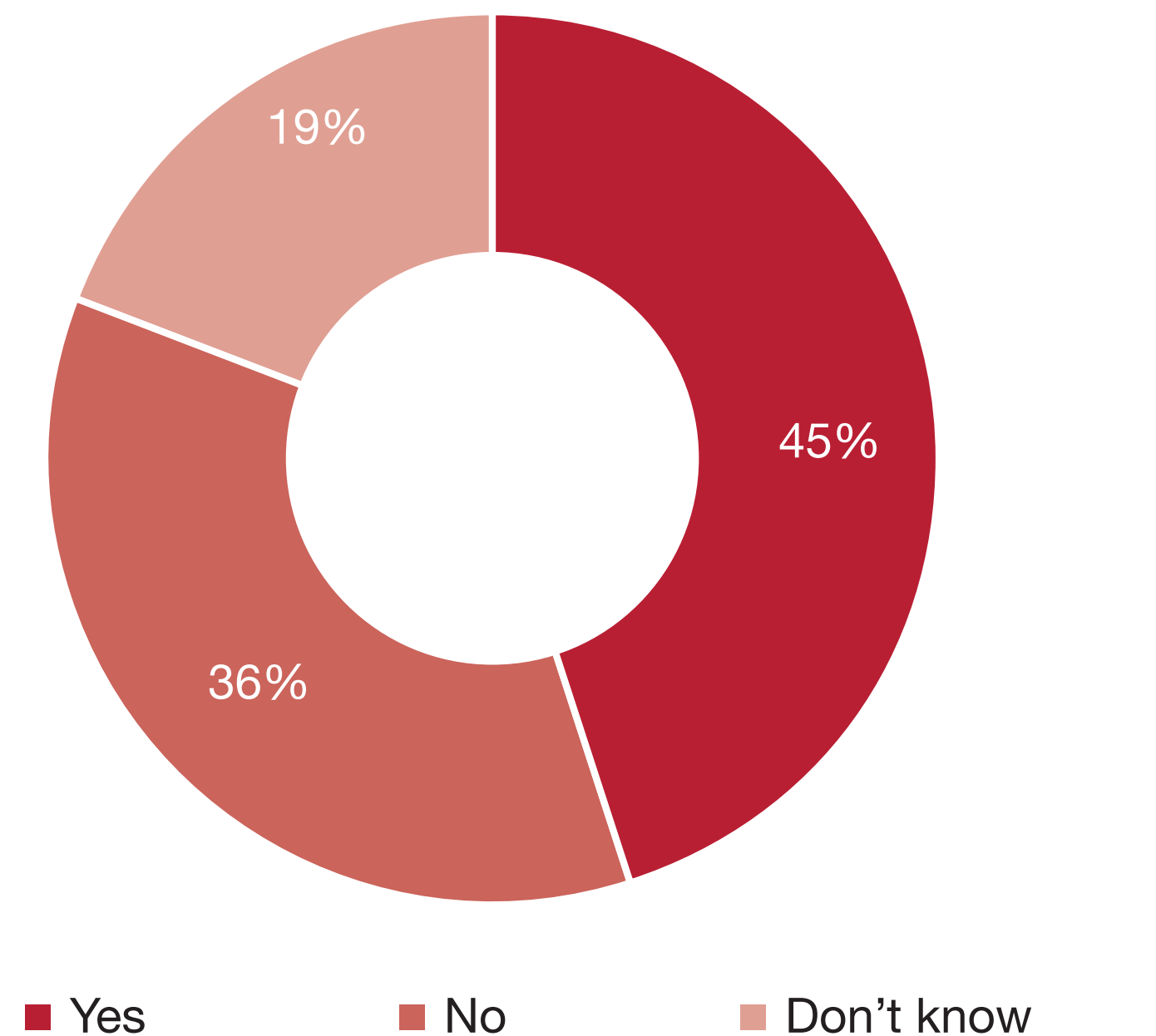

Source: *PwC, 2014 Global Economic Crime Survey—US Supplement*, February 2014



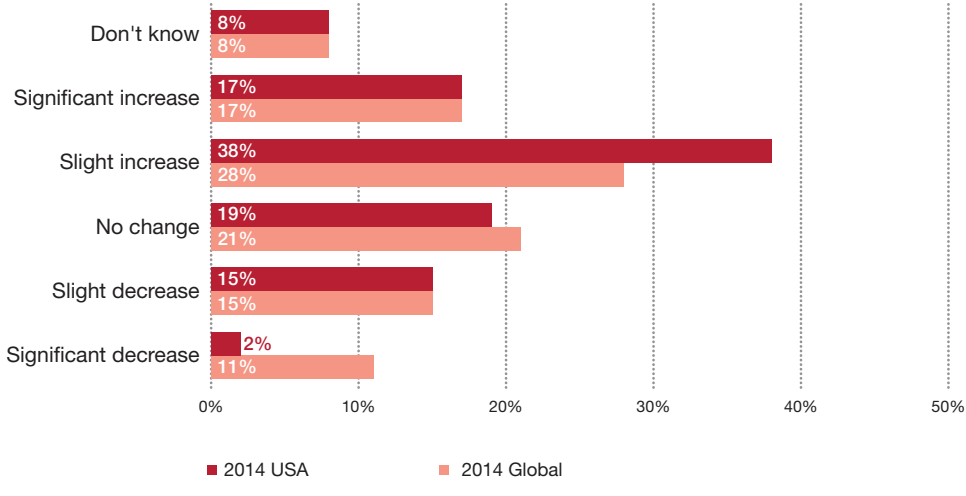

Source: *PwC, 2014 Global Economic Crime Survey—US Supplement*, February 2014



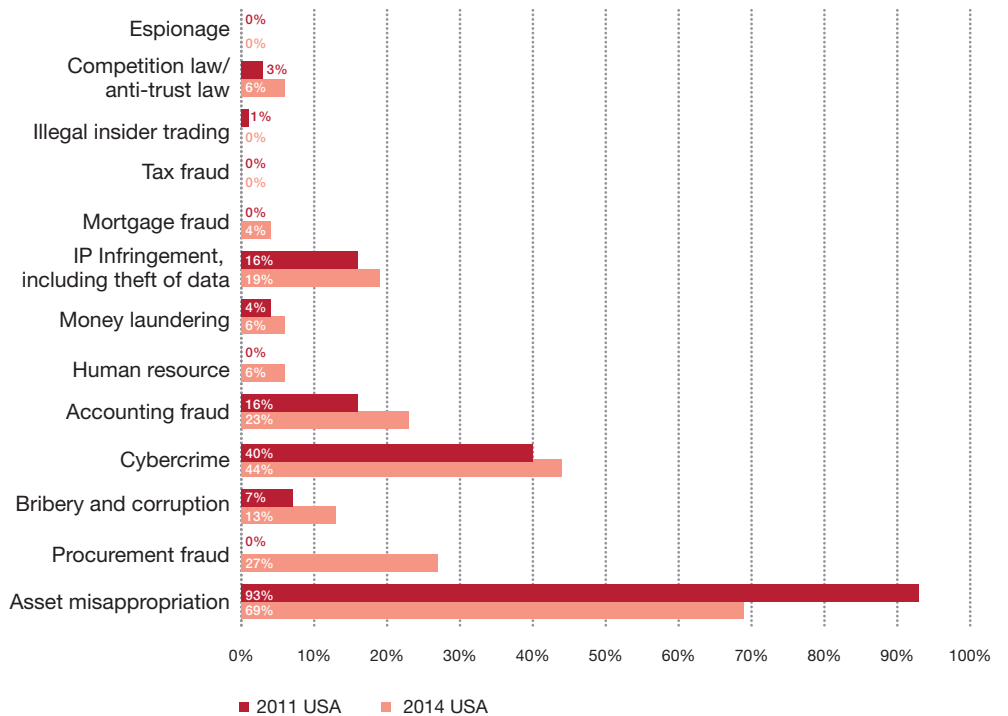

Source: *PwC, 2014 Global Economic Crime Survey—US Supplement*, February 2014



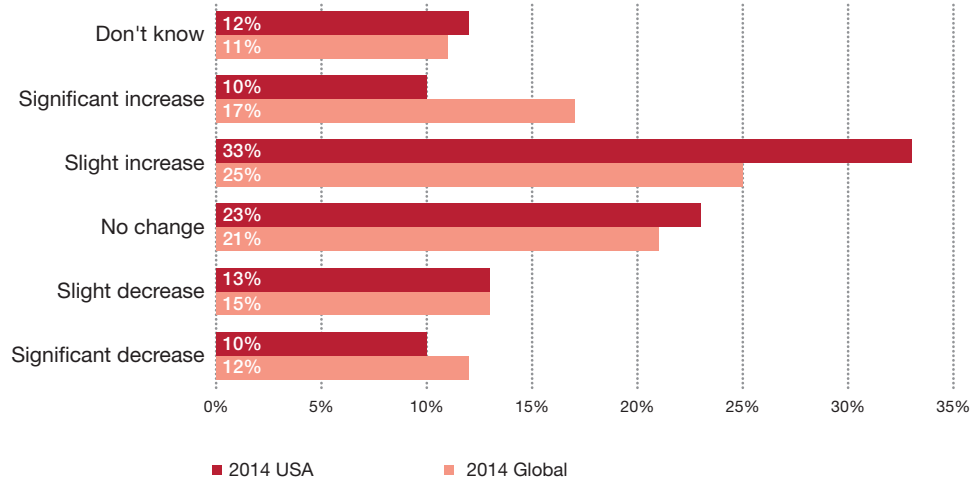

Source: *PwC, 2014 Global Economic Crime Survey—US Supplement*, February 2014



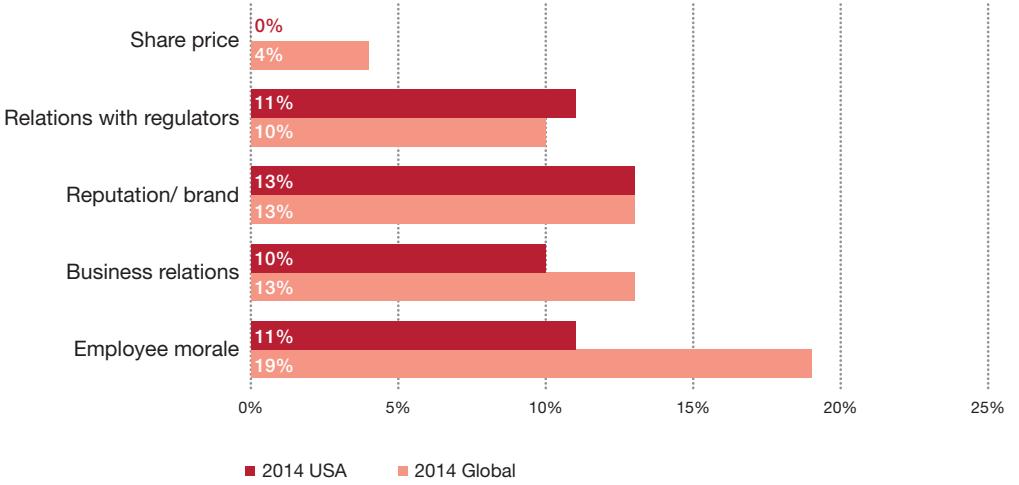

Source: *PwC, 2014 Global Economic Crime Survey—US Supplement*, February 2014




Source: *PwC, 2014 Global Economic Crime Survey—US Supplement*, February 2014




Source: *PwC, 2014 Global Economic Crime Survey—US Supplement*, February 2014




Source: *PwC, 2014 Global Economic Crime Survey—US Supplement*, February 2014

# *Economic crime: a threat to business processes*

**45%**
of U.S. organizations suffered from economic crime in the past two years.

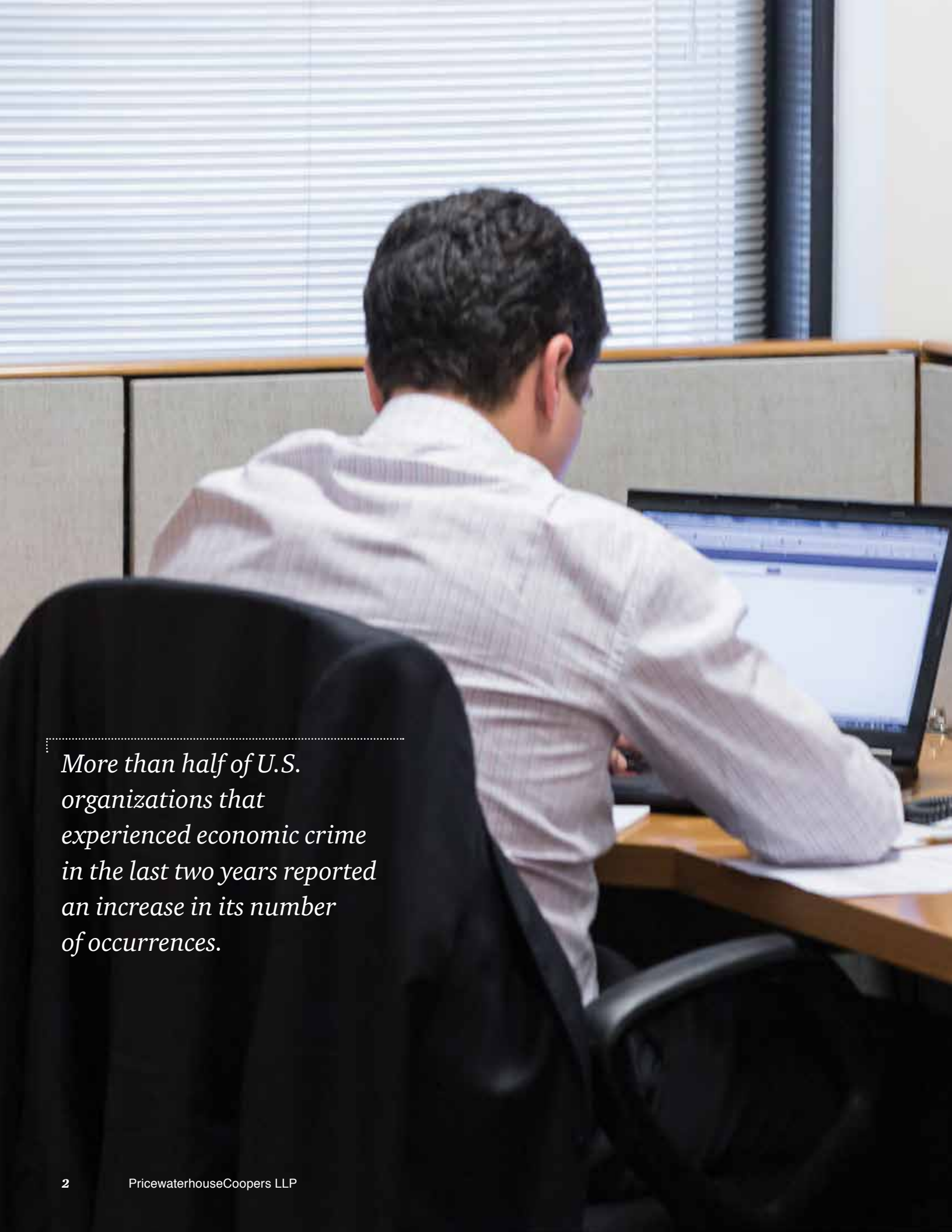
**67%**
of U.S. organizations currently have or planned to have operations in high-risk markets.

**71%**
of U.S. respondents perceived an increased risk of cybercrime over the past 24 months.

pwc

*Economic crime continues to remain in the forefront of corporate concern, posing a threat to fundamental business processes.*

# Contents



*More than half of U.S. organizations that experienced economic crime in the last two years reported an increase in its number of occurrences.*

# *Foreword*
## by Sean Joyce

In 2014, the threat posed by economic crime is fresh in our collective memory as we work to recover from a financial meltdown and near economic collapse caused by fraudulent practices in our financial markets. While important strides have been made in recent years, economic crime continues to pose a grave threat to financial interests in the United States as a whole, and to US businesses both at home and abroad. Economic crime is an ever evolving threat, and new criminal trends relentlessly emerge in different sectors and industries as economic events, natural disasters, and innovation re-shape our world.

### *Economic crime has become a truly borderless threat*

The very technology that binds our global economy and facilitates international commerce has created ample opportunities for abuse. Once-novel threats like cyber-attacks are no longer confined to obscure hacker groups operating in the shadows of our economy; but have become a key weapon in the arsenal of common criminals, organized crime rings, and foreign nation-states. Many companies do not appreciate the gravity of the threats they are facing. Many businesses are often unaware that their systems have been probed or penetrated by criminal elements, let alone the implications these security breaches could have on their business activities. Corporate management must increasingly confront a difficult question—how do you protect yourself when you do not even know you are under attack?

Foreign states have also recognized the potential value of cybercrime, and now routinely support efforts to exploit vulnerable networks to steal cutting-edge technology from US companies. Billions of dollars in investment and R&D can be lost in a matter of minutes. With many US companies at the forefront of innovation, we can expect cyber-attacks and related schemes to increase in frequency and magnitude, resulting in substantial intellectual property, trademark, and patent violations in the coming years.

Technology has allowed criminal elements to extend their reach across national boundaries, vastly expanding their pool of potential victims. Securities fraud schemes originating from countries such as Thailand, Spain and Canada can now target vulnerable investors across the globe, including the United States. The promise of the global economy has been distorted to trick unsophisticated investors into purchasing worthless penny stocks or investing in phantom infrastructure projects in foreign countries. Oftentimes the victims of these crimes represent the most vulnerable sectors of our economy—the elderly, the ill-informed, and those most in need of financial good fortune.

### *Tending our backyard*

The United States has proved to be fertile ground for domestic economic crime in recent years. Catastrophic coastal events on the Eastern and Gulf coasts have generated rampant insurance fraud that squanders taxpayer dollars and undermines community relief and reconstruction efforts. Farther inland, natural gas exploration and fracking have led to boom towns sprouting overnight in places like North Dakota, Wyoming, Utah, and Texas. Many of these towns do not have the infrastructure or governance capability to handle the influx of people, and crime, that inevitably accompany boom-town dynamics. Land lease and mineral rights agreements, zoning ordinances, permits, and licenses have become particularly vulnerable to exploitation.

While certain vulnerabilities in the domestic banking sector, such as bank fraud and loan origination fraud has decreased with improved due diligence, criminals have adjusted their tactics to exploit new weaknesses. Loan modification schemes have become increasingly prevalent, including foreclosure rescue and “own your own home” scams that target unsuspecting American consumers. Once again, it is often the most vulnerable segments of our population that suffer the most severe consequences.

These examples demonstrate that economic crime is a dynamic threat to businesses and consumers alike; and requires a nimble and varied response. For businesses in particular these threats require a second look at many aspects of operations—from the beginning of the supply chain to the consumer. How you sell, who you accept as a vendor, who you partner with in foreign markets, how your HR processes like recruiting and training work—are just some of the fundamental business activities that are threatened by economic crime. We hope that the following report will provide valuable insight to help stakeholders in the private and public sector improve their response to this ever-evolving threat.

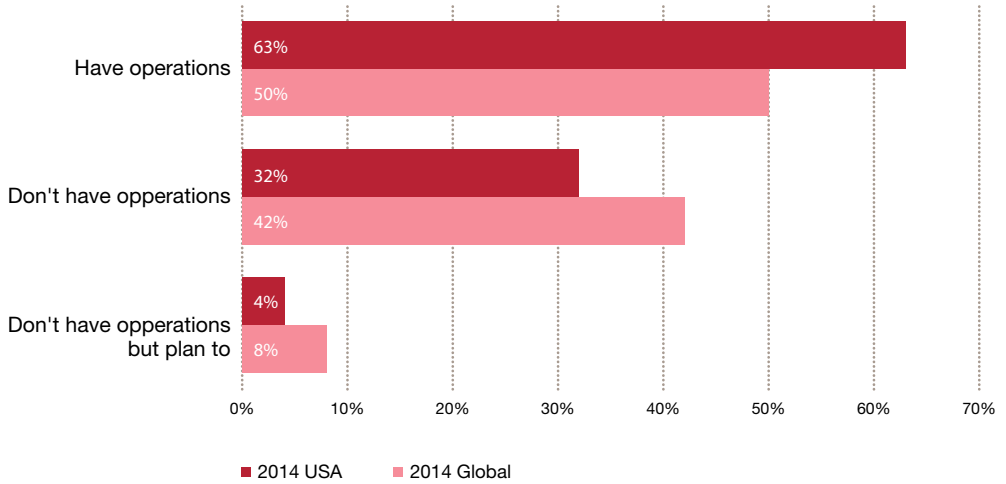
*Although US organizations are more likely to have operations and pursue opportunities in high risk markets, they experience less corruption than their global peers.*

# A global landscape, a global outlook

We are pleased to present the US Supplement to the 2014 Global Economic Crime Survey (GECS). This year's GECS features the perspectives of more than 5,000 respondents from over 100 countries on the prevalence and direction of economic crime. The US Supplement provides an in-depth discussion of the issues facing US-based respondents who participated in the GECS. We will focus on how the perception, incidence, and impact of economic crime changed since our 2011 survey, or differed from global patterns. We will also identify situations that encourage fraud's occurrence and provide methods and strategies to avoid, detect, and mitigate economic crime.

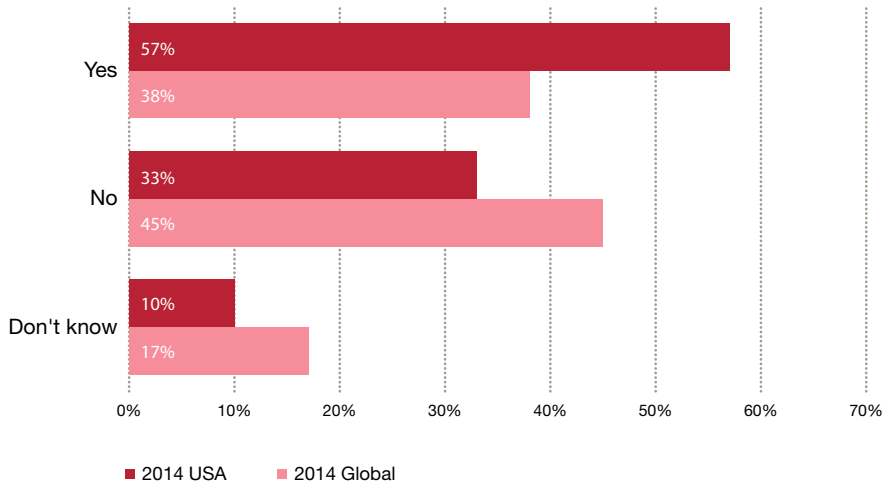
The US respondents' operations differ from those of their global peers in key ways. As in 2011, our US participants reported a larger global footprint, with 80% noting worldwide operations compared to 61% globally. US organizations were also more likely to both have operations and pursue opportunities in markets with high-levels of corruption risk [1] (Figures 1 and 2, respectively). Sixty-seven percent of US respondents indicated their organizations currently have or planned to have operations in high-risk markets, compared to only 58% of global respondents. And 57% of US respondents (versus 38% globally) indicated their organizations pursued opportunities in markets with high-levels of corruption risk within the past 24 months. One reason that so many companies are doing business in high-risk markets is that the economic downturn has pushed businesses to turn their attention to developing markets in order to drive revenue growth. In addition to market opportunity, many developing markets are more likely to present elevated corruption risk.

**Figure 1: High level corruption markets**




1 Defined as a territory with a Transparency International Corruption Perception Index ("CPI") score of 50 or less.

**Figure 2: US organizations pursuing opportunities in market with a high level of corruption risk**

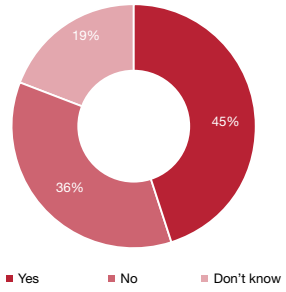



US companies are growing their international operations, and the expanding role of the internet and mobile technology in business can bring risk from beyond their geographic footprint. US employees are equipped with "smart" mobile technology, tablets and laptops which allow for business to be conducted anywhere, anytime. Thus, companies are operating in a "borderless" society in which they may not need to have a bricks-and-mortar operation in a given country to have a presence and possible risk. Additionally, companies may engage sales agents, distributors, consultants and other service providers to drive sales and business operations, which may expose companies to increased risks including corruption, cybercrime, and economic sanctions.

Our 2014 US CEO Survey reveals that executives are seeking more strategic alliances in 2014: 42% plan to enter one this year; only 4% expect they'll exit an existing relationship. They are also planning acquisitions: 39% of US CEOs plan to complete a domestic acquisition this year and 28% are planning on a cross-border deal. As we will see, US respondents are aware of the dangers some third party relationships can present. Whether a company is planning to acquire, partner with or do business through another entity, proper due diligence can help identify and quantify their problems before they become your problems.

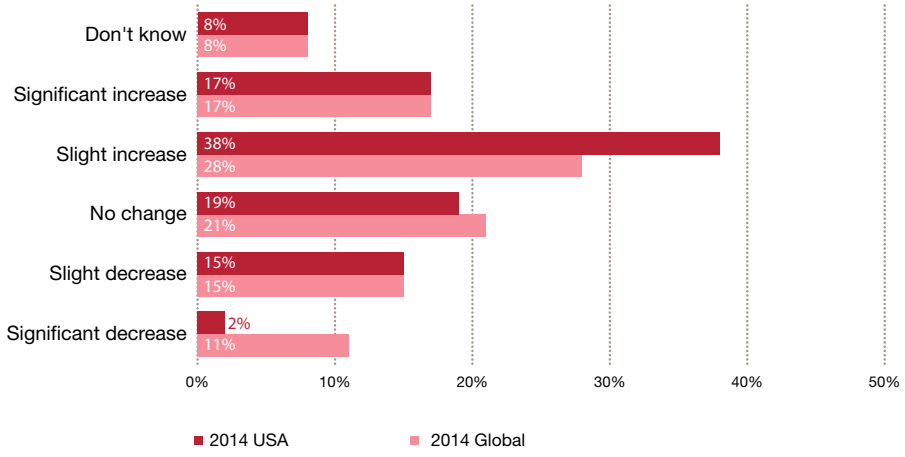
# Economic crime remains in the headlines

**Figure 3: U.S. Organizations reporting incidents of economic crime**




The investigation and prosecution of economic crime, particularly in the wake of the financial crisis, remain at the forefront of public concern. In our 2011 report, we discussed that the additional public scrutiny involving recent high-profile investigations and prosecutions may have heightened the awareness of fraud within organizations, resulting in more organizations reporting fraud (45% in 2011 compared to 35% in 2009). Our 2014 survey results support this idea. As the US economy recovers from the financial crisis, the number of organizations that reported suffering from fraud levelled off at 45% during the survey period (Figure 3).[2] However, over half of respondents who indicated their organizations did suffer fraud reported an increase in the number of occurrences (56%), representing a continuing upward trend in the occurrence and detection of economic crime (Figure 4).

**Figure 4: Perceived changes in the number of occurrences of economic crime**




2 A note about comparative data: In our 2011 survey, respondents were asked to consider the previous 12-month period. In 2014, to align with the bi-annual nature of the survey, we asked respondents to consider the previous 24 months. While we make no comparisons here involving absolute numbers, readers should take into account the longer analytical timespan of the 2014 survey data in assessing trends.

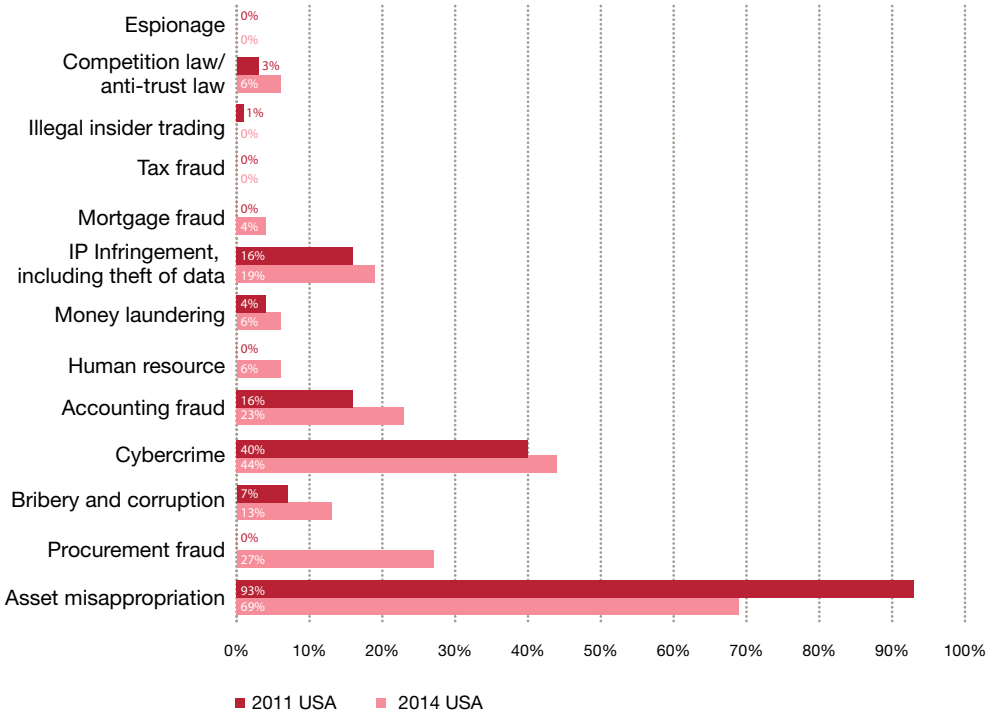
*Incidents of asset misappropriation plummeted by 24% during the survey period, and are now in line with the global average (69%).*

# Charting the landscape of economic crime

The survey results reflect a significant shift in the types of crime suffered by organizations. The distinctions among types of fraud reported by organizations decreased during the survey period, reflecting that organizations are more likely to suffer from a range of economic crimes rather than from one or two discrete types.

As shown in Figure 5, we asked organizations about the types of fraud they experienced. This year, we refined this question by adding three new classifications of economic crime—procurement fraud, human resources fraud, and mortgage fraud. Despite the addition of these new categories, US organizations reported that they experienced increased levels of fraud across all types of economic crime since 2011, except for asset misappropriation and insider trading.

**Figure 5: Types of fraud**



While asset misappropriation remains the most common fraud US organizations suffered, it plummeted from 93% in 2011 to 69% during the survey period. Incidents of asset misappropriation suffered by US respondents are now in line with those reported globally (also at 69%). However, organizations shouldn't downplay its risks, prevalence or likelihood of occurring.

It is unlikely the decrease in asset misappropriation is due to respondents selecting mortgage fraud since these types of fraud are dissimilar and unlikely to be confused. However, it may be possible that some of the decrease is related to adding human resources fraud and, to a lesser extent, procurement fraud in the survey. Additionally, asset misappropriation may be most directly tied to economic pressures from the global recession, and the decrease in reported instances may partially be explained by an improving economy.

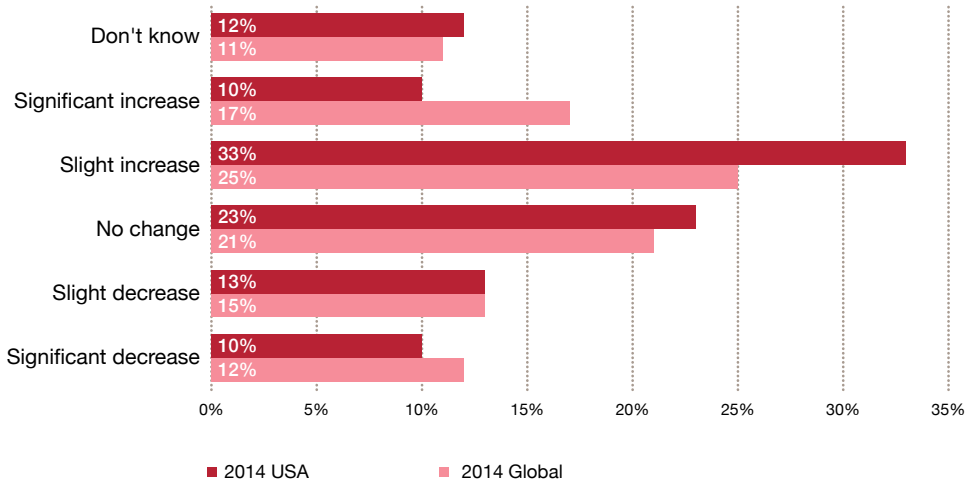
Two types of fraud—accounting fraud and bribery & corruption—made comebacks in 2014. In our 2011 report, we anticipated that these types of fraud would grow in the next few years in the wake of more regulation, stricter enforcement, and increasing investigations. In this survey period, accounting fraud at US businesses essentially rebounded to 2009 levels (23% in 2014 vs. 24% in 2009), after experiencing a drop to 16% in 2011. Similarly, bribery & corruption at 14% doubled from 2011 levels (7%) after dropping by more than a half since 2009 (16%). The increase in accounting fraud and bribery & corruption may be attributable in part to more companies implementing or enhancing internal controls, more robust compliance programs and increased risk assessments, thus leading to more frauds being detected.

Similar to 2011, no US respondents reported suffering from tax fraud or espionage in the survey period and, as previously mentioned, reports of illegal insider trading fell from 1%. Yet companies should remain vigilant; much like lightning, the chances these crimes may affect a business are statistically remote, but they can be potentially devastating should they strike.

# What's the bottom line?

The reality of fraud is that it can be as impactful to a company's revenues as other business and market forces. The abilities to prevent, detect and swiftly respond to fraud can be powerful cost-savings tools. The survey revealed that 54% of US respondents reported their companies experienced fraud in excess of $100,000 with 8% reporting fraud in excess of $5 million. Sixty-six percent of the respondents indicated the financial impact of economic crime on their organization remained the same or increased over the past 24 months, compared to only 23% who indicated a decrease (Figure 6). As discussed in further detail later in the report, the statistics support that executing stronger fraud prevention and detection measures could lead to a reduction in fraud and its financial cost. By implementing more robust anti-fraud controls, organizations can prevent losses and increase savings and profitability.

**Figure 6: Perceived changes in cost of fraud**



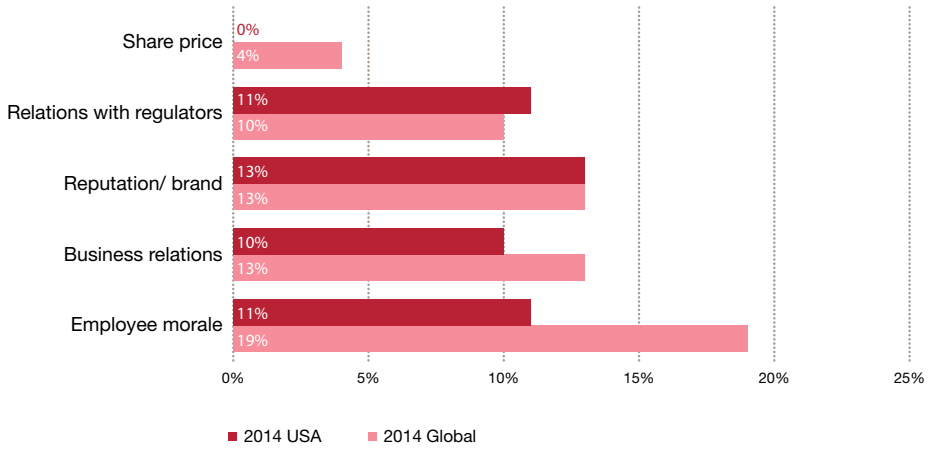

The Department of Justice (DOJ) and Securities Exchange Commission (SEC) both consider a company's existing compliance program and cooperation in determining how to resolve investigations. Having a robust compliance and ethics program, self-reporting, providing full cooperation and accepting responsibility often lead to reductions in an organization's culpability score, possibly reducing fines and penalties. Conversely, unreasonable delays reporting the offense could lead to an increase in a company's culpability score, and the corresponding fine imposed. Companies have the ability to directly influence the cost of fraud by implementing an effective and updated corporate compliance program, and conducting comprehensive internal investigations once wrongdoing is uncovered.

# Collateral damage

The effects of fraud cannot be completely measured in dollars alone. In fact, economic crime may have a more damaging effect on intangibles such as brand, reputation, and employee morale than on the immediate bottom line. Ultimately, this collateral damage may impact revenue, earnings and growth years after the crime has been uncovered.

The survey reflects that companies are recognizing the threat of indirect damage. US respondents indicated that the indirect impact of fraud across all categories increased from 2011, with the exception of relations with regulators which experienced a small 1% decline from 2011 (Figure 7).

**Figure 7: Impact of fraud**




The reality is clear—organizations recognize that rebuilding employee morale, customer goodwill and brand loyalty, and re-establishing trust with business partners and regulators ultimately impact profitability, even if these factors don't appear on organizations' balance sheets or income statements. These kinds of losses, while difficult to quantify in financial terms, can be more significant and longer-lasting than the initial financial impact of fraud, and they can be harder to control. In today's highly connected world where the internet, social media and 24/7 news channels drive the news cycle, it is increasingly difficult for organizations to control the message when bad news occurs. The good news is that companies often emerge stronger and more resilient by building a strong compliance and threat management system, recapturing market share lost as a result of crisis. Often, a thorough review of the compliance environment identifies ways that an organization can improve transparency and the flow of information connected to its business processes, providing benefit and efficiencies to the entire company.

# Go to battle against fraud (because your business processes are under attack)

Not only does economic crime expose companies to regulatory and legal peril and monetary loss, but it can also strike at a company's strategic business goals and objectives. For instance, bribery and bid rigging can not only lead to inflated costs, arrest and eroded business relationships, but can also lead to substandard safety. In addition, accounting and tax fraud can not only mask larceny, but can also disrupt the free flow of vital information needed to make strategic business decisions; such as in merger and acquisition deals where misrepresented and falsified financial information can impact a potential acquirer's valuation of a target company. Cybercrime and data theft not only compromise customer data and critical company information, but also may disrupt the confidence a company places in its otherwise innovative IT strategy, hurt its goodwill with customers and can lead to expensive remediation costs when an attack does occur.

Every business unit has a stake in minimizing the company's exposure to economic crime. What this means is that responsibility for fraud control and prevention belongs to everyone in an organization, not just its legal or compliance functions. Additionally, those on the front lines such as controllers, IT technicians and salespeople are the company's "eyes and ears" and are also most likely to be the first responders in the wake of a crisis. Treating economic crime as a business concept, and integrating prevention into business strategies, can maximize compliance and detection and help ensure that a company will remain vigilant on all fronts.

### *The perils of economic crime*

Fraud and economic crime can cause financial harm, but sometimes it can endanger employee and public health. Shortcuts and inferior product substitution can affect the structural stability of construction projects. Bid rigging and kickbacks can lead to the selection of substandard contractors or unskilled labor. Environmental crimes can often be traced back to efforts to cut costs or extract revenue. Product substitution or counterfeiting can impact automobile and aircraft safety. Pharmaceutical crime is growing according to Interpol, and counterfeit medication puts lives at risk. Disruption to municipal computer systems by cyber criminals or hacktivists can compromise public security systems. Lead contamination and food borne illnesses can result from supply chain fraud or negligence.

## *Macro trend: urbanization*

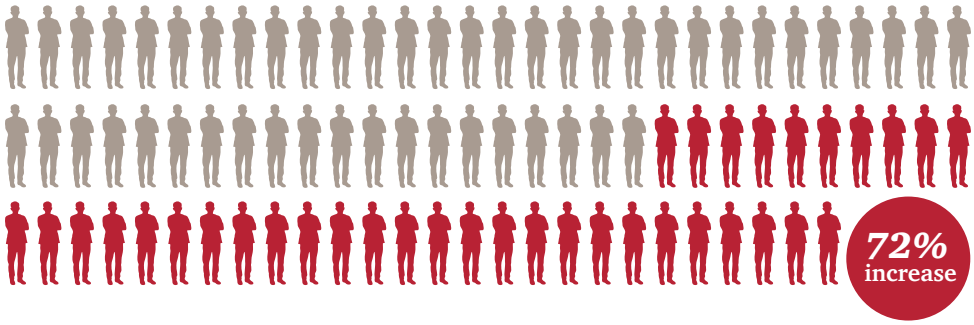
*"The 19th century was a century of empires, 20th century was a century of nations and 21st century will be a century of cities."*

—Wellington E. Webb, former mayor of Denver.

As we continue to move closer together, cities create opportunities for greater connectivity, culture, innovation, productivity and energy efficiency. However, as cities grow and change, they may have an effect on the economic crime landscape.

The demand for infrastructure as well as residential and commercial construction will increase; however those projects often bring high levels of interaction with government officials, heavy reliance on third parties and an industry (Construction & Engineering) with historically high corruption risk. Companies and municipalities alike should ensure they have adequate safeguards in place to prevent and detect such crimes as bribery, bid rigging, kickbacks and contract fraud.

## World urban population




The world urban population is expected to increase by 72% by 2050

Source: World Urbanization Prospects: 2011 Revision, produced by the UN Department of Economic and Social Affairs

# Cybercrime is here to stay

Our 2011 survey focused on the increasing prevalence of cybercrime—and the 2014 results confirmed this trend. Forty-four percent of US organizations that suffered from economic crime in the past 24 months identified cybercrime as one of the frauds experienced, while 44% of all US organizations indicated they thought it was likely they would suffer from cybercrime within the next 24 months.

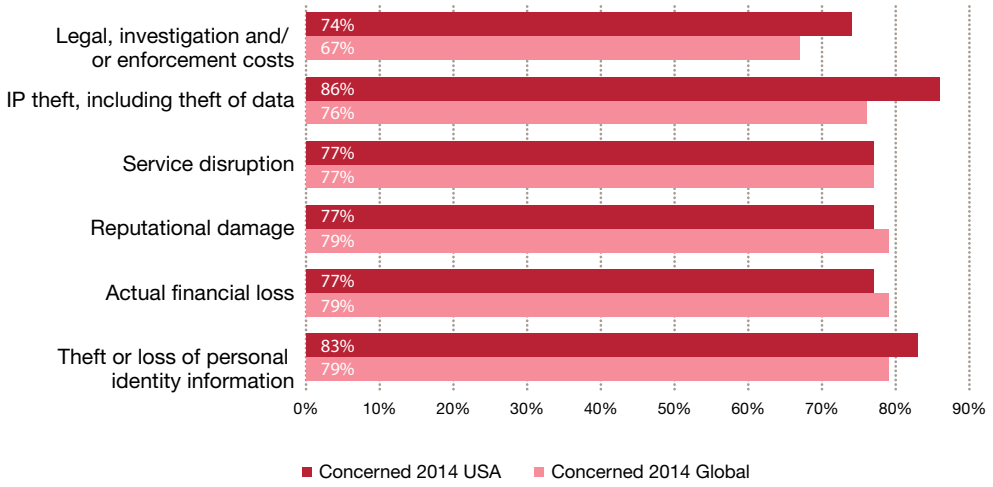
The Internet has changed the way the marketplace operates since virtually all organizations somehow rely on it to conduct business. Additionally, more business processes are automated and more customer and proprietary data are available in digital form. Mobile technology has become an accepted medium for commerce. More organizations and consumers rely on cloud computing and storage for both internal processes and customer data, a trend that will continue to increase over time. It is not surprising that cybercrime has moved to the forefront of companies' concerns. Companies are beginning to change how they think about cybersecurity—viewing it as a business issue, not just an IT issue:

- Seventy-one percent of US respondents indicated their perception of the risks of cybercrime increased over the past 24 months, rising 10% from 2011.
- US respondents' perception of the risks of cybercrime exceeded the global average by 23%.
- US respondents still perceive the greatest cybercrime threat coming exclusively from the external cybercriminal. However, this trend is shifting from 2011 and the internal cybercriminal is closing the margin.
- Compared to their global counterparts, US organizations lost more through cybercrime in financial terms: 7% of US organizations lost $1 million or more, compared to 3% of global organizations; 19% of US organizations lost $50,000 to $1 million, compared to 8% of global respondents.
- Despite having more to lose, US respondents were generally less aware of the cost of cybercrime: 42% of US respondents were unaware of cybercrime's cost to their organizations, compared to 33% of global respondents.

*Cybercrime: Respondents believe the greatest threats to be theft or loss of IP, data or personal identity information.*

More organizations are collecting and maintaining personal and financial data on their customers (real and potential) and employees (past, present, and prospective). Data mining allows companies to gain better insight to their customer's spending habits in order to better inform marketing and other business strategies; however, data mining can pose a cybersecurity threat as it has been a prime target of hackers, as evidenced by multiple major personal data breaches recently in the headlines. Similarly, governments are engaging in both intra-border and cross-border cyber-surveillance programs. It's not surprising, therefore, that our respondents were most concerned about the risks of cybercrime directed at their data processing and storage systems: 86% of US respondents were concerned with cybercrime allowing intellectual property (IP) infringement, including theft of data; 83% were concerned with it leading to theft or loss of personal identity information (Figure 8). Given this trend along with a myriad of cyber incidents making the headlines, many governments are debating data-center localization strategies along with internet framework bills.

**Figure 8: Threats of cybercrime**



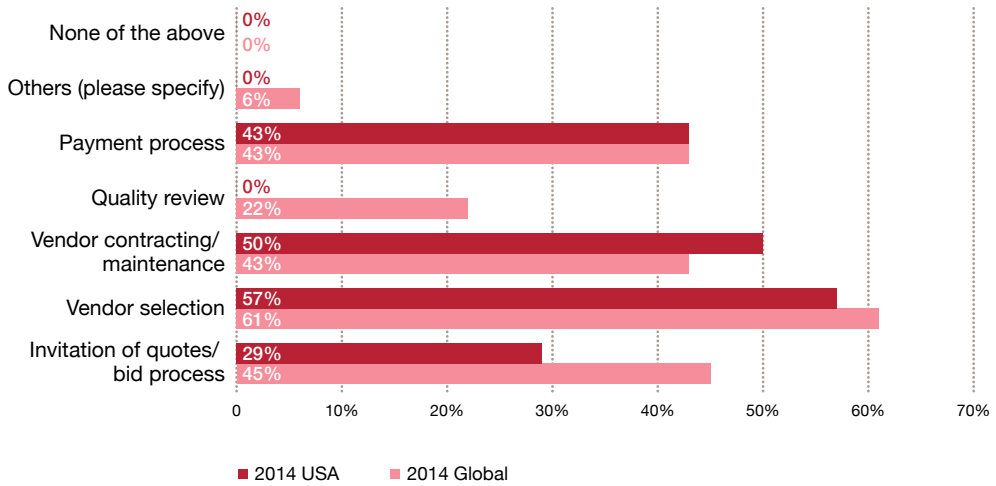

Today's circumstances and risks mean that both companies and governments should walk the fine line between enhanced security and protecting their own economic interests within the country. Critical cyber data is valuable and appealing to organized criminal enterprises for economic gain, to nation states for political espionage, to competitors for a business advantage, and to the rogue individual for purported social motivations. Social collaboration, expanding use of mobile devices, moving information storage to the cloud, digitizing sensitive information, moving to smart grid technologies, and embracing workforce mobility alternatives expose companies to fraud and also provide opportunities to strengthen their cybersecurity profiles. Thus, US corporations need to better leverage and implement the computational and analytical power of cybersecurity technologies to help combat the increasing global presence of cybercrime. US business leaders seem to understand the threat: our 2014 US CEO Survey shows that respondents were more concerned about cyber threats (including the lack of data security) and the speed of technological change than their global peers. Technological advances do not just present challenges- they can bring opportunities to better protect organizations from fraud. The upside is that technology may allow companies to better monitor their processes and implement real time controls. Automation, dashboard compliance strategies and improved inventory controls are all tools which companies can use to safeguard their assets, information and brands.

# Procurement fraud

As previously noted, for the first time we specifically asked respondents about procurement fraud—illegal conduct by which the offender gains an advantage, avoids an obligation, or causes damage to his organization. The results were stark—more than 1/4 of US respondents reported suffering from procurement fraud (27%), thus immediately placing it as the third most frequent type of fraud experienced by US organizations. The US results regarding procurement fraud generally mirrored the global average of 29% of organizations reporting they experienced procurement fraud within the past 24 months.

The high response-rate in connection with procurement fraud reflects the increasing interconnectedness of companies and ongoing trend toward outsourcing more aspects of their businesses. Organizations are especially vulnerable to procurement fraud when their purchasing, supply, and payment processes are susceptible to circumvention. In order to remain economically competitive, companies are often forced to lengthen their supply chain and rely heavily on the manufacturing of their goods outside of their own countries to capture the benefits of cheaper labor. This further complicates matters as the compliance function must now expand into sometimes unchartered foreign territories, thus enabling more opportunity for procurement fraud in various forms. Economic pressures set by headquarters can sometimes lead to unintended consequences of procurement fraud.

**Figure 9: Where did the procurement fraud primarily occur**



Most procurement fraud occurred at the vendor level, whereby key stakeholders in the procurement sometimes influence vendor selection or maintenance through bribery, rigged bids and kickback schemes. Procurement fraud during the payment process occurred in almost half of the instances, both in the US and globally (43% each). These statistics support the need for organizations to engage in robust vendor due diligence before pursuing outside business opportunities and partnerships. Clearly, companies that have existing robust global compliance programs that are scalable are better adapted to procuring goods and services in new territories. Often is the case that the companies that have not previously operated in foreign high risk territories fall victim to these schemes. But sometimes, compliance failures can lead to reputational damage when contracting with third parties that themselves commit procurement fraud, often unbeknownst to the company. These frauds can lead to reputational damage by association. Companies must remain vigilant regarding who they do business with, both on the inside and the outside.

## *Procurement fraud*

A few of the mechanisms by which procurement fraud can occur:

**Bid Rigging:** Fraud that impedes competitive bidding and disallows free and open competition in order to obtain the best goods and services at the lowest price.

**Kickbacks:** Any money, fee, commission, credit, gift, gratuity, any item of value, or compensation of any kind that is provided, directly or indirectly, in exchange for preferential treatment.

**Bribery:** The offering, giving, receiving, or soliciting of any thing of value to influence action as official or in discharge of legal or public duty.

**Collusion:** The secret combination, conspiracy, or concert of action between two or more persons for fraudulent or deceitful purpose.

Source: US General Services Administration Office of Inspector General

# Bribery and corruption is on the rebound

Although only 14% of US respondents suffered from bribery & corruption, organizations shouldn't downplay its risks, prevalence, or likelihood of occurrence. In our 2011 report, we anticipated that reported bribery & corruption would grow in the next few years in the wake of growing global regulation and increasing investigations uncovering more instances of corruption. In fact, 14% of organizations that experienced economic crime within the past 24 months identified bribery & corruption as a type of fraud suffered (doubling from 2011 level of 7%).

Bribery & corruption persists despite efforts of US organizations, law enforcement and regulators, and antifraud practitioners:

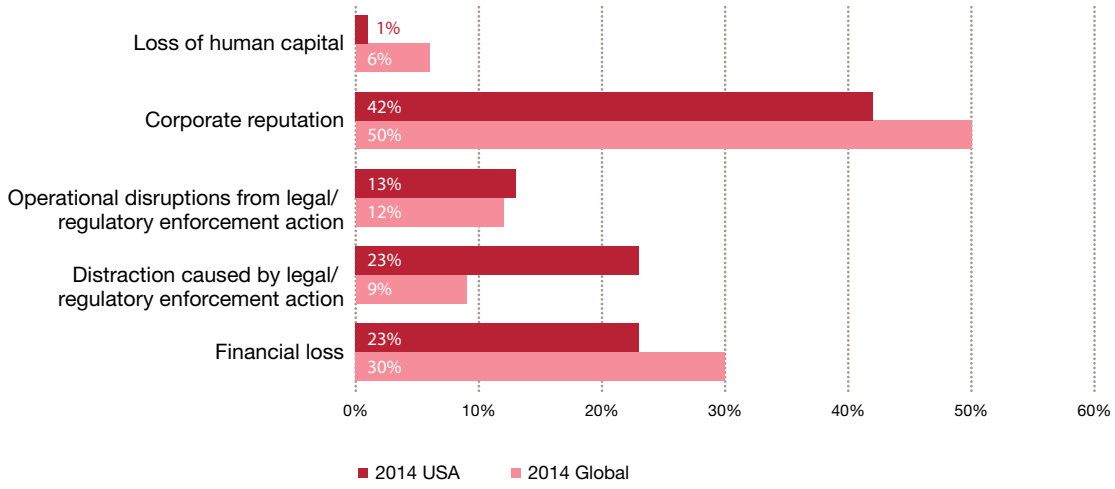
- US and global organizations experienced similar financial losses[3] through bribery & corruption: 4% of US organizations lost $1 million or more, compared to 5% of global organizations; and 28% of US organizations lost $50,000 to $1 million, compared to 27% of global respondents. US and global respondents were also similarly unaware of the cost of bribery & corruption on their organizations: 36% of US respondents were unaware of the cost, compared to 34% of global respondents.
- US respondents were more likely than their global counterparts to report that bribery & corruption presented a higher risk than money laundering and anti-competitive practices: 58% of US respondents indicated bribery & corruption posed the highest risk compared with 53% of global respondents; 26% of US respondents indicated anti-competitive practices posed the highest risk, compared with 21% of global respondents; and 10% of US respondents indicated money laundering posed the highest risk, compared with 22% of global respondents.
- Seventeen percent of both US and global respondents reported their organization had been asked to pay a bribe within the past 24 months; in addition, 15% of US respondents reported their organization lost an opportunity to a competitor they believed paid a bribe, compared with 22% of global respondents.

The risk of bribery & corruption grows as US organizations increasingly operate in and pursue opportunities in high-risk markets. Organizations are doing more business with and in territories that have cultures and histories relatively more tolerant of bribery & corruption, and officials who may be predisposed to expect payment of bribes. Bribery & corruption attacks the sales and marketing processes – and while the risk of bribery & corruption exists in most transactions, it is of particular concern when dealing with government officials in emerging markets.

As US organizations extract themselves from the economic crisis and vie for global competitive advantage and increased market share, sales and marketing staffs often experience increased pressure to deliver higher sales and drive profitability. This can make them particularly susceptible to offering bribes or kickbacks, or otherwise rigging the sales process. US organizations are taking note – 42% of respondents perceived that bribery & corruption had the most severe impact on corporate reputation, whereas 23% of respondents perceived it had the most severe impact on financial loss and distraction caused by legal/regulatory enforcement (Figure 10).

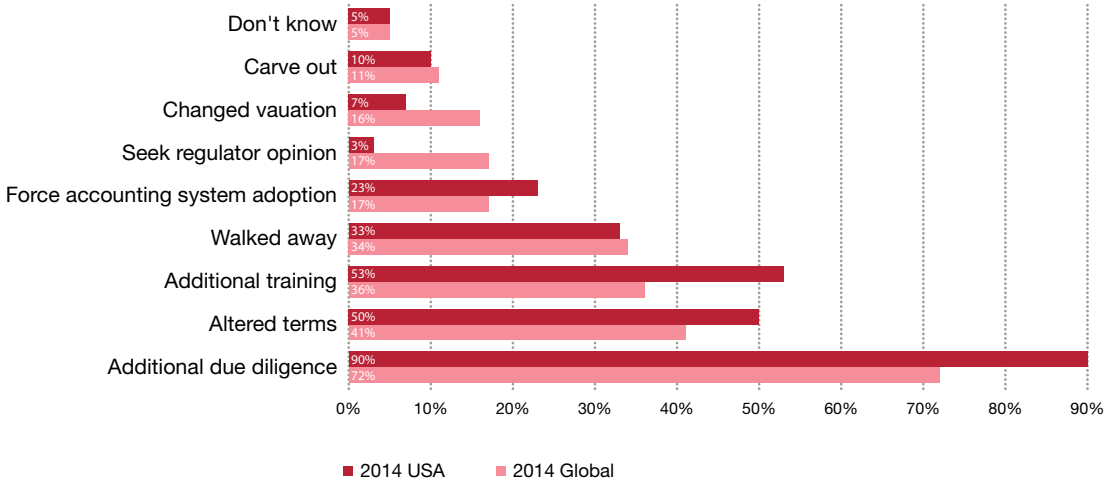
3 The GECS—US Supplement defined "financial loss" as including both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to "loss of business opportunity".

## Figure 10: Perceived threat of corruption




Bribery & corruption also impacts the way US organizations pursue business opportunities. In pursuing opportunities in high-risk markets, US organizations altered their business plans or strategies more often than the global average (46% US, 39% Global), and engaged in disparate methods of altering their business plans or strategies (Figure 11).

## Figure 11: Method of alteration of business plan or stratagy



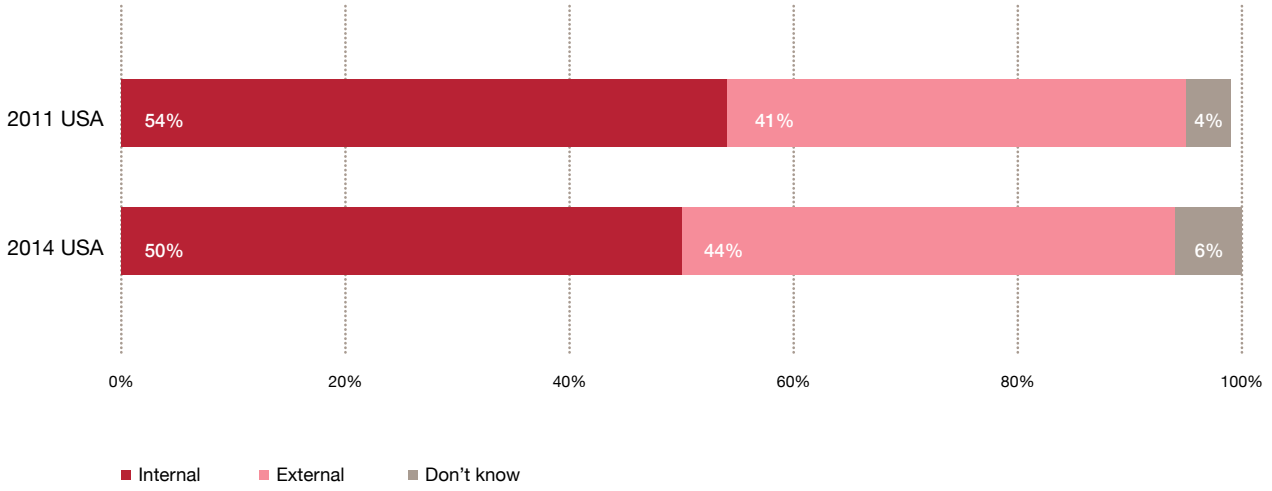
More than 1/3 of US organizations walked away from potential opportunities when doing business in high-risk markets, losing out on immeasurable benefits. The numbers don't necessarily need to be that high. Many situations can be remediated and a company with a strong, robust compliance system already in place will find it easier to understand the scope of potential corruption risk and navigate through it successfully. Luckily, US companies understand the benefit of having a robust compliance program and are outperforming their global peers (US 90% vs Global 72%) in terms of performing additional due diligence. By increasing additional due diligence in M&A deals, companies can promptly identify, understand and minimize the risks of a potential walk away late in the deal process which could prove costly. It appears that a benefit of US companies doing more global business, in riskier areas, than their global peers may cause them to adopt stronger compliance programs. This can be a competitive advantage that allows US companies to move more quickly and with better confidence in identifying business opportunities.

*The good news is U.S. organizations are out-pacing their global counterparts in performing additional due diligence.*

# Profile of the perp

Our survey results reflect that the "external enemy" is almost as likely as the "internal enemy" to commit fraud. Although US respondents reported that the most serious economic crime experienced within the past 24 months was more likely committed by an internal actor (50%) than an external actor (44%), the external fraudster is closing the gap (Figure 12).

**Figure 12: Main perpetrator of fraud**




This trend is consistent with more organizations pursuing and engaging in business opportunities in high-risk markets. Additionally, as organizations rely more on technology, they increasingly do business in a "borderless economy" where they are more susceptible to threats from all sides. The results are clear – while companies certainly should not lose sight of the internal perpetrator of fraud, they need to remain wary of the external perpetrator.

We asked respondents what factor they felt contributed most to the economic crimes committed by internal actors. Using the common "fraud triangle" model, respondents could choose from ability/opportunity, rationalization, and incentive/pressure to commit fraud. Organizations have limited ability to implement controls that reduce incentives and pressures to commit fraud or the perpetrators' ability to rationalize their actions since these factors are more likely "personal" to the

perpetrator. However, organizations do have the power to take away the opportunity and ability to commit fraud by introducing and implementing tougher internal controls. The responses reflect that organizations are losing out on their potential to effectively mitigate fraud committed by internal actors. At 73%, US respondents indicated that ability/opportunity far outpaced rationalization (at 15%) and incentive /pressure as a factor to commit fraud (at 12%)(Figure 13).

**Figure 13: Factors of fraud**

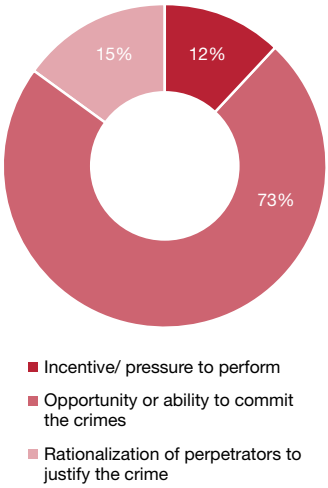
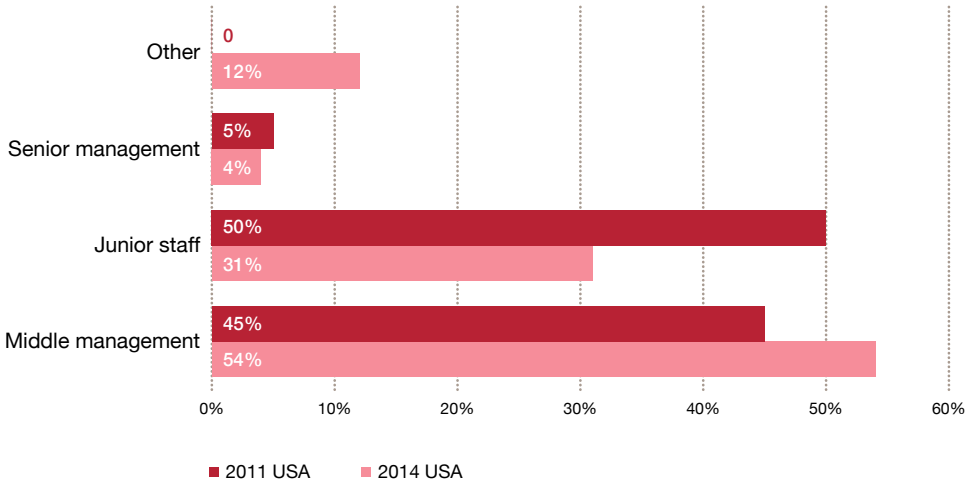



**Figure 14: Main perpetrator of internal fraud**



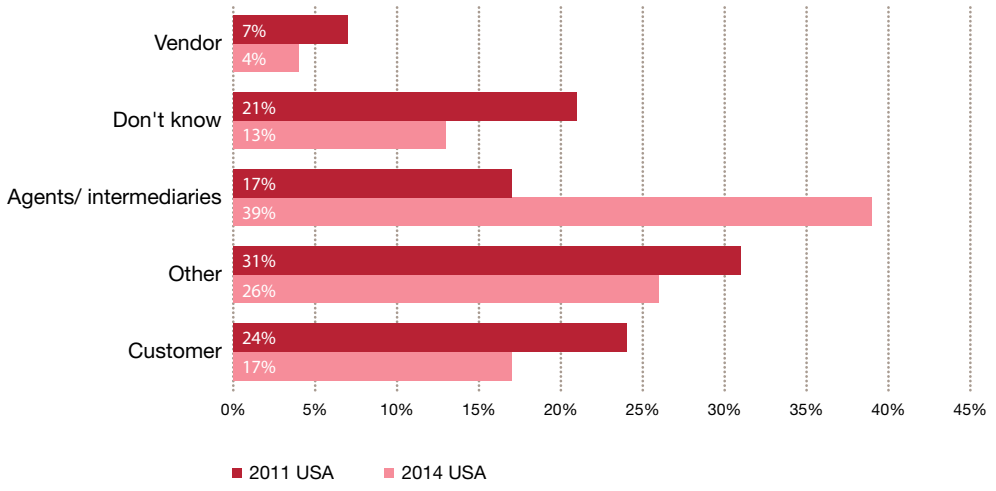

As shown in Figure 14, the US survey results also reflect a sharp rise in internal fraud committed by middle management (54%) compared to junior staff (31%). Economic downturns often disproportionately affect new employees and lower paid personnel, causing increased financial pressures which may contribute to the incentives to commit fraud; as we experience an economic recovery, the financial pressures on junior staff may decrease, and thus the incentives for fraud. Middle management overtaking junior staff as the main perpetrators of reported fraud may correlate with the respondents' indication that ability/opportunity is the leading factor contributing to economic crime.

## *Common profile characteristics of internal fraudsters*

Both US and global respondents most frequently identified the following characteristics of internal fraudsters:

- Gender: Male (77% US, 77% Global)
- Age: 31 to 40 years old (39% US, 40% Global)
- Length of Service: Employed between three and five years (27% US, 29% Global)
- Education: College degree (35% US, 35% Global)

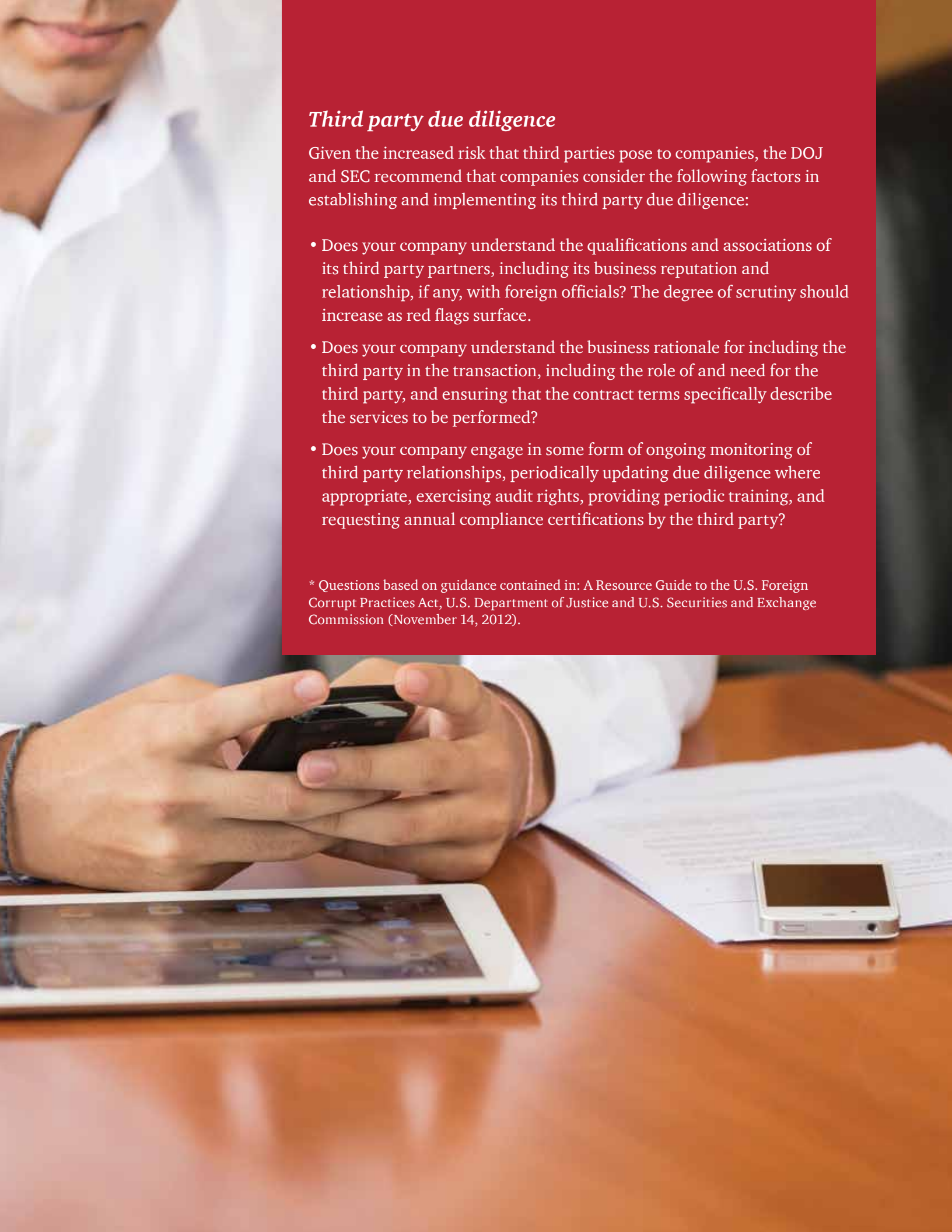
**Figure 15: Main perpetrator of external fraud**




Meanwhile, fraud committed by US senior management remained relatively low at 4% (up from 3% in 2011) compared to the global average where 20% of respondents cited senior management as the main perpetrator of internal fraud. This finding could be related to the relatively smaller sizes of global respondents' companies, which may have proportionately more senior staff than the larger US companies.

As previously noted, the external fraudster poses an increased threat to organizations, and companies are taking heed. Fewer respondents reported they didn't know the profile of the main perpetrator of external crime during the survey period (13%) compared to 2011 (21%). However, as revealed by Figure 15 , the profile of the external fraudster underwent a major shift since 2011, reflecting an ongoing need for organizations to understand with whom they do business.

Our US results show that respondents rated agents/intermediaries as the leading perpetrator of external fraud (39%) - and more than double the rate of the 2011 survey. This also differs from the global average which experienced the opposite – customers were most often reported as the main perpetrator of external fraud (33%), followed by others (24%) and agents/intermediaries (18%). Agents/intermediaries often function as extensions of the organization, acting as the company's "face" to end-customers and reflecting the organization's brand to the world; their misdeeds can be attributed to the company itself and cause serious damage to a company's reputation. In certain circumstances, legal liability may attach as well. Agents and intermediaries are likely to operate outside of companies' compliance environment and there is often limited transparency as to their interactions with government officials. The need to curb external fraud committed by agents/ intermediaries is critical with organizations increasingly concerned about the impact of fraud on their reputation.



## *Third party due diligence*

Given the increased risk that third parties pose to companies, the DOJ and SEC recommend that companies consider the following factors in establishing and implementing its third party due diligence:

- Does your company understand the qualifications and associations of its third party partners, including its business reputation and relationship, if any, with foreign officials? The degree of scrutiny should increase as red flags surface.
- Does your company understand the business rationale for including the third party in the transaction, including the role of and need for the third party, and ensuring that the contract terms specifically describe the services to be performed?
- Does your company engage in some form of ongoing monitoring of third party relationships, periodically updating due diligence where appropriate, exercising audit rights, providing periodic training, and requesting annual compliance certifications by the third party?

* Questions based on guidance contained in: A Resource Guide to the U.S. Foreign Corrupt Practices Act, U.S. Department of Justice and U.S. Securities and Exchange Commission (November 14, 2012).

# *Tough on the outside, but soft on the inside*

Although we continue to see that US respondents generally reported taking tougher action than did global peers against both internal and external fraudsters, there was a noticeable divergence in the US treatment of internal and external perpetrators. US companies took fewer actions against internal fraudsters during the survey period compared to 2011. The decreases were across all categories except civil action taken and warning/reprimand. In addition, 4% of US respondents reported taking no action against internal fraudsters during the survey period, whereas no respondents reported taking no action in 2011 (Figures 16 and 17).

**Figure 16: Action taken against internal perpetrator of fraud**

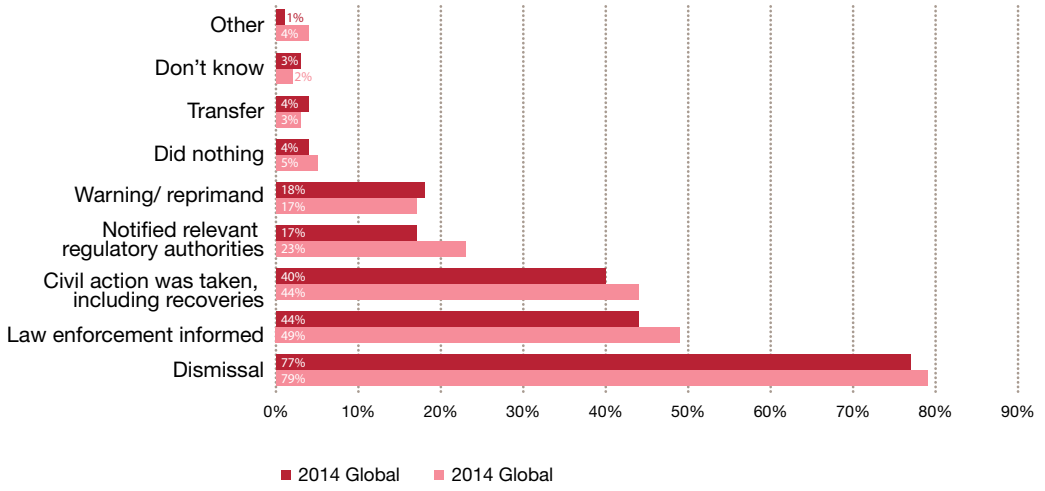
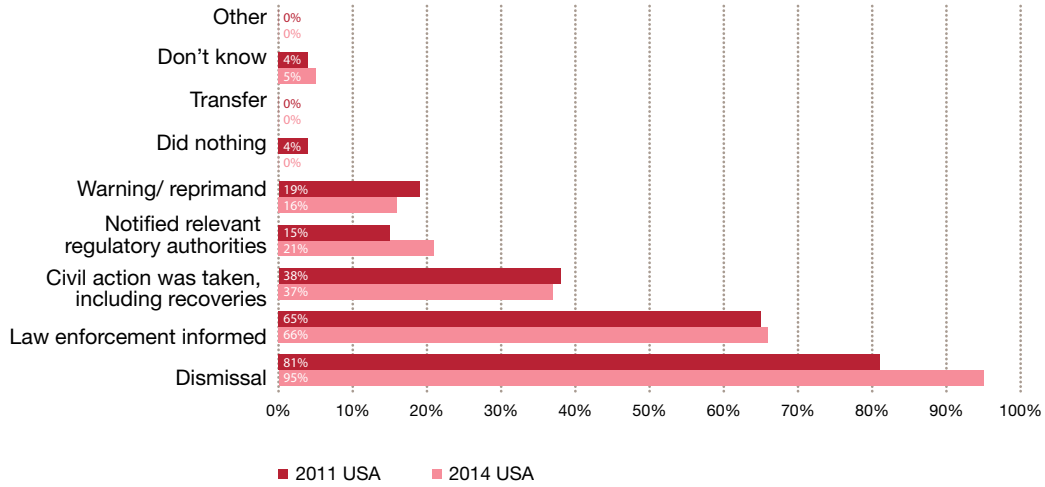



**Figure 17: Action taken against internal perpetrator of fraud**



Meanwhile, US companies took greater action against external fraudsters compared to 2011 with increases across all categories, and the number of respondents who reported taking no action against external fraudsters decreased to 4% from 7% in 2011. (Figures 18 and 19).

**Figure 18: Action taken against external perpetrator of fraud**

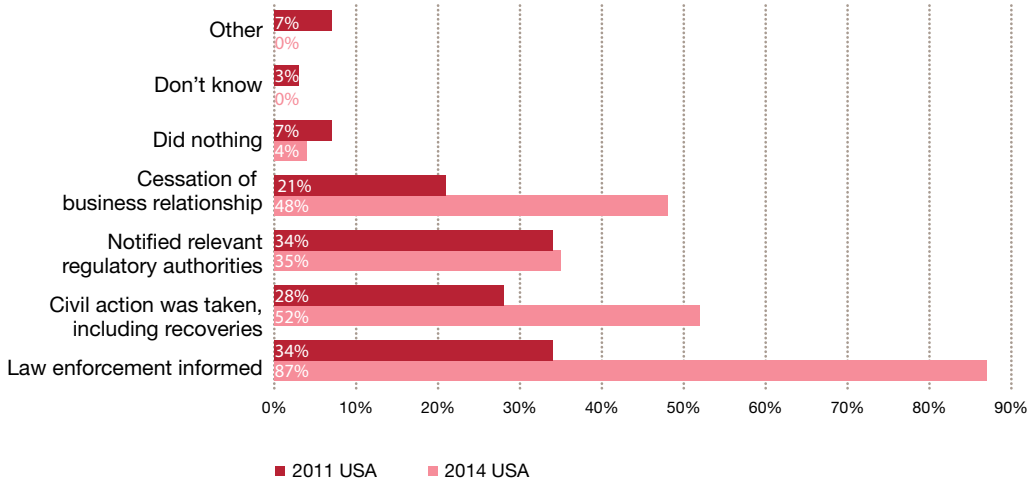
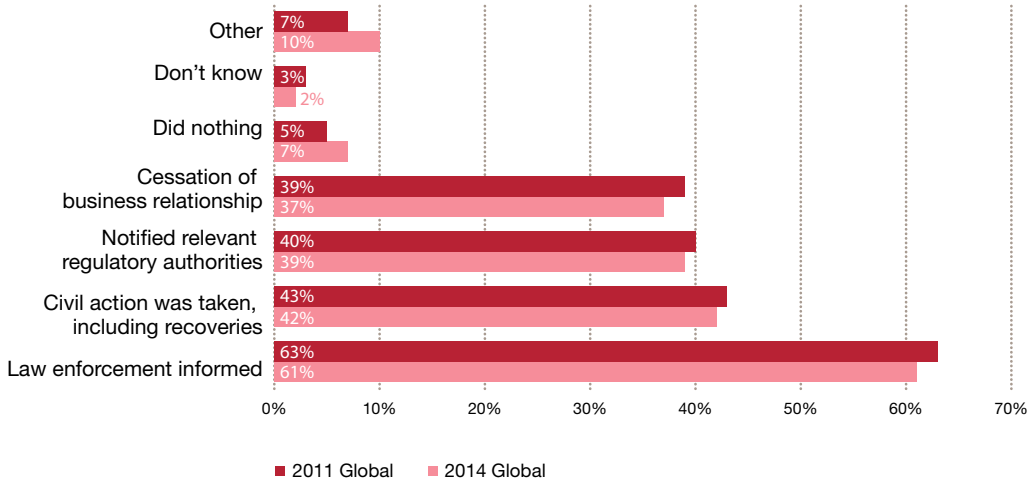



**Figure 19: Action taken against external perpetrator of fraud**



There are also notable differences when comparing equivalent actions taken by US companies against internal and external perpetrators. Organizations informed law enforcement about external perpetrators 22% more often than internal perpetrators (87% external, 65% internal), notified relevant regulatory agencies about external perpetrators 20% more often than internal perpetrators (35% external, 15% internal), and took civil actions, including recoveries, against external perpetrators 13% more often than against internal perpetrators (52% external, 39% internal). Organizations did report terminating the business relationship with internal perpetrators more often than with external perpetrators, with 81% of organizations terminating internal fraudsters compared with 48% of organizations ceasing business relationships with external fraudsters. However, the margin is narrowing from 2011, with dismissal of the internal perpetrator dropping 14% and cessation of the business relationship with the external perpetrator increasing 27% from 2011.

These trends are consistent with the corresponding decrease in frauds committed by internal actors and the increase in frauds committed by external actors to the extent that organizations may be increasingly focusing their efforts against the external fraudster. However, it will be interesting to see if the weaker actions taken against internal actors and stronger actions taken against external actors will lead to an increase in frauds perpetrated by internal fraudsters and decrease in frauds perpetrated by external fraudsters in our next survey.

Under relevant guidelines, both the SEC and DOJ place a high premium on self-reporting, along with cooperation and remedial efforts in determining the appropriate resolution of Foreign Corrupt Practices Act (FCPA) matters. They specifically consider whether the company made a timely and voluntary disclosure and the company's remedial actions, including efforts to improve existing compliance programs or appropriate disciplining of wrongdoers ("A company's remedial measures should be meaningful and illustrate its recognition of the seriousness of the misconduct, for example, by taking steps to implement the personnel, operational and organizational changes necessary to establish an awareness among employees that criminal conduct will not be tolerated.").[4] By implementing tougher actions against fraudsters, companies have the opportunity to mitigate the collateral effects of economic crime, and their criminal and civil liability.

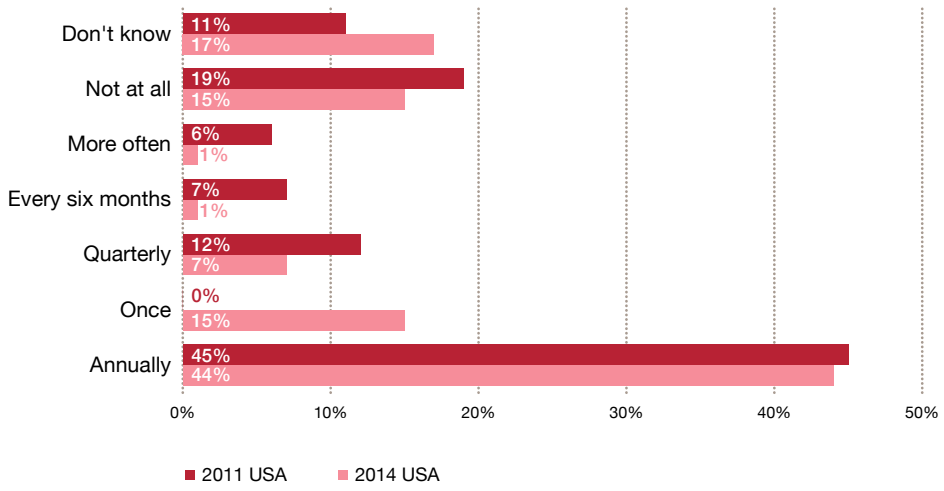
4 A Resource Guide to the U.S. Foreign Corrupt Practices Act, U.S. Department of Justice and U.S. Securities and Exchange Commission (November 14, 2012).

# Performing fraud triage

Our 2014 survey results reflect that US organizations took a less proactive approach to fraud prevention than in 2011, consistent with the uptick in economic crime experienced across most fraud categories since 2011.

Although more US organizations reported performing fraud risk assessments than in 2011 (during the survey period 15% of respondents reported performing "none at all" down from 19% in 2011), those organizations that did make fraud risk assessments performed them less frequently than reported in 2011.[5] Additionally, the number of respondents that were not aware of whether their organization performed fraud risk assessments increased to 17% from 11% in 2011 (Figure 20).

**Figure 20: Frequency of fraud risk assessments**




The frequency with which US respondents performed fraud risk assessments decreased across all categories since 2011. A little over a half of organizations performed fraud risk assessments annually or more often (53%), a significant drop from 2011 when 70% of organizations performed fraud risk assessments annually or more often. More US organizations reported performing at least one fraud risk assessment within the past 24 months (68%) compared with the global average (63%). However, of the organizations that did perform fraud risk assessments, the US trails the global average in performing the most frequent fraud risk assessments with 9% of US organizations performing fraud risk assessments at least once every six months compared with the global average of 19%.

5 In the 2014 survey, respondents were asked whether and how often they had performed a fraud risk assessment in the previous 24 months; in the 2011 survey, respondents were asked whether and how often they had performed a fraud risk assessment in the previous 12 months. Therefore, organizations responding to our survey that did perform fraud risk assessments once every two years, but not annually, would have selected performing "none at all" in 2011, whereas organizations responding to our 2014 survey would have had the option of selecting "once every two years."

Should your company prove to have potential exposure in a criminal or regulatory investigation, often the best thing it can do is uncover issues as early as possible and self-disclose. To do so, the proper trip-wires need to be in place, as well as a response strategy. The very first step is a comprehensive risk assessment

## *Drive the bus—don't fall under it*

Being aware of your risk environment is critical for maximizing the opportunity to prevent and detect economic crime. Identifying, investigating, and promptly disclosing misconduct or potential criminal activity could ensure that your company gets credit from regulators and prosecutors, and possibly a seat at the table instead of in the corner. The DOJ and SEC recommend that companies should consider the following factors in establishing and implementing compliance procedures:*

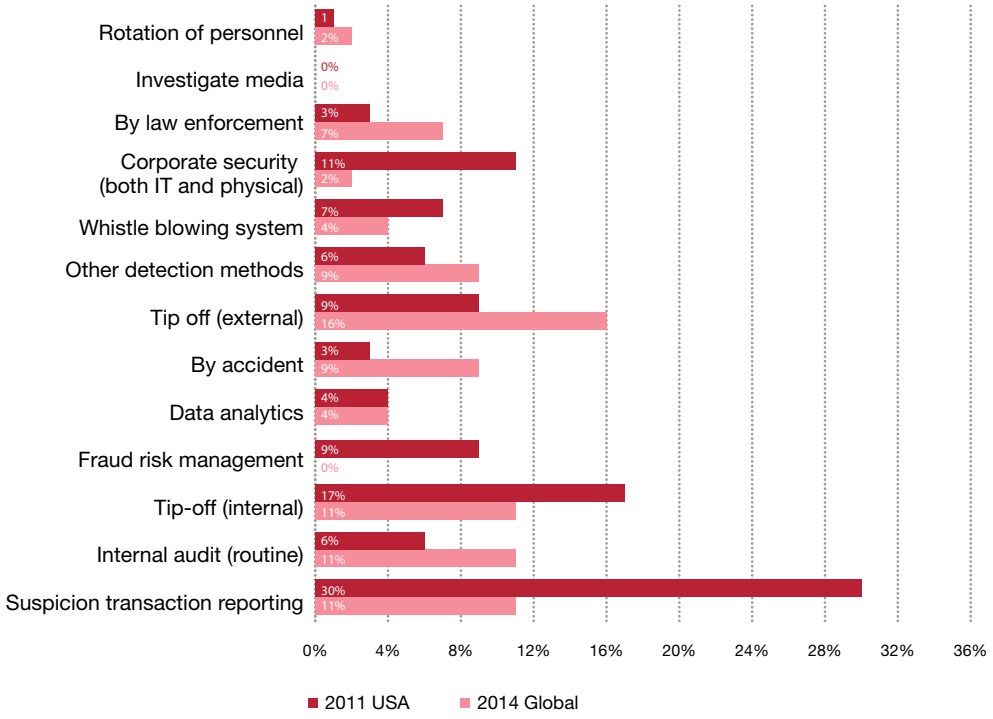
- Risks presented by the country and industry sector;
- The business opportunity;
- The potential business partners;
- The level of involvement with governments;
- The amount of government regulation and oversight; and
- The exposure to customs and immigration in conducting business affairs.

* Based on guidance contained in: A Resource Guide to the U.S. Foreign Corrupt Practices Act, U.S. Department of Justice and U.S. Securities and Exchange Commission (November 14, 2012).

# The best defense is a good offense

In addition to asking companies about their fraud prevention measures, we asked organizations how they initially detected the most serious economic crime their organization experienced in the last 24 months (Figure 21). Consistent with the decrease in frequency of organizations performing fraud risk assessments, frauds detected by external measures[6] or by accident (32%) more than doubled from 2011 (15%).

**Figure 21: Method by which most serious fraud was initially detected**




The shift away from internal detection measures to external ones should be a wake-up call – costs can be staggering when frauds are increasingly detected by external methods rather than internal ones. The sooner organizations identify fraud or its susceptibility to fraud, the more opportunities they have to mitigate its potential consequences. The earlier such activity can be detected, the more opportunity there is to control the course of events through internal investigation and, if necessary, self-disclosure to authorities. When such activity is discovered only when there is a "knock at the door" by regulators or prosecutors, one of the best opportunities to gain meaningful consideration in the face of an investigation is lost.

6 External measures are defined as those identified by "external tip-offs," "law enforcement" or "investigamedia."

| DOJ/SEC Hallmarks of effective compliance programs* | Take away questions |
|---|---|
| Commitment from Senior Management and a Clearly Articulated Policy Against Corruption: | Does senior management have clearly articulated company standards that are communicated in unambiguous terms, adhered to scrupulously and disseminated throughout the organization? |
| Code of Conduct and Compliance Policies and Procedures: | Does senior management periodically review and update its code of conduct to ensure that it remains current and effective, including: outlining responsibilities for compliance within the company; detailing proper internal controls, due diligence practices, and documentation policies; and setting forth disciplinary procedures? |
| Code of Conduct and Compliance Policies and Procedures: | Has your company assigned responsibility for oversight and implementation of its compliance program to one or more specific senior executives who have the proper authority, adequate autonomy from management, and sufficient resources to ensure your company's compliance program is implemented effectively? |
| Oversight, Autonomy and Resources: | Has your company, in good faith, implemented a comprehensive, risk-based compliance program that is tailored to its industry, size, nature of transaction, and method and amount of third-party compensation? |
| Risk Assessment: | Does your company provide periodic training and certification for all directors, officers, employees, and, where appropriate, agents and business partners, consistent with the size and sophistication of your company? |
| Training and Continuing Advice: | Does your company provide guidance and advice on complying with your company's ethics and compliance program, including when such advice is needed urgently? |
| Incentives and Disciplinary Measures: | Does your company have appropriate and clear disciplinary procedures that are applied reliably and are commensurate with the violation and applied fairly and consistently across the organization? |
| Third-Party Due Diligence and Payments: | Does your company engage in risk-based due diligence on third parties, inform third parties of your company's compliance program and commitment to ethical and lawful business practices, and where appropriate, seek assurances from third parties, through certifications or otherwise, of reciprocal commitments? |
| Continuous Improvement—Periodic Testing and Review: | Does your company regularly review and improve its compliance programs in light of any changes to the business, the environments in which it operates, the nature of its customers and the laws that govern its actions and standards of the industry? |
| Mergers & Acquisitions—Pre-Acquisition Due Diligence and Post Acquisition Integration: | Does your company conduct effective due diligence on its acquisition targets? Does your company ensure the acquired company promptly incorporated its internal controls and compliance programs, trained new employees, re-evaluated third parties under company standards and, where appropriate, conducted due diligence on new business? |

*Source: A Resource Guide to the US Foreign Corrupt Practices Act, US Department of Justice and US Securities and Exchange Commission (November 14, 2012)

US companies reported that fraud was initially detected most often through external tip-offs (16%), taking the top spot from suspicious transaction reporting which plummeted by almost two thirds (30% vs. 11%) since our last survey. However, viewed together with the 2009 survey results, it appears as if this could be a reversion to the mean and that the 2011 results represented a "spike". This may have been due, in part, to an increase in historical fraudulent activity being uncovered and reported through "look backs" in the mortgage and financial industries as a result of the economic crisis.

Interestingly, despite the decrease in frequency of fraud risk assessments performed by US organizations discussed above, the statistics reflect that performing fraud risk assessments succeeds in preventing and detecting fraud – frauds initially detected by fraud risk management more than doubled to 9%, up from 4% in 2011. When regulators and prosecutors decide whether and to what extent to investigate and pursue actions against organizations for fraud, they consider the existence and comprehensiveness of the organizations' internal controls and whether the fraud was self-reported or discovered outside of corporate governance efforts. In addition, the sanctions, penalties, judgments and government-mandated corporate compliance programs imposed on organizations as a result of a fraud scandal add substantial, and avoidable, costs to organizations. Since 2011, there has been an observed inverse relationship between whistle-blowers and law enforcement; fraud being reported by whistle-blowing declined whereas fraud being reported to law enforcement has increased. This could be due to whistleblowers feeling incentivised through Dodd Frank to report directly to law enforcement or regulators rather than attempting to report internally.

## *Blowing the whistle on fraud*

In the wake of Dodd-Frank implementation, we added questions about organizations' whistleblower mechanisms:

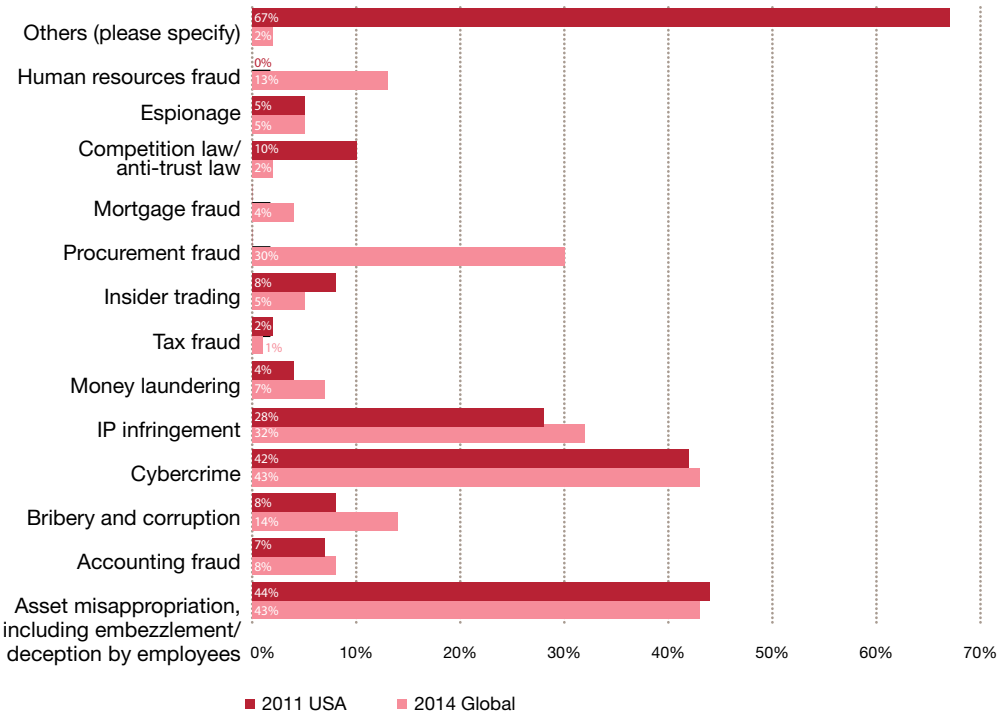
- 86% of respondents indicated their organization had a whistleblower mechanism
- Regarding frequency of use within the past 24 months, organizations reported using their whistleblower mechanism:
  - More than 100 times: 12%
  - 11-100 times: 21%
  - 1-10 times: 24%
  - Zero times: 9%
  - Don't know: 34%
- Regarding effectiveness in preventing and detecting economic crime, organizations evaluated their whistleblower mechanisms as:
  - Effective: 83%
  - Not effective: 5%
  - Don't know: 12%

# All eyes on the horizon

US respondents think it's more likely they will experience dangers from fraud across almost all categories of economic crime than they did in 2011 (Figure 22). This trend is likely driven by organizations' actual experiences with fraud over the past 24 months, as organizations became more aware of and increasingly impacted by the significant financial cost and collateral damage associated with economic crime.

Respondents are more worried about bribery & corruption than they were in 2011. This may be due in part to the continued robust enforcement of the FCPA as well as the first cases stemming from the UK Bribery Act. In addition to these laws, other countries such as Spain, India, and Brazil have adopted new anti-corruption measures.

**Figure 22: Likely frauds to be suffered**

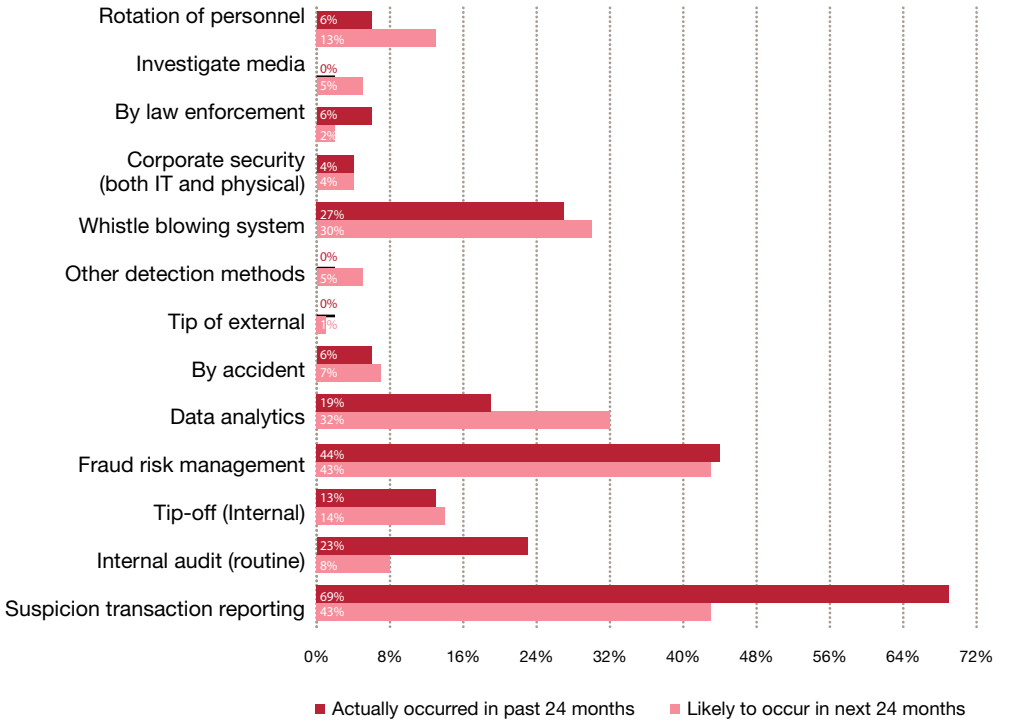


Comparing US respondents' experiences with fraud with their projections for the future (Figure 23), a few striking paradoxes emerge.

First, although 69% of respondents experienced asset misappropriation in the survey period, only 43% predict that it is likely to affect their companies in the next two years. Also, while 23% reported experiencing accounting fraud in the survey period, only 8% predict that it may strike over the next two years. These differences could reflect the confidence some respondents have in new anti-fraud controls and policies their organizations adopted after being victimized.

Second, over twice as many respondents expect to experience human resources fraud in the next two years as experienced it in the survey period. Similarly, 32% expect to experience IP infringement even though only 19% experienced it in the survey period. This heightened awareness may reflect a growing concern that such crime is on the rise, or that the respondents' organizations may not be equipped with adequate controls to protect against such threats.

**Figure 23: Comparison of types of fraud actually suffered to types of fraud likely to be suffered**



With more opportunities come more risks; no longer can organizations focus their fraud prevention and detection strategies on only a few types of fraud, a certain profile of fraudster, or certain perceived threats. They must be prepared to cast a wider net, for the threats associated with fraud are growing.

Certainly, the interplay among enhanced global regulatory scrutiny, more skilled and technologically-sophisticated fraudsters, and the emergence of an increasingly borderless business environment presents ongoing challenges to organizations as they combat fraud during the economic recovery period. However, organizations simply cannot afford to take a passive or reactive approach toward fraud. In addition to the initial financial impact, our survey respondents were acutely attuned to the collateral and potentially irreparable damage fraud causes to their organization's brand and reputation among its present and prospective customers, employees, and business partners. Ideally, this heightened awareness will prompt organizations to make the up-front investment in fraud prevention and detection methods, which continuously prove less costly than implementing damage control measures after the fact. By taking a pre-emptive and proactive approach to fraud, organizations can gain a competitive advantage and set themselves up for sustained success.

# Acknowledgments

*A core team at PwC worked diligently on the US Supplement of the 2014 Global Survey. We'd like to acknowledge the contributions of:*

**Didier Lavion**
Principal
didier.lavion@us.pwc.com
(646) 471-8440

**Steven Skalak**
Partner
steven.skalak@us.pwc.com
(646) 471-5950

**Sean Joyce**
Principal
sean.joyce@us.pwc.com
(703) 918-3528

**Peter Zanolin**
Manager
peter.l.zanolin@us.pwc.com
(646) 471-4815

**Lauren Bush**
Experienced Associate
lauren.r.bush@us.pwc.com
(646) 471-1903

**Paul Charbonnet**
Experienced Associate
paul.d.charbonnet@us.pwc.com
(646) 471-9879

## *Forensic Leadership*

**Chris Barbee**
Global Advisory Forensics Leader
chris.barbee@us.pwc.com
(267) 330-3020

**Erik Skramstad**
U.S. Advisory Forensics Leader
erik.skramstad@us.pwc.com
(617) 530-6156

# Contacts

## *PwC Forensic Services*


### Atlanta

**Robert Gallagher**
robert.e.gallagher@us.pwc.com
(678) 419-4314

### Boston

**Chris Barry**
christopher.c.barry@us.pwc.com
(617) 530-6304

**John May**
john.m.may@us.pwc.com
(617)-530-5340

### Florida

**Mona Clayton**
mona.m.clayton@us.pwc.com
(305)-347-3510

### Chicago

**James Bucrek**
james.bucrek@us.pwc.com
(312) 298-3907

**Ted Hawkins**
ted.hawkins@us.pwc.com
(312) 298-3181

**Kevin Kreb**
kevin.kreb@us.pwc.com
(312)298 -2587

**Ryan Murphy**
ryan.murphy@us.pwc.com
(312) 298-3109

**Kris Swanson**
kris.swanson@us.pwc.com
(773) 551-0293

### Dallas

**Todd Ranta**
todd.c.ranta@us.pwc.com
(214) 754-4513

**Charles Reddin**
charles.reddin@us.pwc.com
(214) 754-5173

### Houston

**Karyl Van Tassel**
karyl.van.tassel@us.pwc.com
(713) 356-4242

**Brian Wycliff**
brian.wycliff@us.pwc.com
(713) 356-5499

### Los Angeles

**Alexandre Blanc**
alexander.blanc@us.pwc.com
(213) 217-3384

**Owen Murray**
owen.w.murray@us.pwc.com
(213) 356-6097

### New York

**Manny Alas**
manny.a.alas@us.pwc.com
(646) 471-3242

**Frank Badalamenti**
frank.badalamenti@us.pwc.com
(646) 471-1460

**Kevin Bandoian**
kevin.bandoian@us.pwc.com
(646) 471-2058

**Emanuel Bulone**
emanuel.bulone@us.pwc.com

**Brian Castelli**
brian.castelli@us.pwc.com
(646) 471-2563

**Dyan Decker**
dyan.a.decker@us.pwc.com
(646) 313-3636

**Patricia Etzold**
patricia.a.etzold@us.pwc.com
(646) 471-3691

**Brian Fox**
brian.t.fox@us.pwc.com
(646) 471- 3398

**Joe Guistino**
joe.guistino@us.pwc.com
(646) 471-8523

**Charles Hacker**
charles.r.hacker@us.pwc.com
(646) 471-8580

**David Jansen**
david.jansen@us.pwc.com
(646) 471-8329

**Philip Koos**
philip.koos@us.pwc.com
(646) 471-2454

**Grace Lamont**
grace.lamont@us.pwc.com
(646) 471-7449

**Didier Lavion**
didier.lavion@us.pwc.com
(646) 471-8440

**Ted Martens**
ted.martens@us.pwc.com
(646) 471-7340

**Dana McIlwain**
dana.mcilwain@us.pwc.com

**SandraMaria Parrado**
sandra.maria.t.parrado@us.pwc.com
(646) 471-5552

**Matthew Shelhorse**
matthew.j.shelhorse@us.pwc.com
(646) 471-5749

**Steven Skalak**
steven.skalak@us.pwc.com
(646) 471-5950

**Darren Tapp**
darren.j.tapp
(646) 471-1384

**Philip Upton**
philip.upton@us.pwc.com
(646) 471-7508

## Orange County

**Jeff Leedom**
jeff.leedom@us.pwc.com
(949) 437-5774

## Philadelphia Metro

**Chris Barbee**
chris.barbee@us.pwc.com
(267)-330-3020

**Mark Gerber**
mark.gerber@us.pwc.com
(267) 440-1888

## San Francisco

**Jane Allen**
jane.allen@us.pwc.com
(415) 498-5656

**James Meehan**
james.r.meehan@us.pwc.com
(415) 498-6531

**Kristin Rivera**
kristin.d.rivera@us.pwc.com
(415) 498-6566

**Bruce Vanderbush**
bruce.a.vanderbush@us.pwc.com
(415) 498-6595

**Kim Wiatrak**
kim.wiatrak@us.pwc.com
(415) 498-6528

## San Jose

**David Marston**
david.l.marston@us.pwc.com
(408) 817-3803

## Washington Metro

**Charles Beard**
charles.e.beard@us.pwc.com
(703) 918-3318

**David Burg**
david.b.burg@us.pwc.com
(703) 918-1067

**Mike Hamilton**
mike.hamilton@us.pwc.com
(202) 756-1778

**Sean Joyce**
sean.joyce@us.pwc.com
(703) 918-3528

**Neil Keenan**
neil.keenan@us.pwc.com
(703) 918-1216

**Frederic Miller**
frederic.r.miller@us.pwc.com
(703) 918-1564

**Shane Sims**
shane.sims@us.pwc.com
(703) 918-6219

**Sanjay Subramanian**
sanjay.subramanian@us.pwc.com
(703) 918-1509

**James Thomas**
james.w.thomas@us.pwc.com
(703) 918-3050

**Al Vondra**
al.vondra@us.pwc.com
(703) 918-1534

**Glenn Ware**
glenn.ware@us.pwc.com
(703) 918-1555

*www.pwc.com/us/crimesurvey*

This publication is printed on McCoy Silk. It is a Forest Stewardship Council™ (FSC®) certified stock containing 10% post consumer waste (PCW) fiber and manufactured with 100% Green-e certified renewable energy

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2014 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.

LA-14-0127 US Global Economic Crime Survey