Contents

Economic crime: A threat to business globally

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

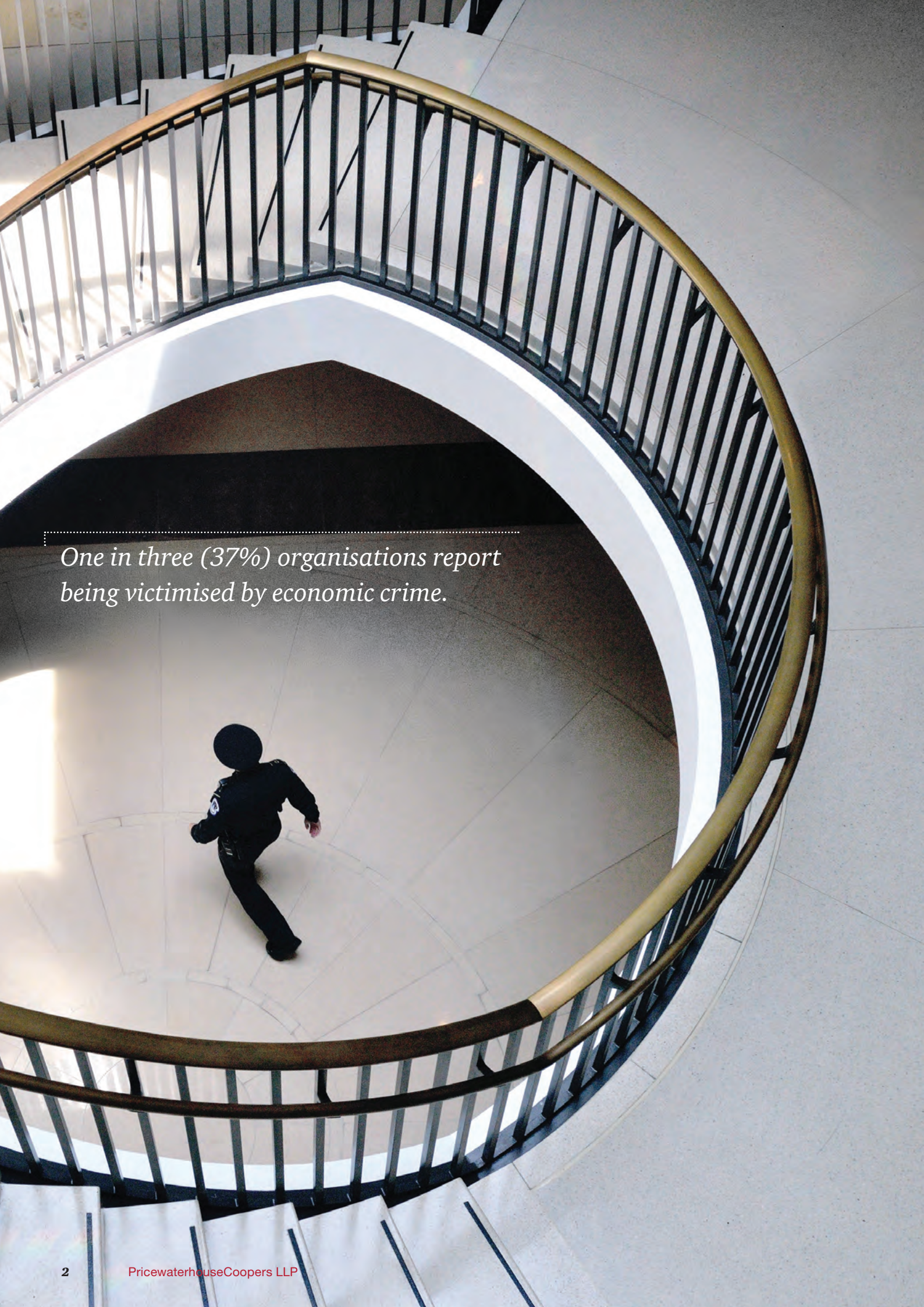
53%
More than half of CEOs surveyed reported being concerned about bribery and corruption.

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

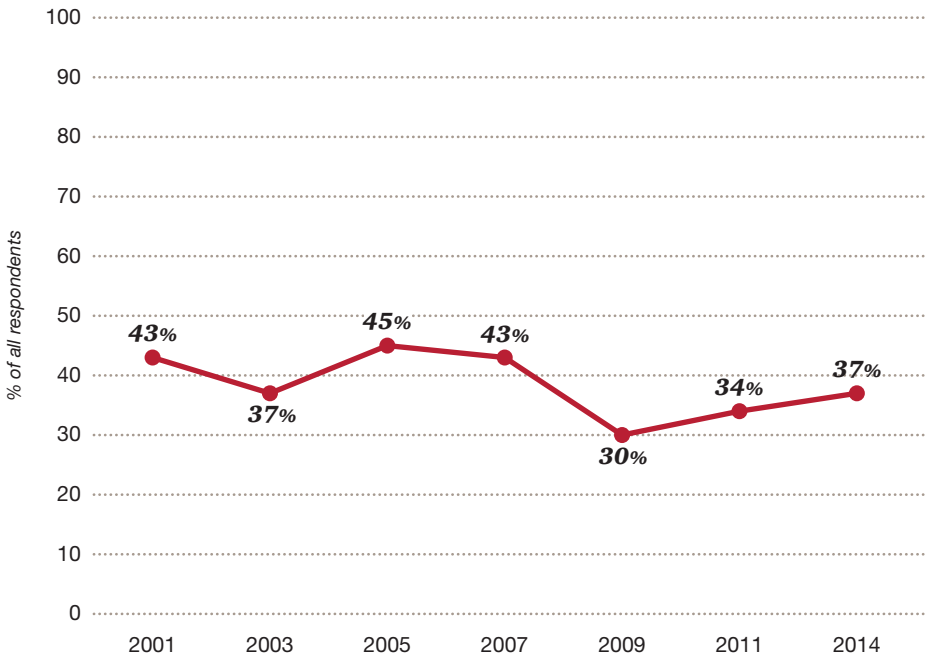
Our 2014 survey respondents included 5,128 representatives from over 95 countries around the world. More than half (54%) of our respondents were employed by organisations with more than 1,000 employees, and over one third (35%) of the survey population represented publicly traded companies.

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%**

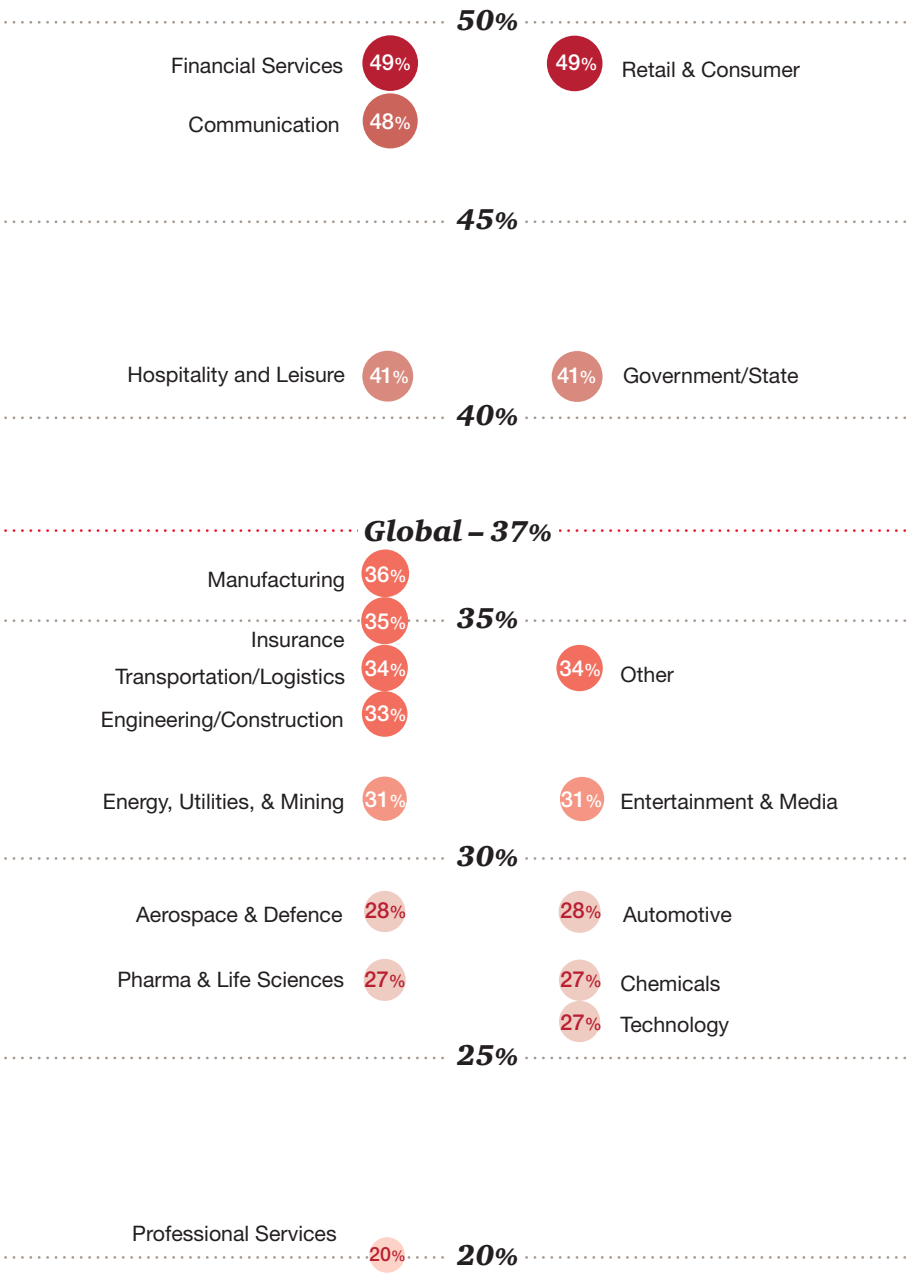
**Emerging Eight include Brazil, China, India, Indonesia, Mexico, Russia, Turkey, and South Africa*

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

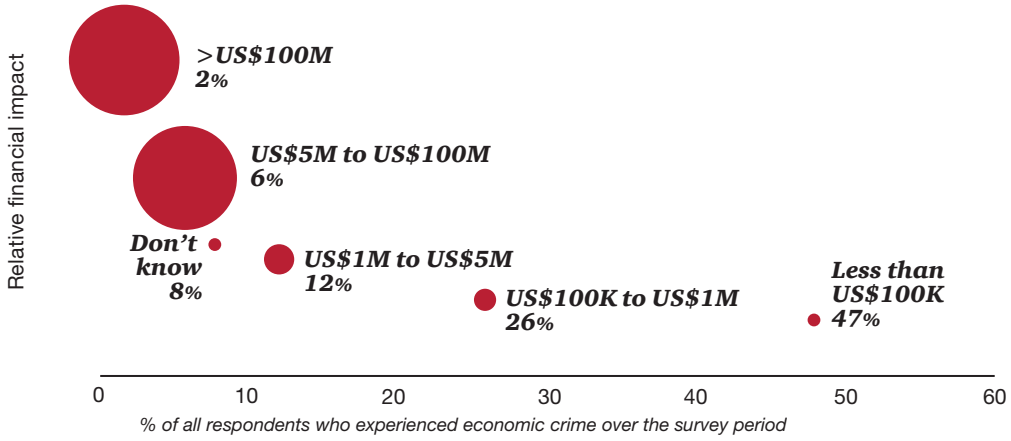
Organisations often don't grasp the true financial impact of an economic crime until after it has happened—sometimes well after. As in previous years, our survey underscores that the cost of fraud—both in financial and non-financial terms—is significant.

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.

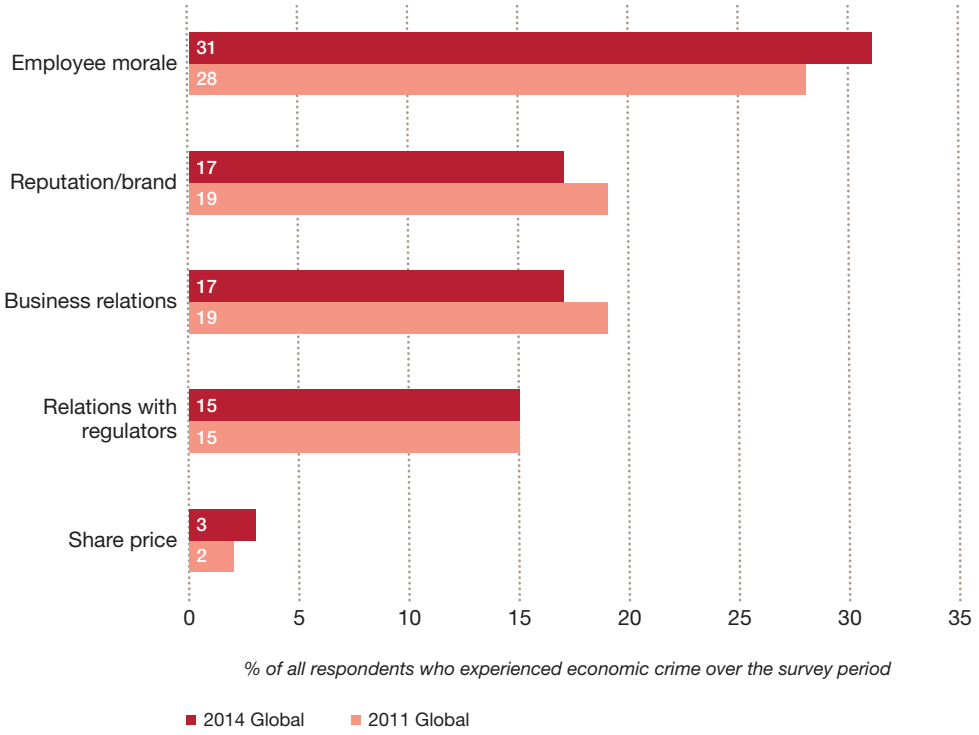
Figure 6: Relative financial impact of economic crime on organisations



Collateral damage: Hard to quantify, hard to ignore

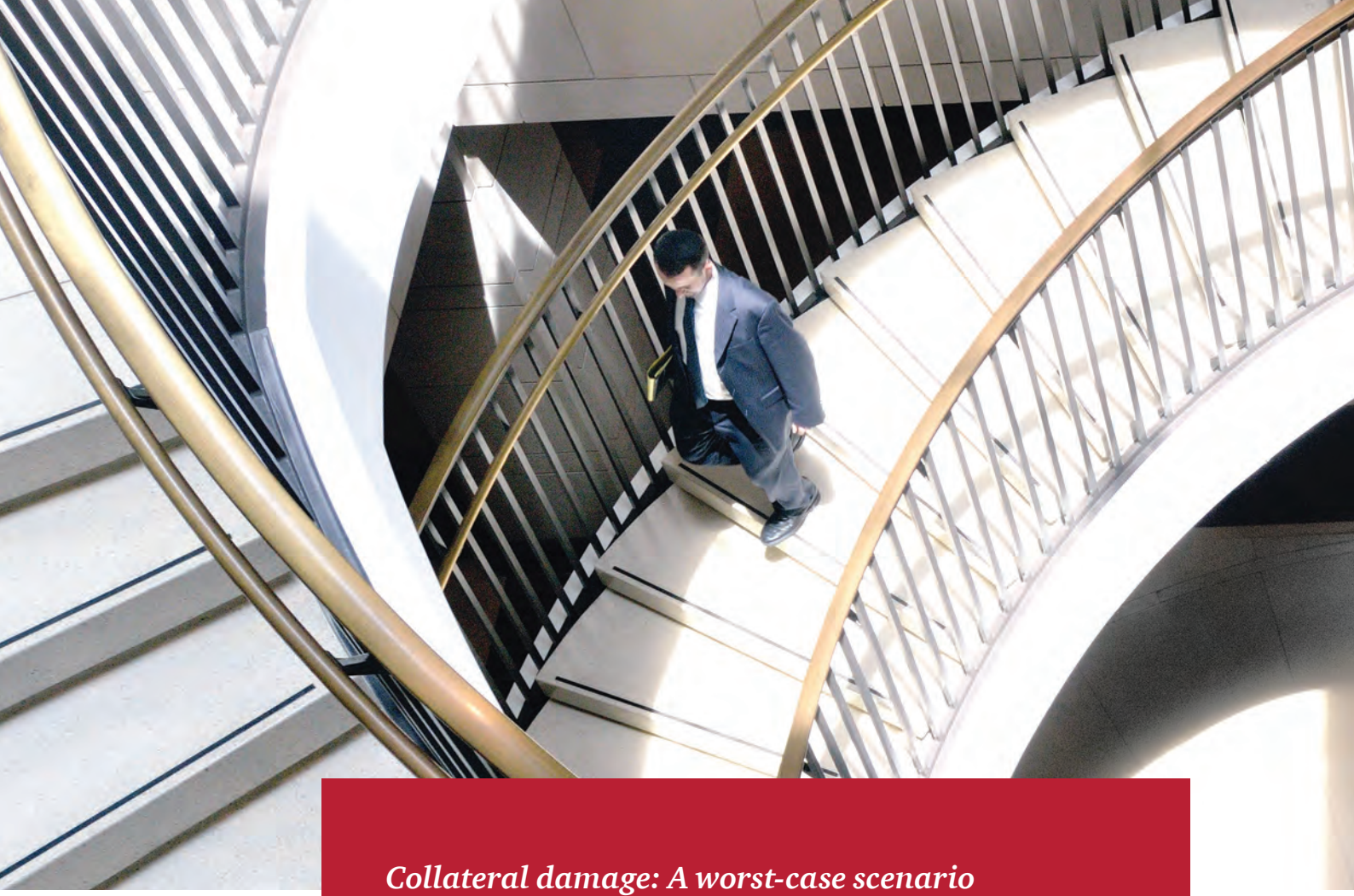
Economic loss is not the only concern that companies face when combating fraud. Our respondents pointed at damage to employee morale, corporate and brand reputation, and business relations as some of the most severe non-financial impacts of economic crime.

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.

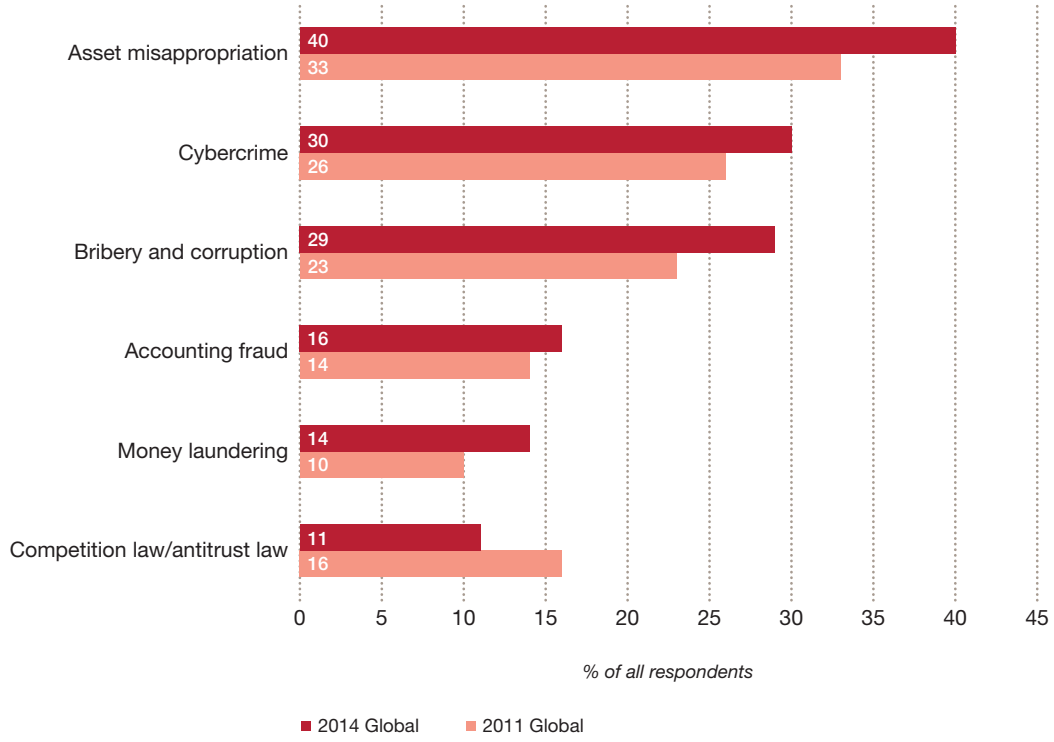
Starting with a report of a single event such as insider trading or financial statement fraud, incidents may appear compartmentalised, involving only one account, division, or customer. Still, in a competitive marketplace, there are often few reasons for customers, counterparties or partners to maintain 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

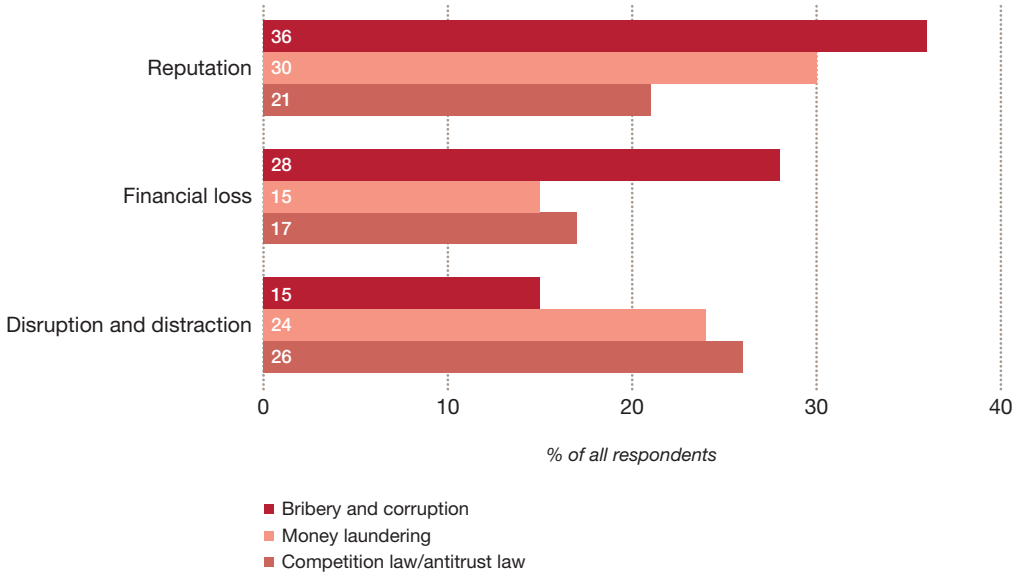
Some types of economic crimes attract significantly more attention from government enforcement agencies than others. For this reason we have decided to dedicate a section of our analysis to an important subset of economic crime—bribery and corruption, money laundering, and anticompetitive behaviour.

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

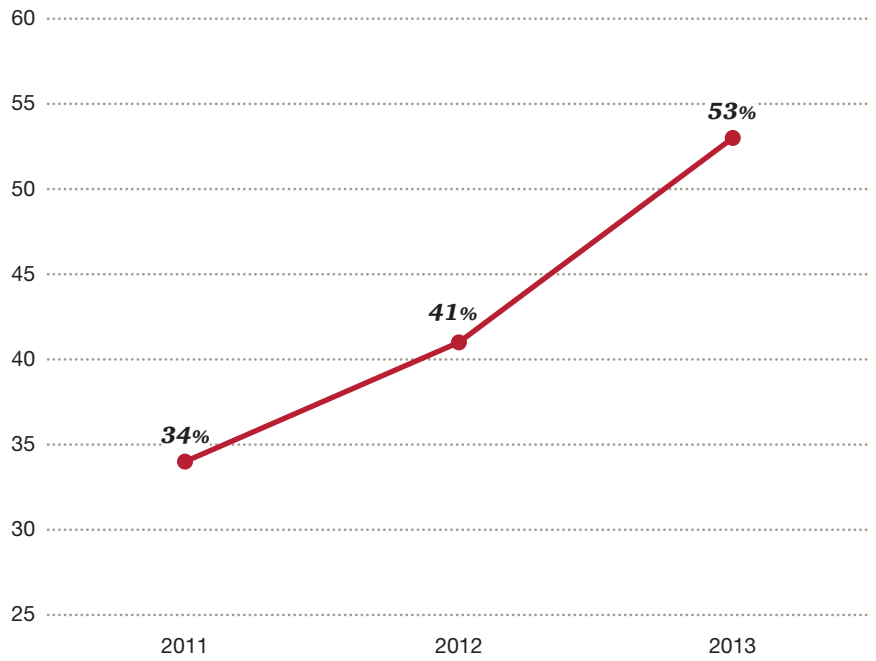


Bribery and corruption: The C-Suite gets the message

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.

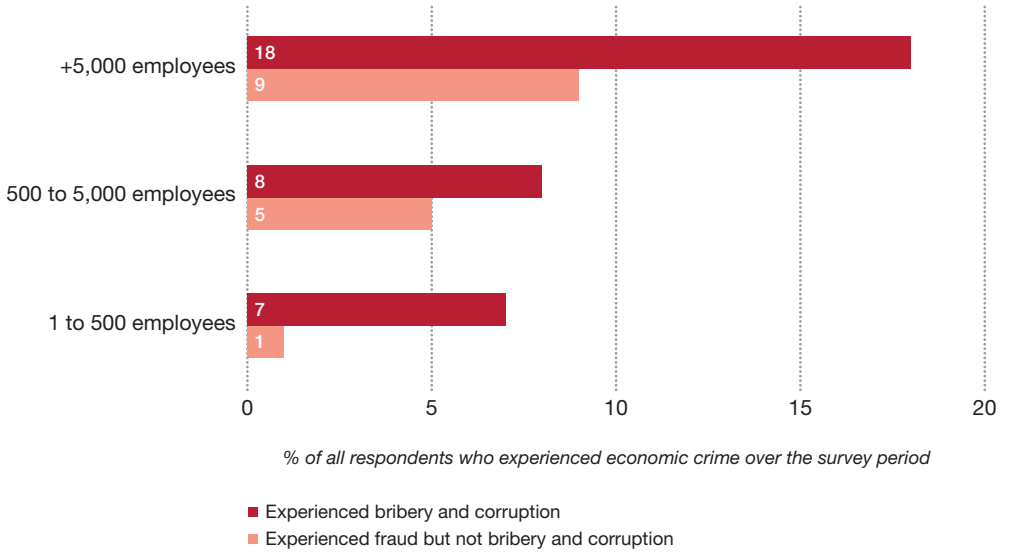
If the territory has a culture that is relatively permissive to bribery and corruption, some of these officials may be predisposed to expect or at least be open to bribes. This exerts pressure on sales and marketing staff, who have been tasked by leadership with bringing a new product to a growing market—pressure 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

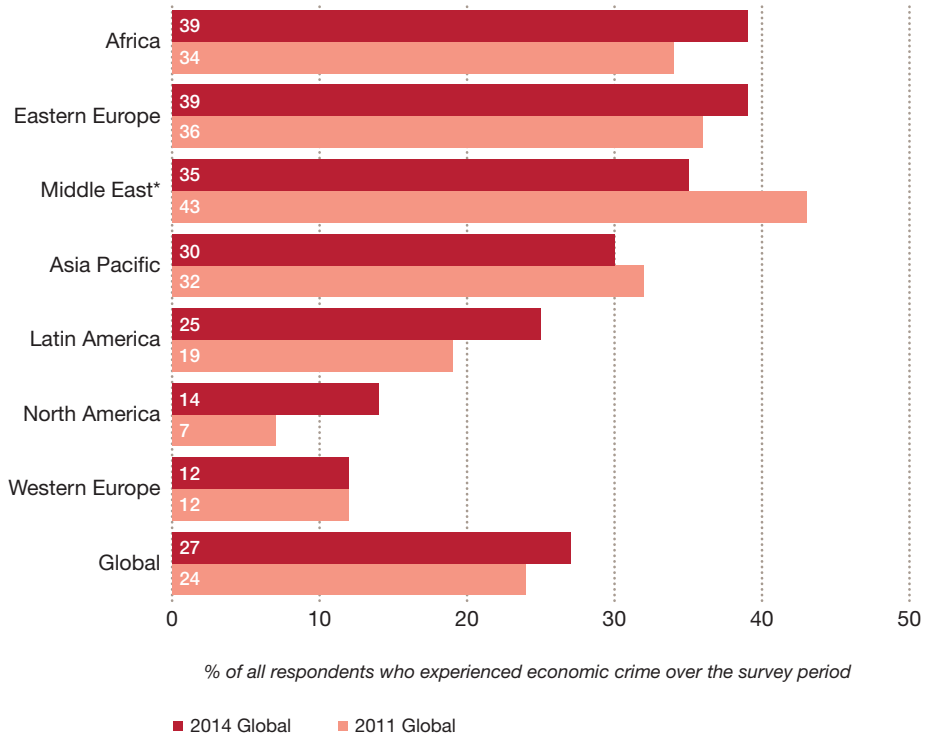
The global economy is generally on the rebound, potentially reinvigorating organisations' appetite for expansion and risk. Our survey results confirm that a large number of organisations operate in territories identified as posing a high corruption risk (50%) and/or plan to pursue opportunities in such 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.

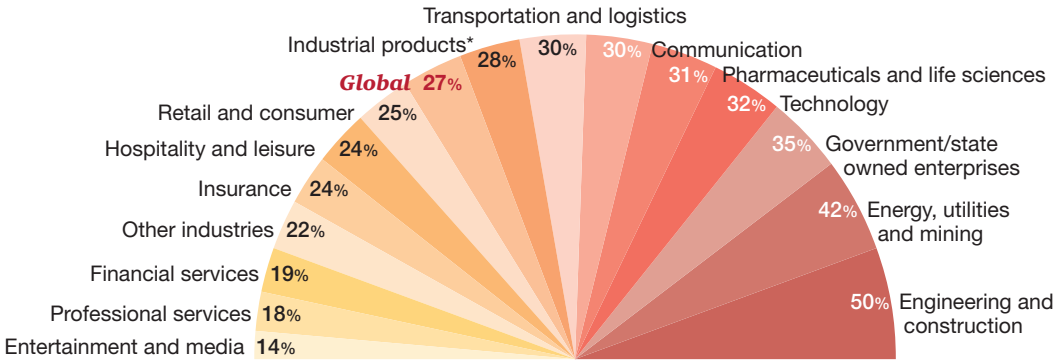
1. Respondents were asked if their organisation had operations or was pursuing operations in high risk areas, with a reference to the 2012 Transparency International Corruption Perception Index ("CPI"). The CPI is compiled annually by Transparency International, a non-profit organisation which tracks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

Figure 12: Reported bribery and corruption, by region



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

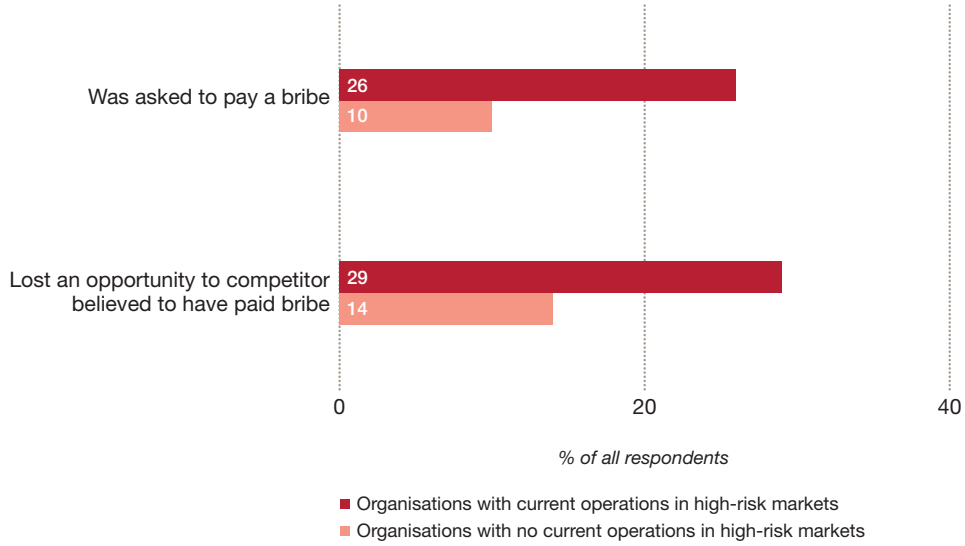
Figure 13: Reported bribery and corruption, by industry



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.

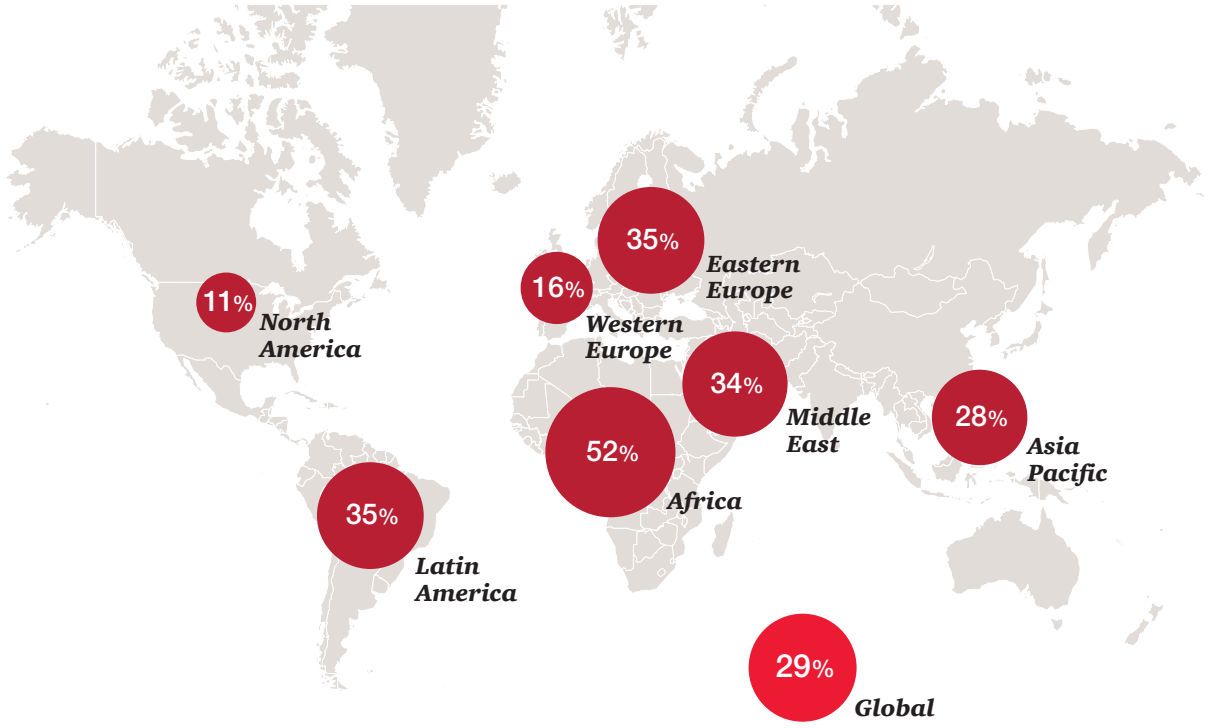
Today's perceptions, tomorrow's predictions

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.

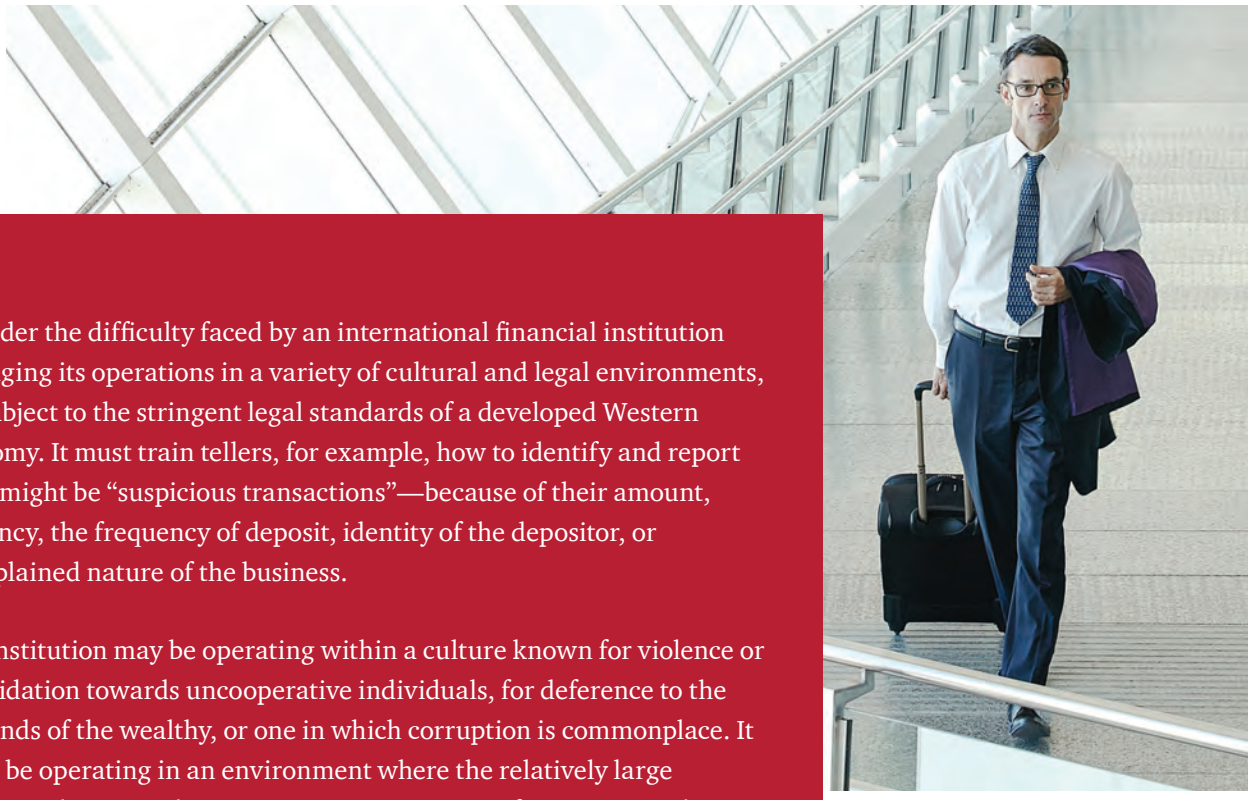
Money laundering represents a risk if a financial institution fails to report it. If the organisation is diligent in its compliance efforts to review customer transactions in accordance with the law, they are not likely to be punished by regulators, even if some incidents do occur.

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.

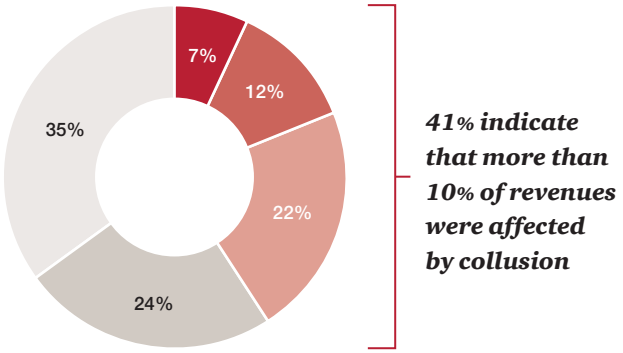
So operating in environments that pose a systemic threat of money laundering to the business processes of financial institutions is a unique challenge. Not only are money laundering schemes numerous and sophisticated, but they create a potentially significant tension between the equally laudable goals 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%).

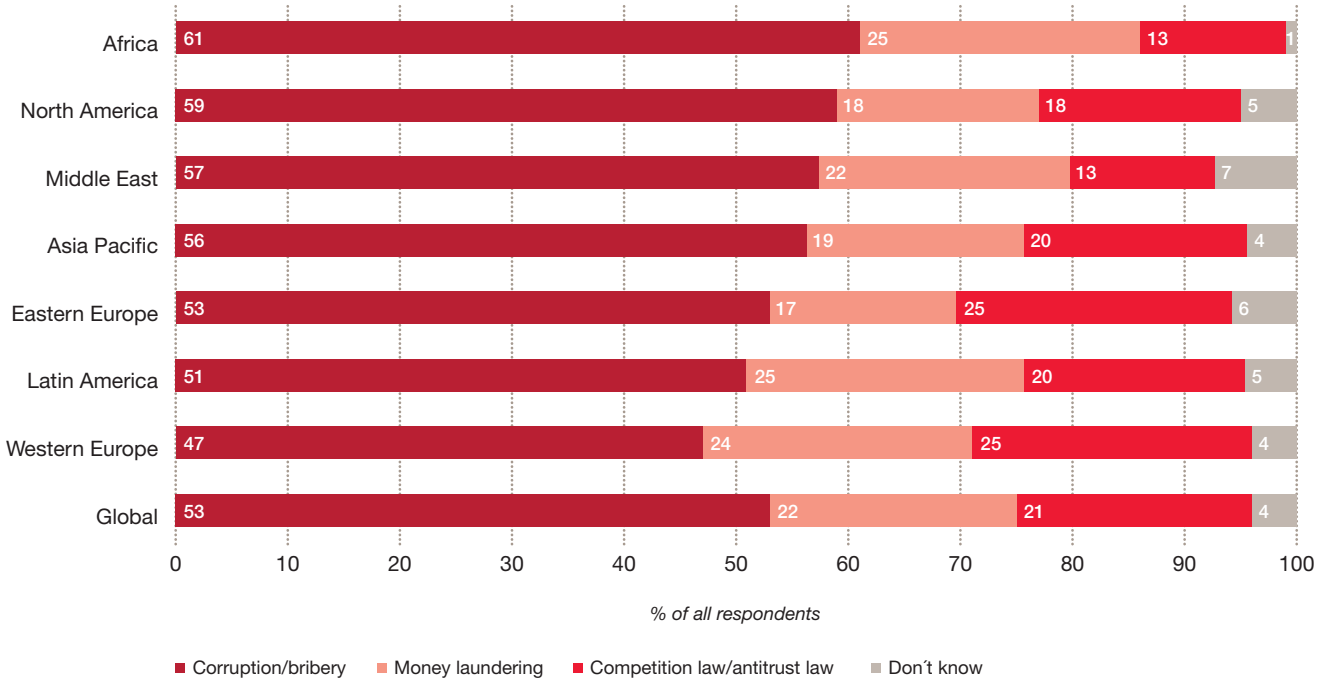
Figure 17: Perceived greatest relative economic crime risk

% 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.

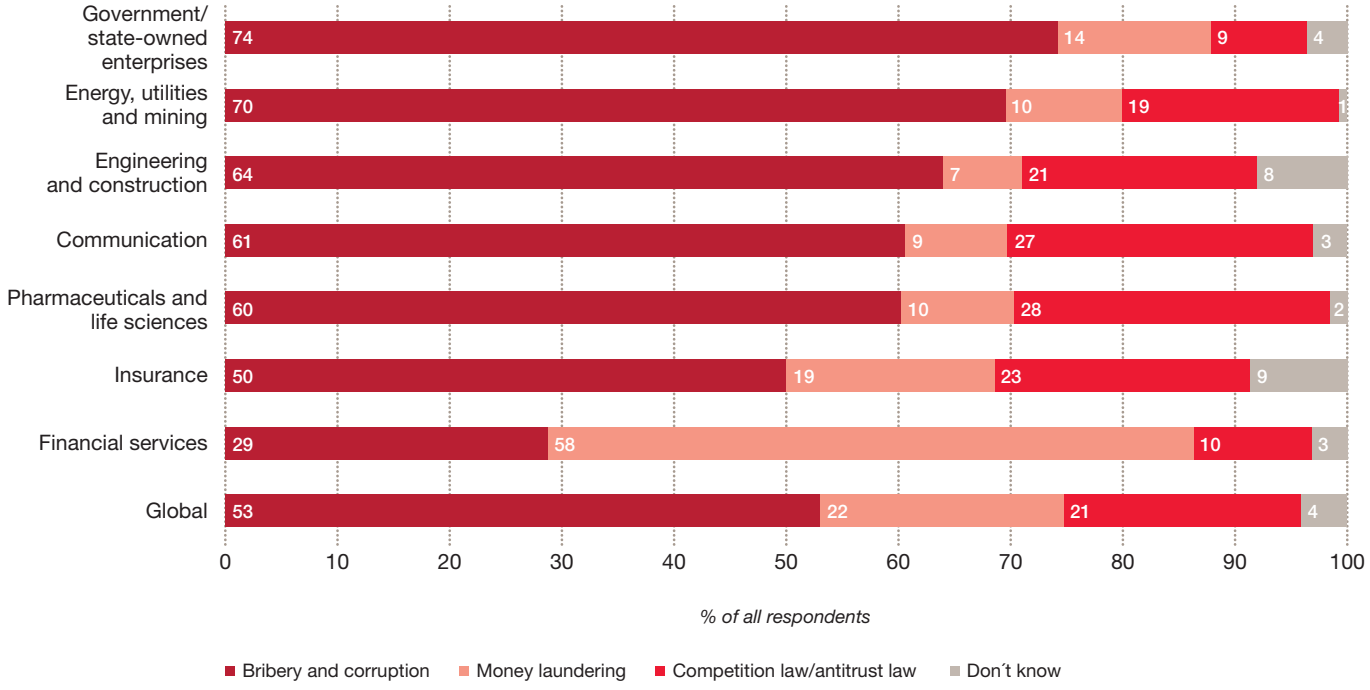
Figure 18: Perceived greatest relative economic crime risk, by region



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.

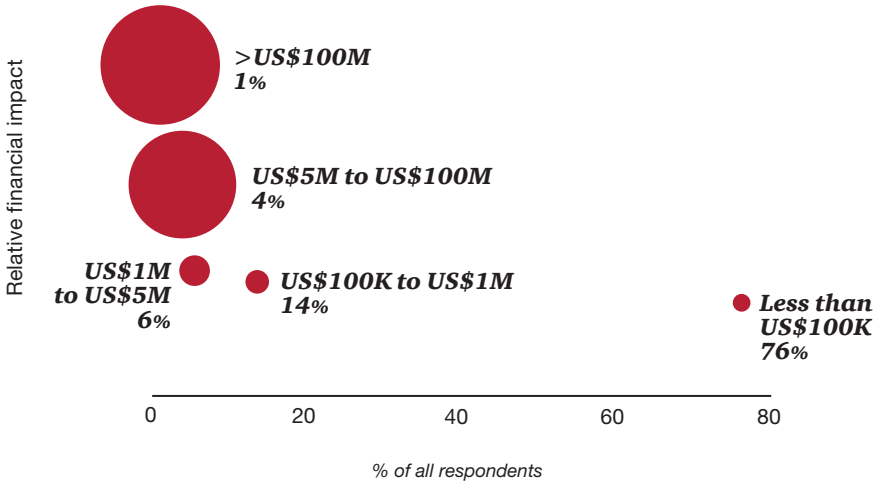
Cybercrime:
The risks of a networked world

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

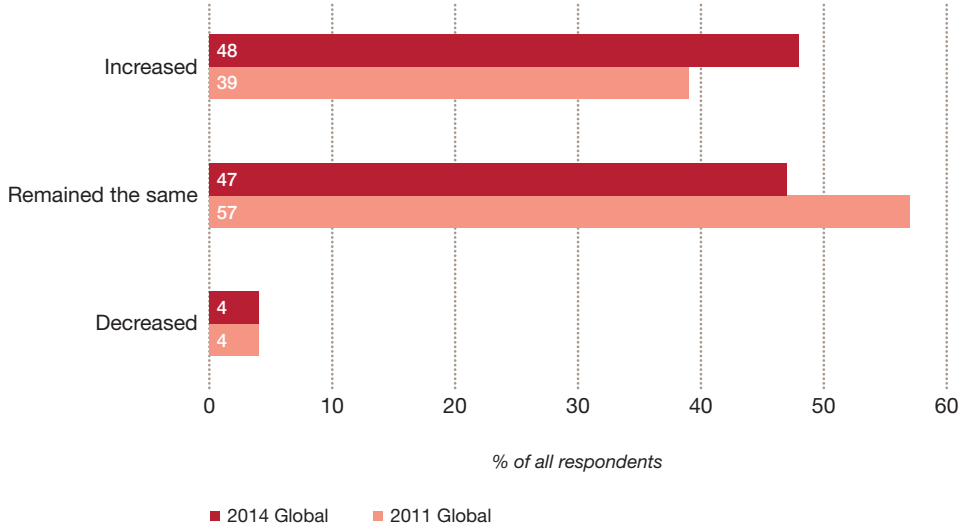


Our 2011 Global Economic Crime Survey was the first in our series to highlight cybercrime as a high-level threat to organisations. This year's survey confirms the significant, continuing impact of this crime on business, with now one in four of respondents reporting they have experienced a cybercrime—and 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?

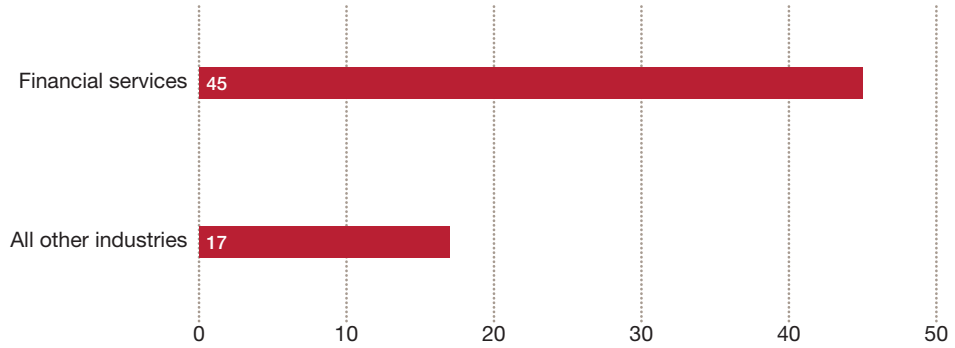
The bottom line is that much of the damage caused by these kinds of attacks is not disclosed, either because it is not known, because it is difficult to quantify, or because it is not shared. Naturally, this poses risks in a global business ecosystem that is increasingly reliant on both technology and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

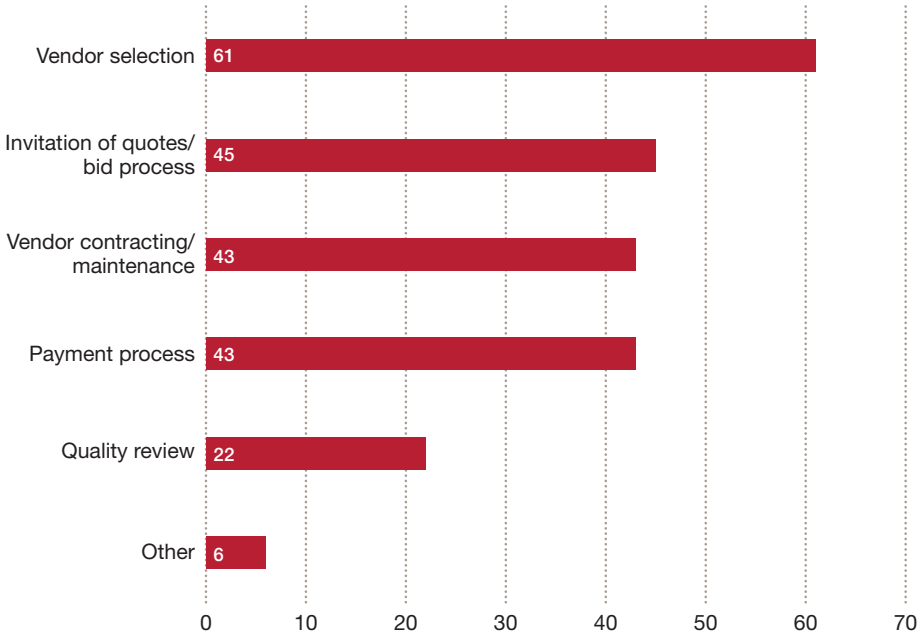
First, there has been an increase in more-competitive public tender processes from governments and state-owned businesses, unleashing the possibility of fraudulent activity on the part of agents and other third parties. No doubt, in past surveys procurement-related kickbacks, bid-rigging, or similar 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

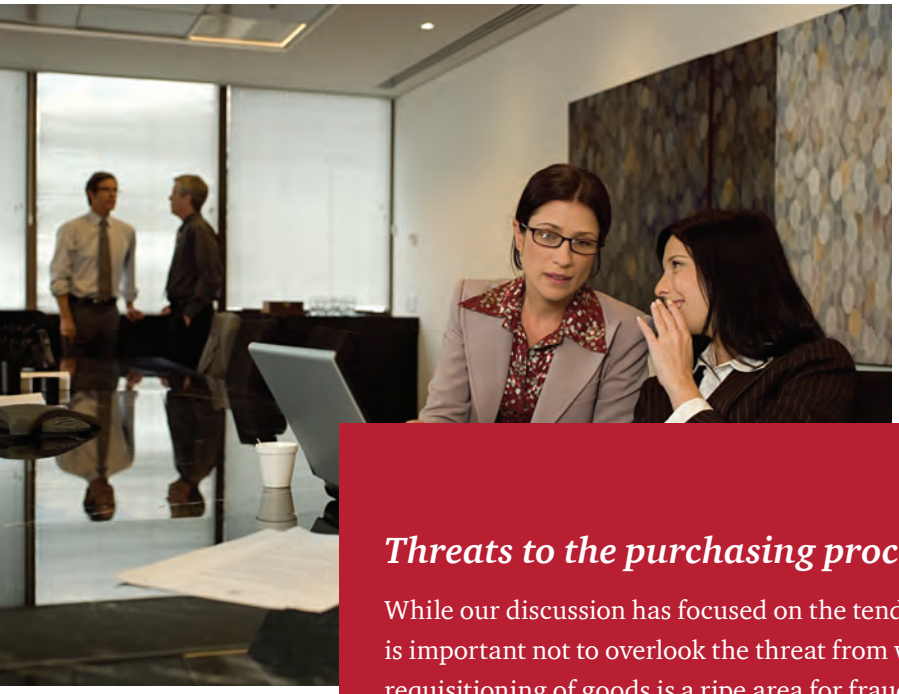
It's worth noting that procurement frauds are not only investigated and enforced at the sovereign level. In recent years, the World Bank has taken a more active stance against fraud in general, with 79 cases opened in 2012. As the institution commonly funds infrastructure projects in developing countries, 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.

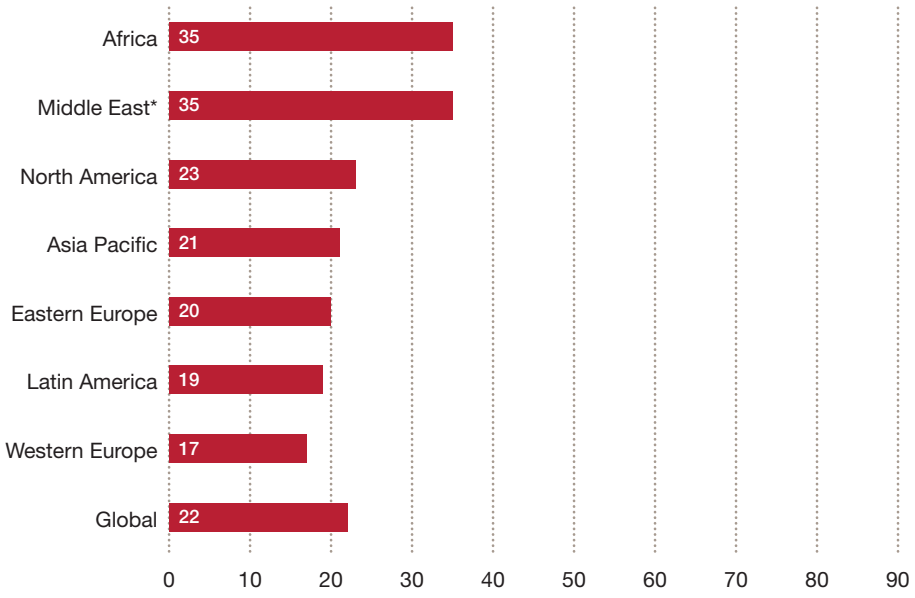
Financial statements are a fundamental barometer of a business—and a traditional starting point for analyses relating to credit decisions, contract awards, and capital raising in public markets. Accounting fraud—which includes misleading or falsely prepared financial statements—can dupe banks, lessors, 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.

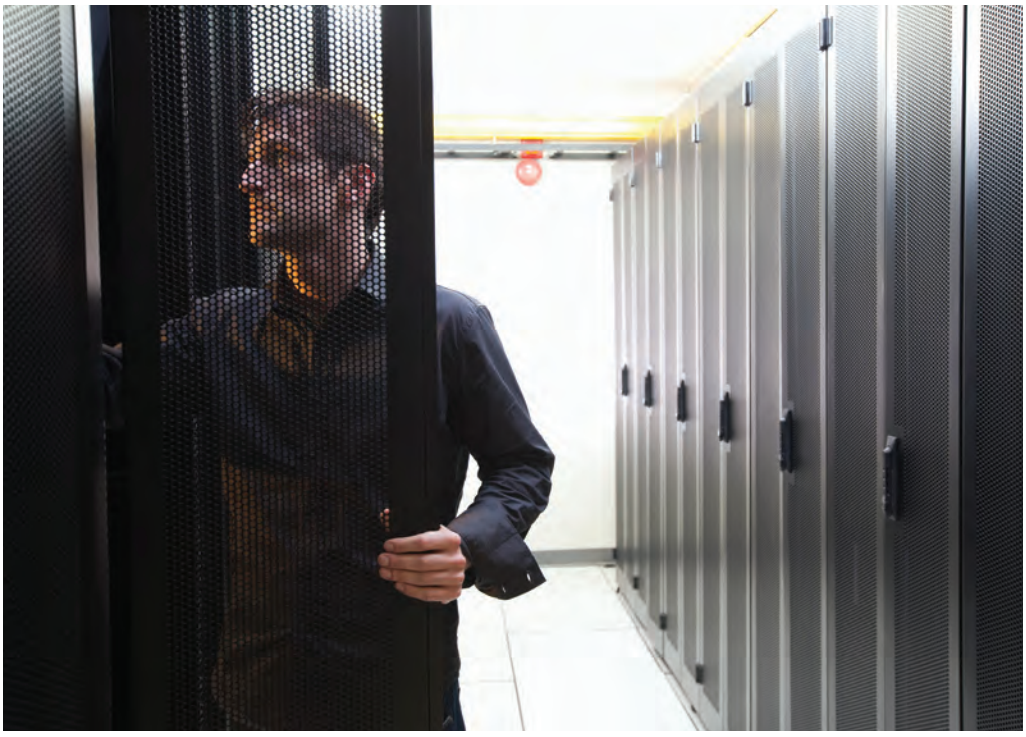
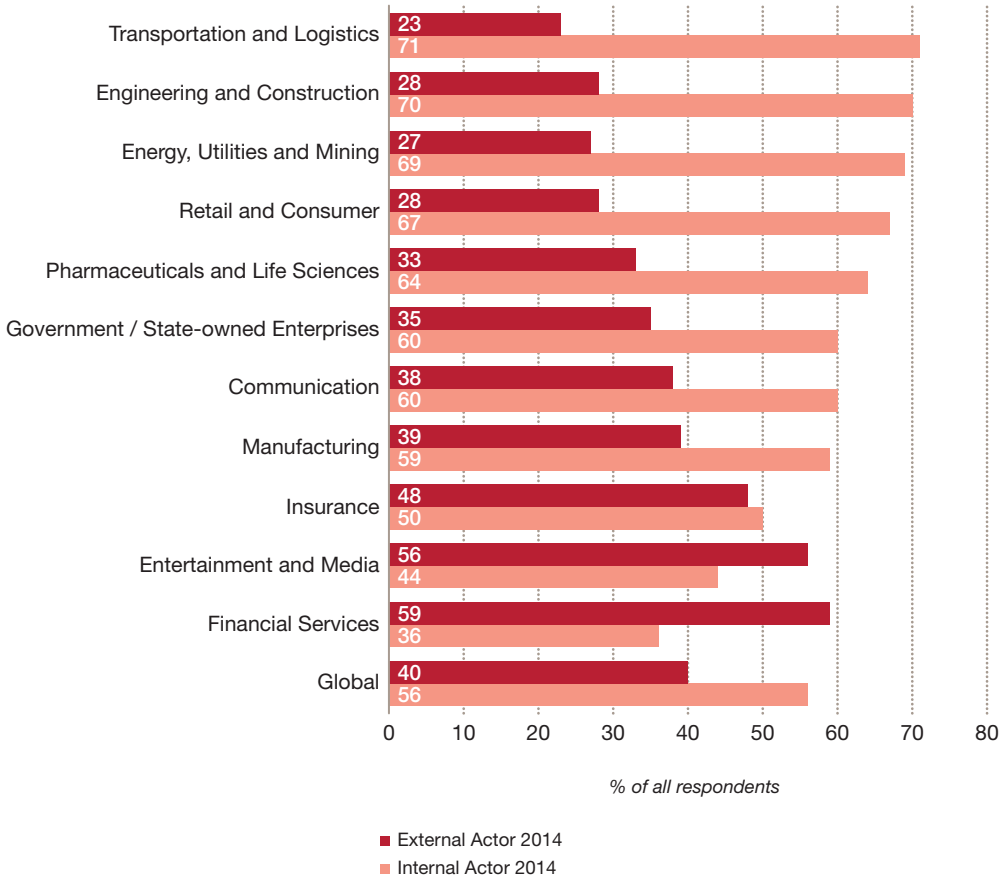


Figure 25: Internal vs. external perpetrator, selected industries



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

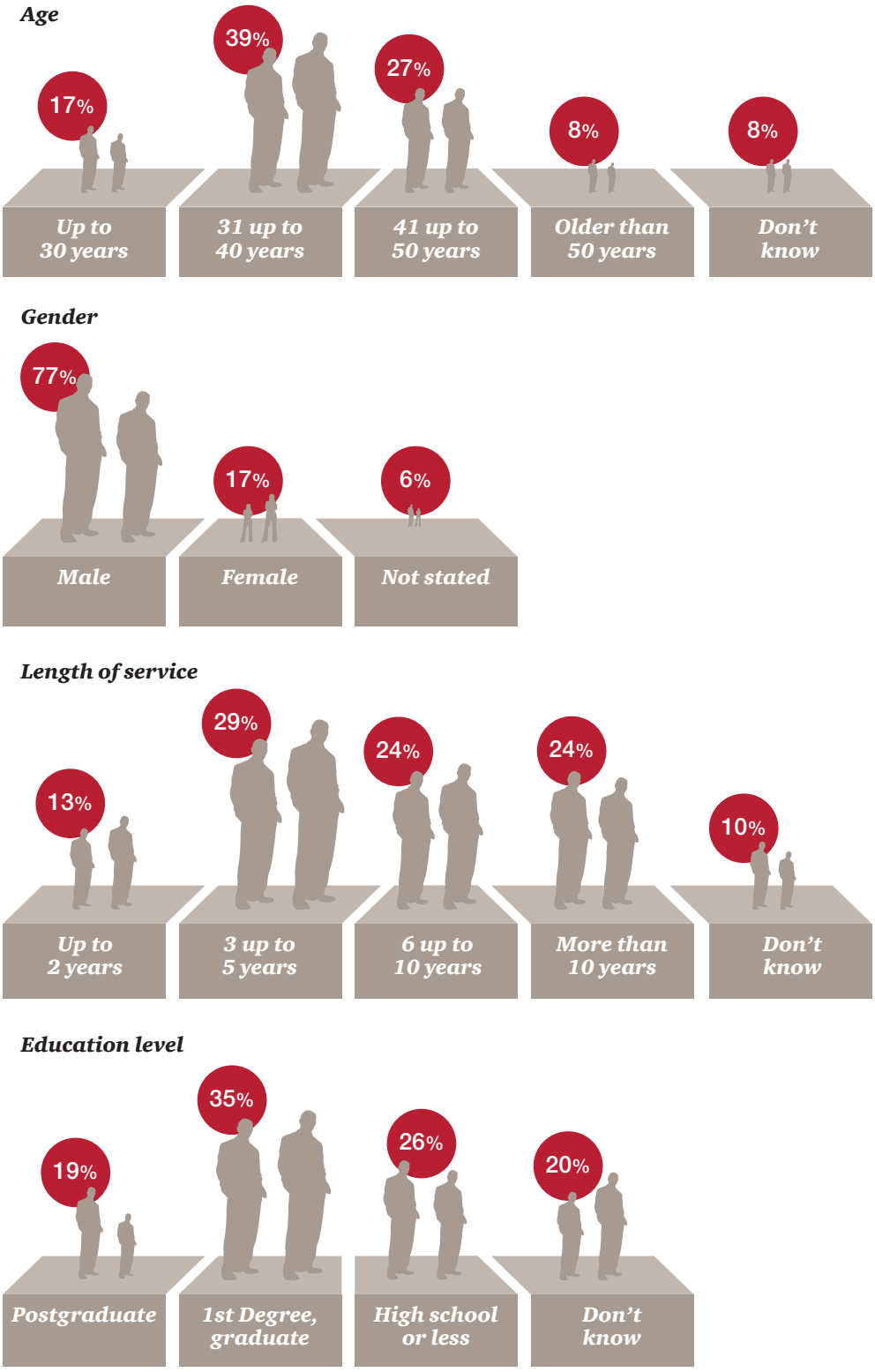
Practitioners commonly refer to a "Fraud Triangle"—the three elements that are often present when a perpetrator commits fraud: pressure, opportunity and rationalisation.

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

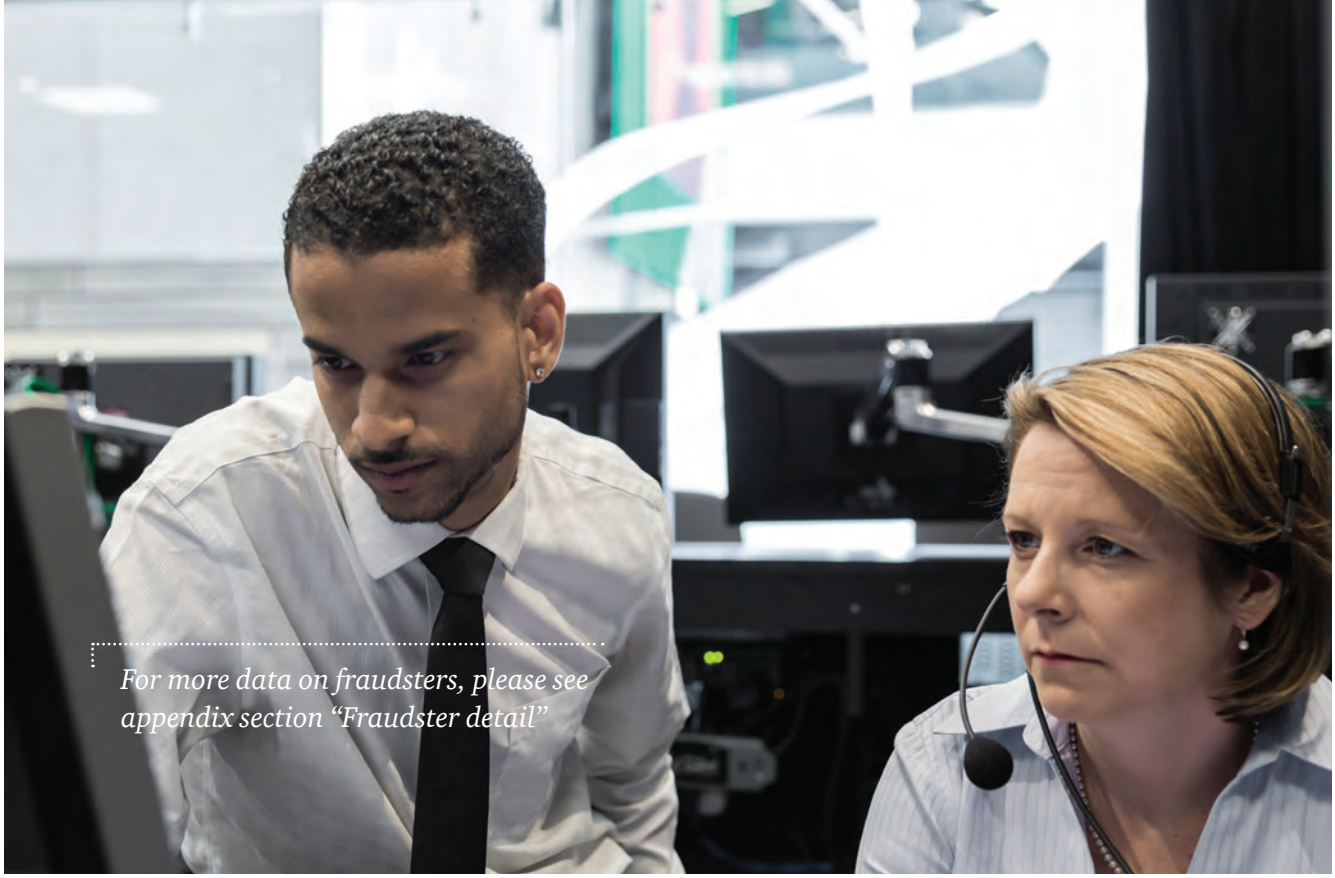
● 2014 Global

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.

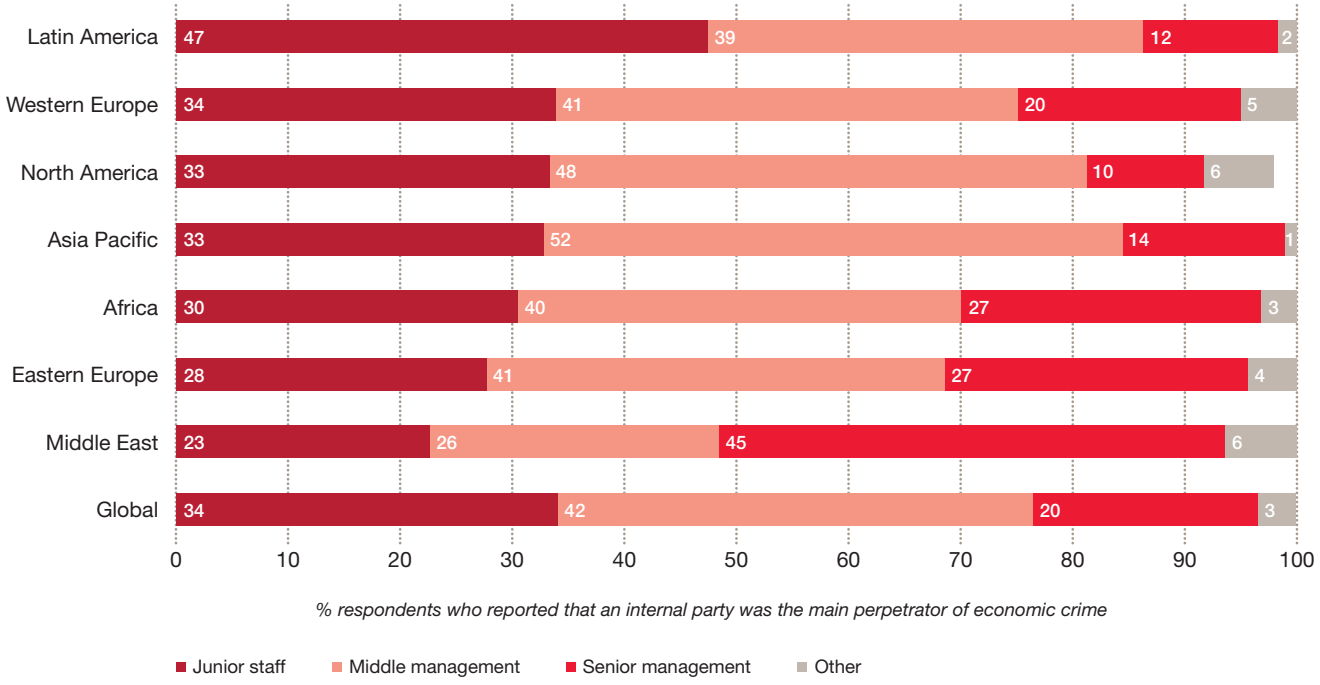
Consider the senior private banker who assures the wire transfer operators that he'll handle the client call-back procedure to confirm instructions for payments. Or the boss who says she'll take care of getting the documentation needed to support the payment. Or even the division manager who budgets 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

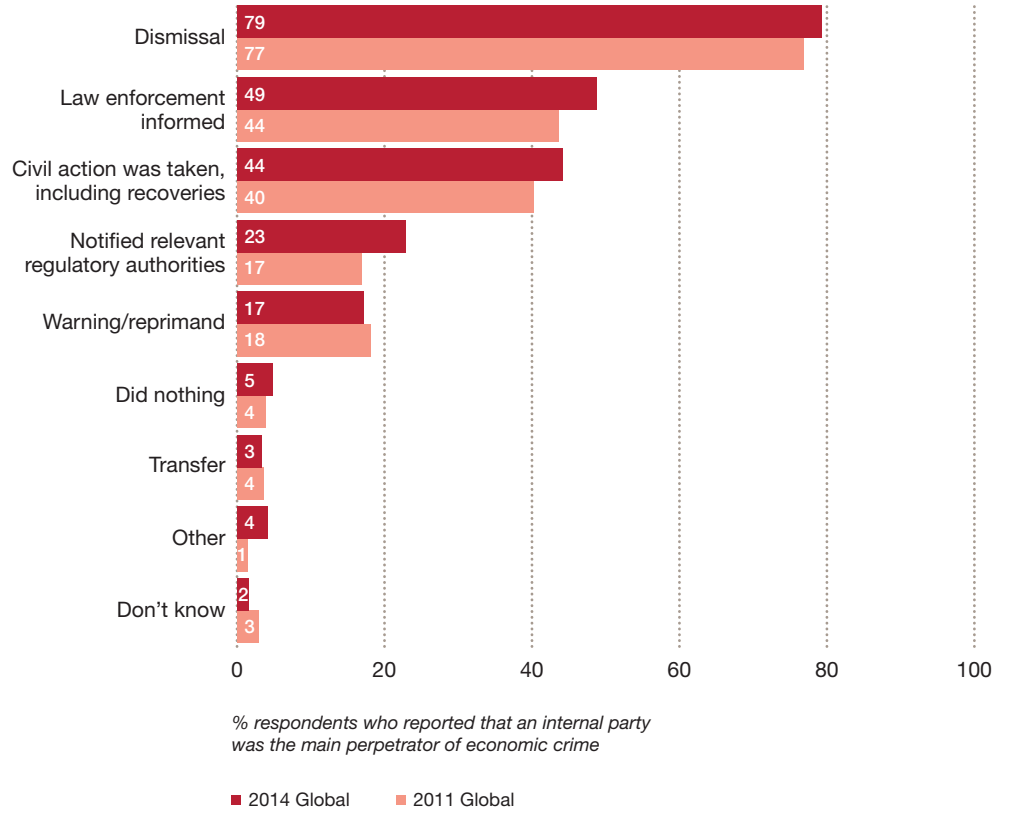


Figure 34: Profile of external perpetrator

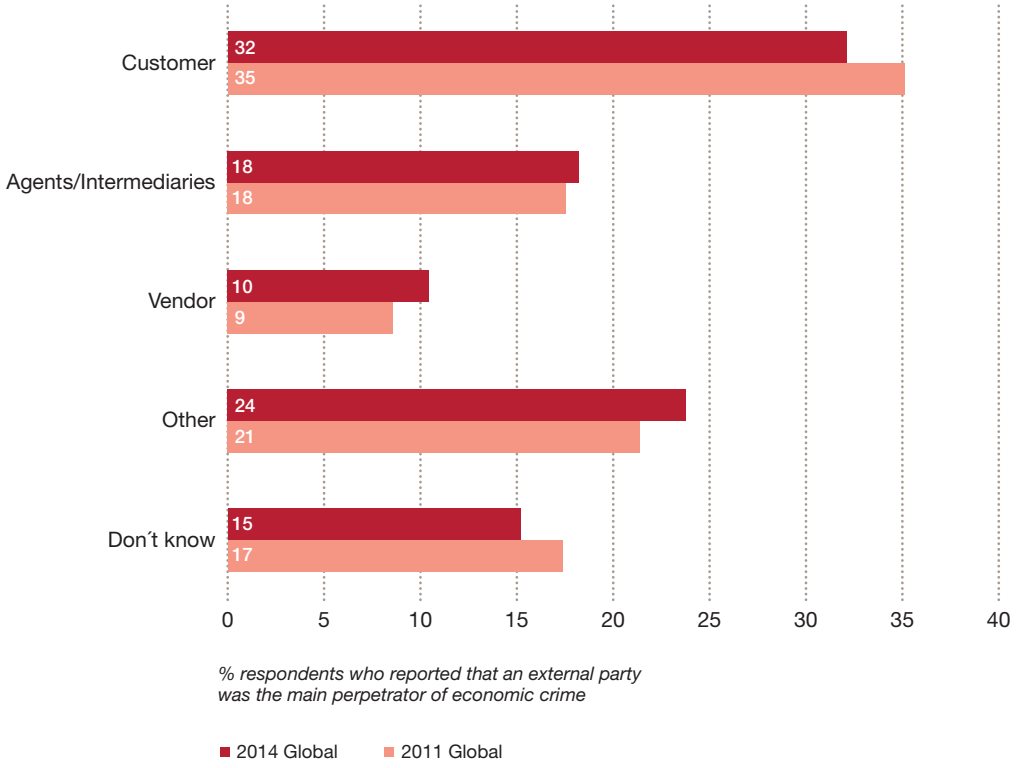
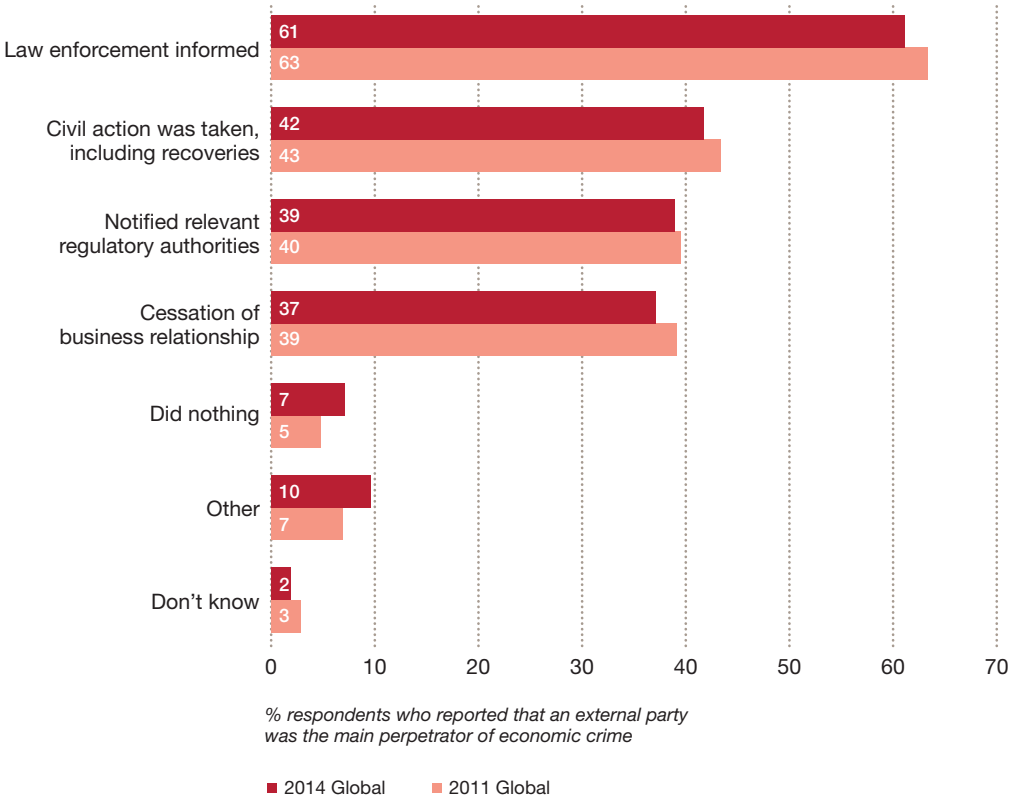


Figure 35: Actions taken against external perpetrator



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

Designed by US Studio CMD NY-14-0348

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.

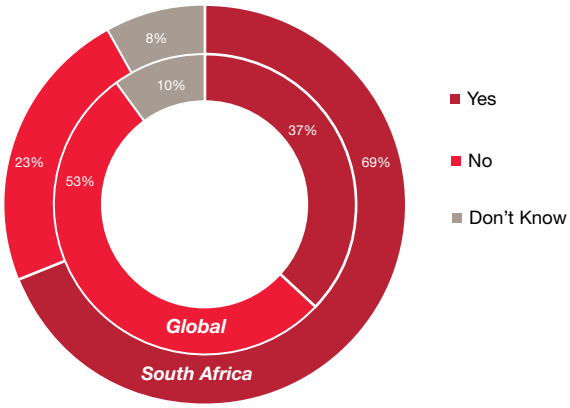
Economic crime remains a serious challenge to business leaders, government officials and private individuals in South Africa with 69% experiencing some form of economic crime in the last 24 months.

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



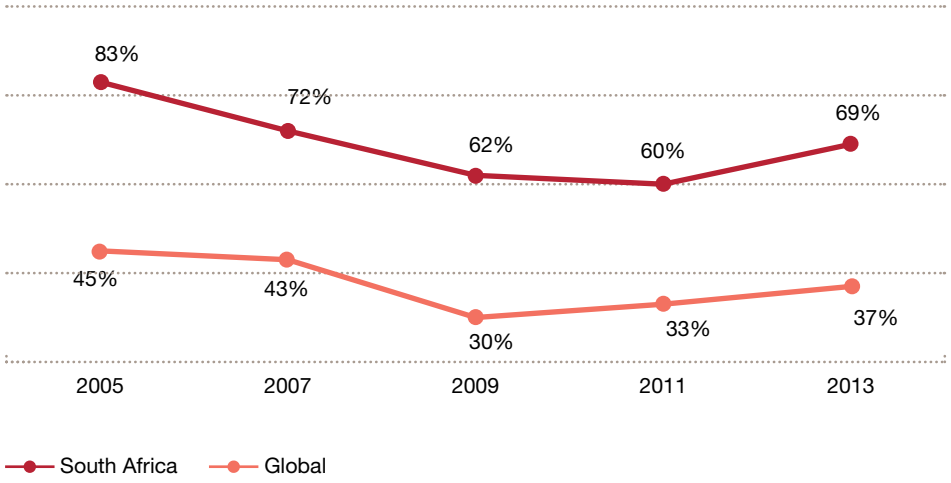
Q: Has your organisation experienced any economic crime within the last 24 months?

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.

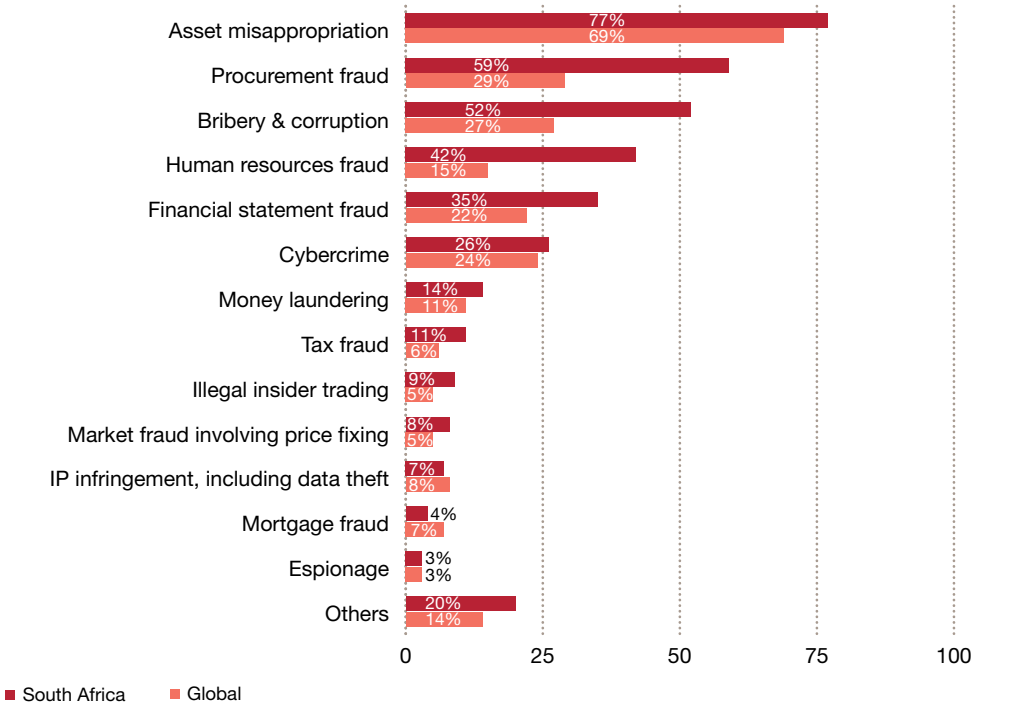
Profile of economic crime in South Africa

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 • Product/service boycotts • Negative media attention • Civil litigation • Falling share prices
Financial damage	• Loss of future business • Legal costs defending civil litigation/claims
Operational damage	• Disruptions caused by criminal/regulatory investigations • 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).

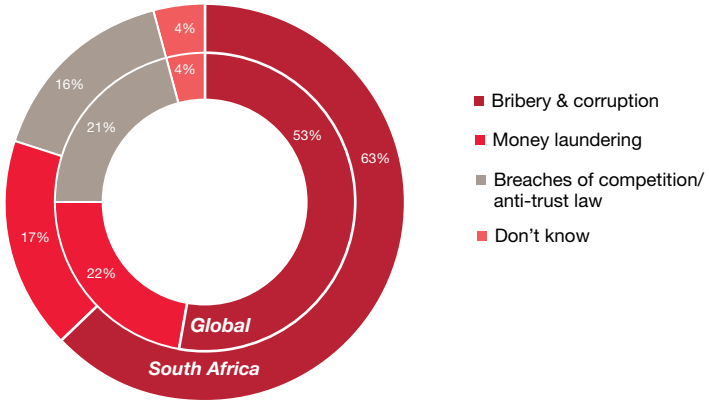
Bribery & corruption is a major problem in Southern Africa

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 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** 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 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** 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.

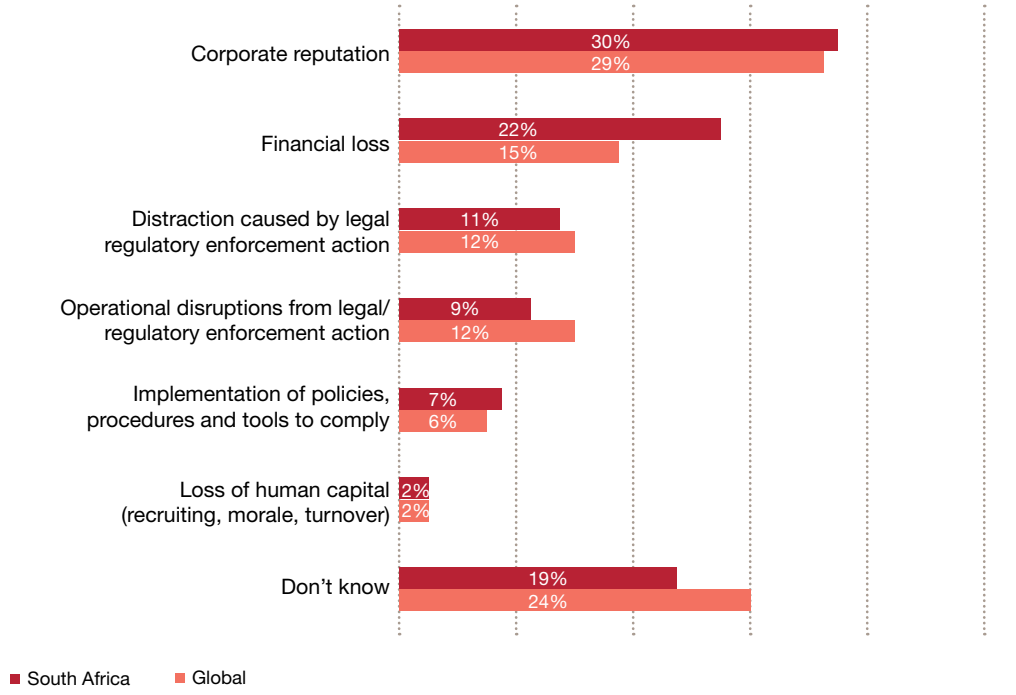
Money laundering

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

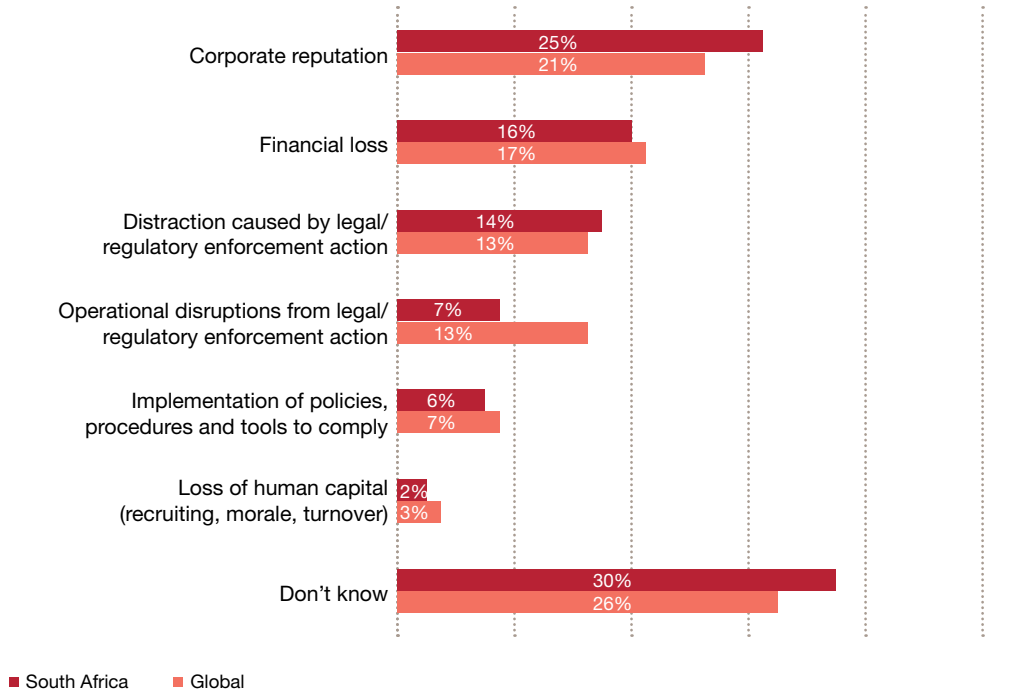
Figure 3 shows that 8% of South African respondents reported having experienced a competition law infringement during the survey period, compared to 5% globally.

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.

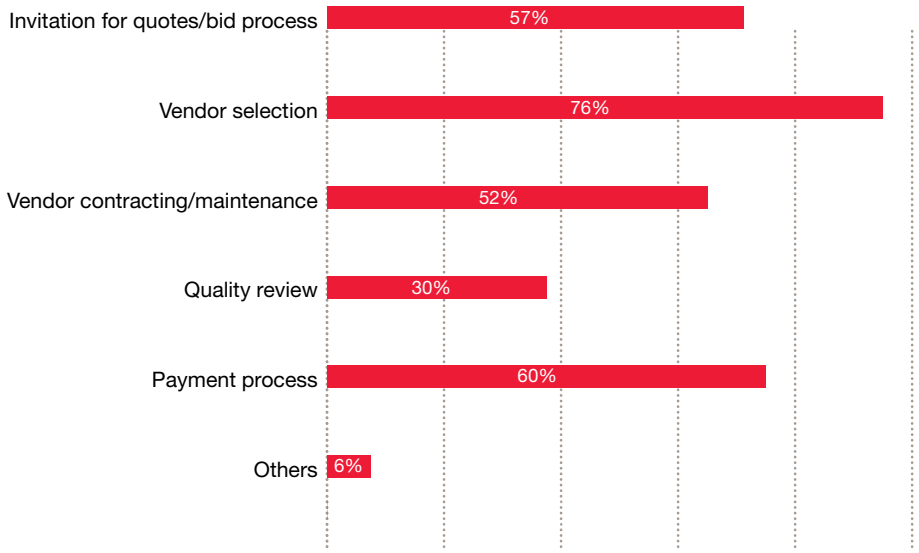
Procurement fraud

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



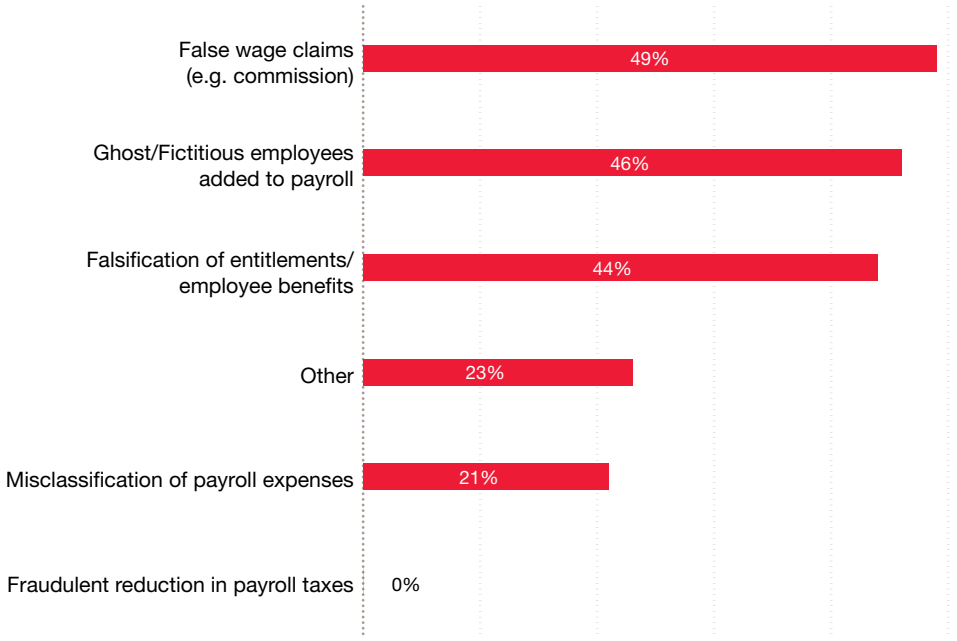
Q: Where did the procurement fraud primarily occur?

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

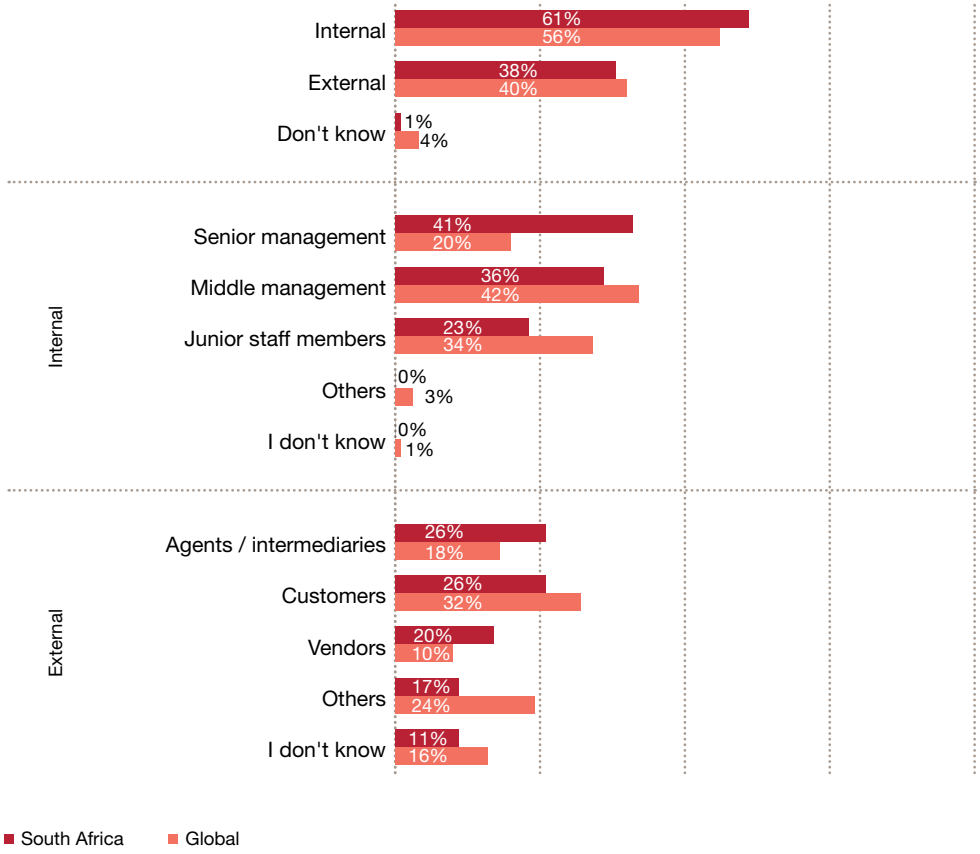


Q: What was the type of Human Resources fraud suffered?

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

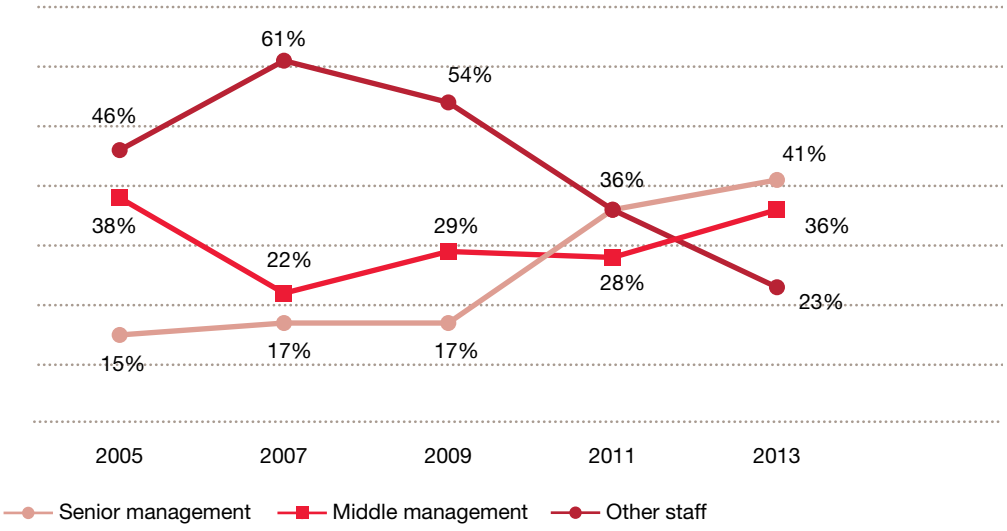


Q: Thinking about the most serious economic crime your organisation experienced in the last 24 months, who was the main perpetrator ?

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.

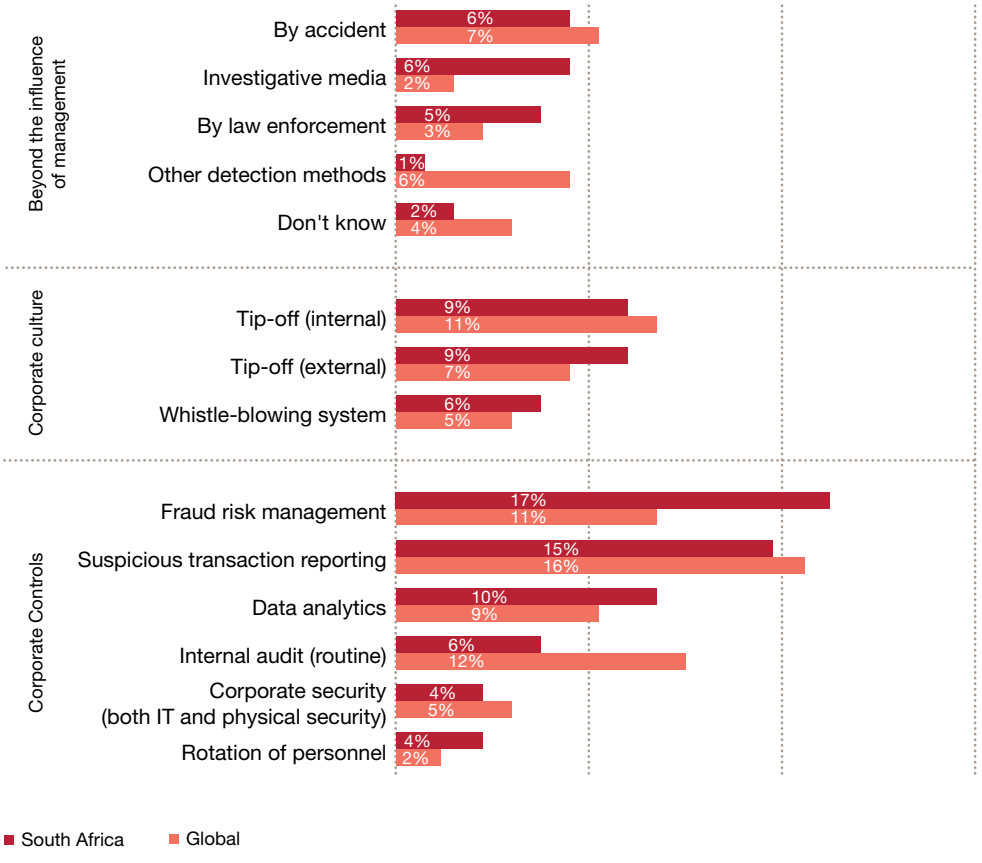
Detecting fraud

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



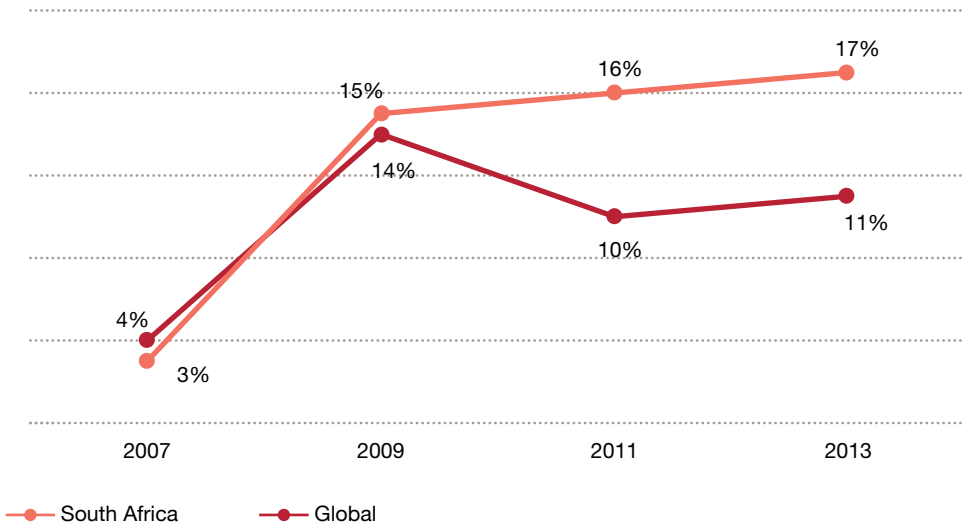
Q: Thinking about the most serious economic crime your organisation experienced in the last 24 months, how was the crime initially detected?

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

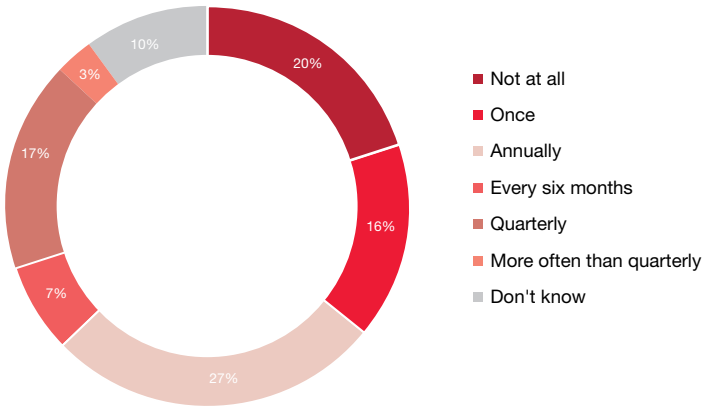
Figure 12 shows how formal fraud risk management (including formal fraud risk assessments) has established a sustainable trend in effectively detecting fraud globally, and to an even greater extent, in South Africa. Accounting for 17% of fraud detections in this survey (2011: 16%), it has been the most 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?

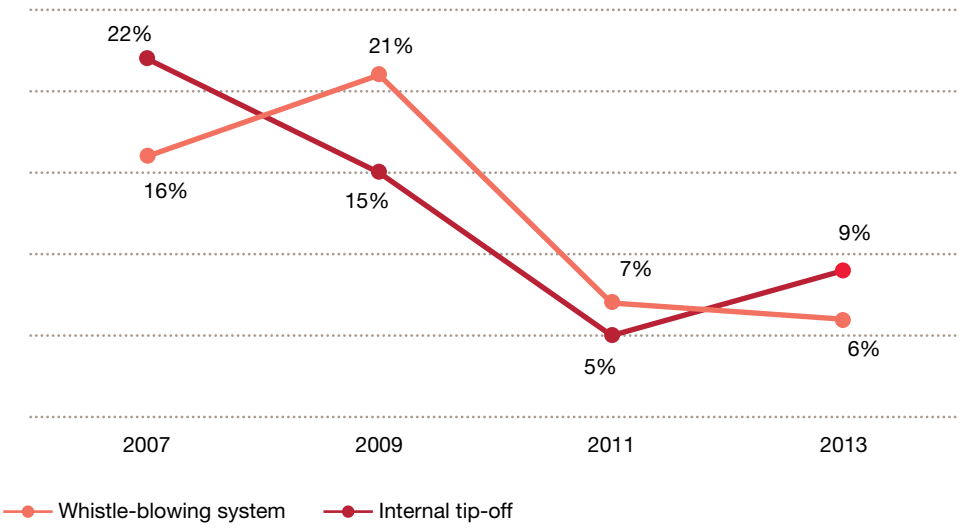
Despite being the most effective detection method, not all organisations seem to realise the value of a formal fraud risk management mechanism. Figure 14 shows that one fifth of organisations in South Africa have never carried out a formal fraud risk assessment. However, it is encouraging to note that 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

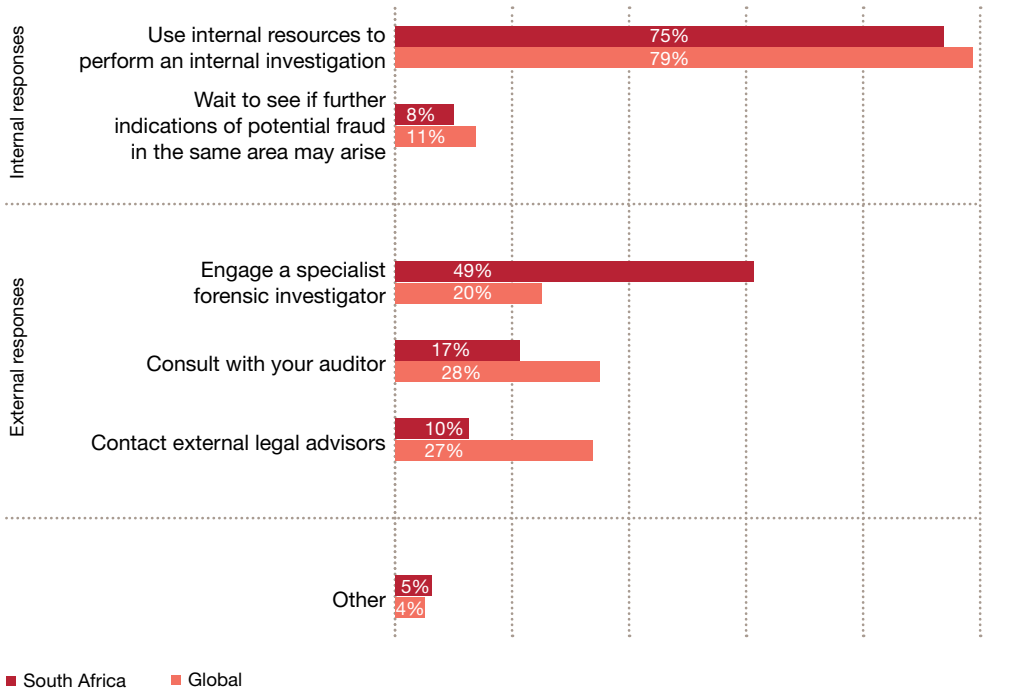
Once fraud has been detected, it is critical that an organisation takes, and is seen to take, appropriate action. Less than one in ten South African respondents (8%) and 11% of those globally confirmed their organisation would 'wait and see if further indications of potential fraud in the same area may 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

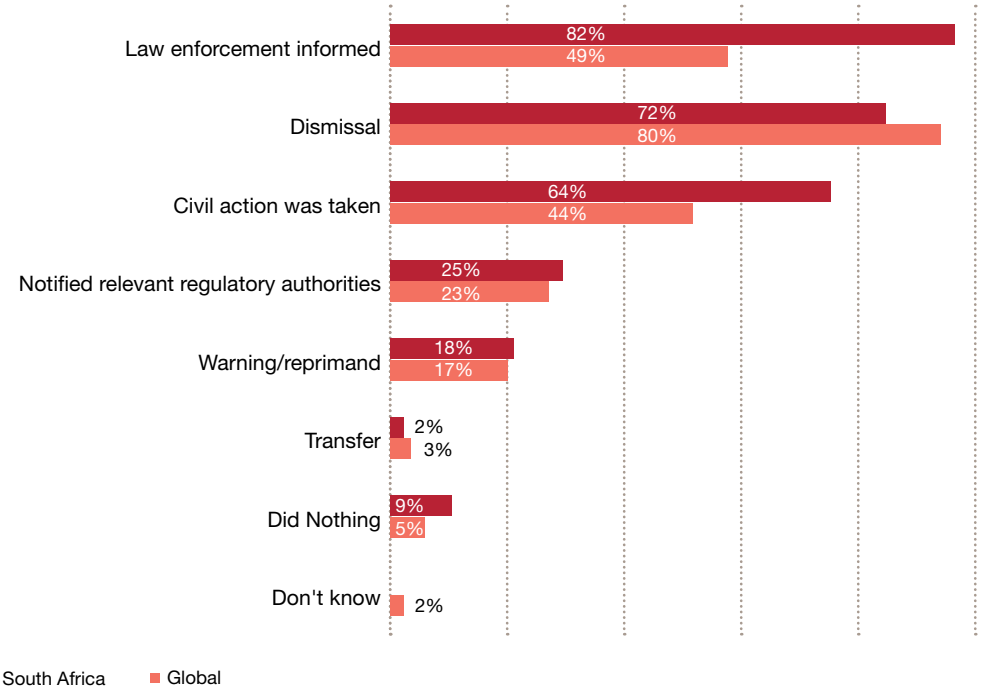


Q: When you identify an incident of potential fraud, which action(s) are you likely to take?

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?

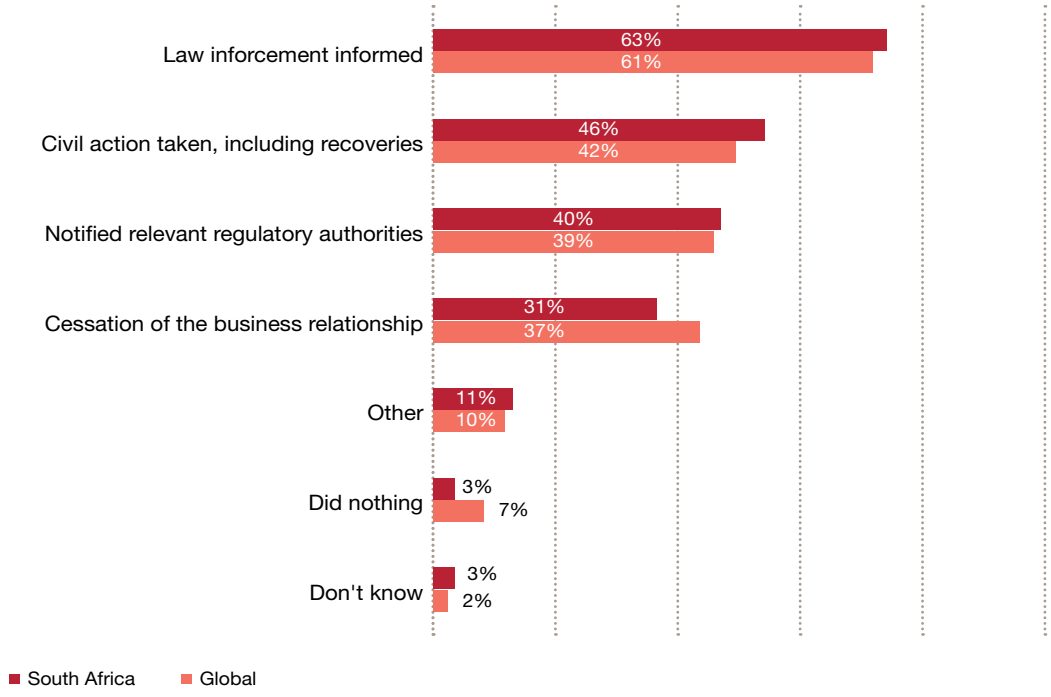
Interestingly, when it came to the most serious economic crime committed by insiders, South African entities took no action in 9% of cases, opted for transfers in 2% or warnings in 18% of cases.

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

Designed by PwC Design Studio (JB 14-14493)

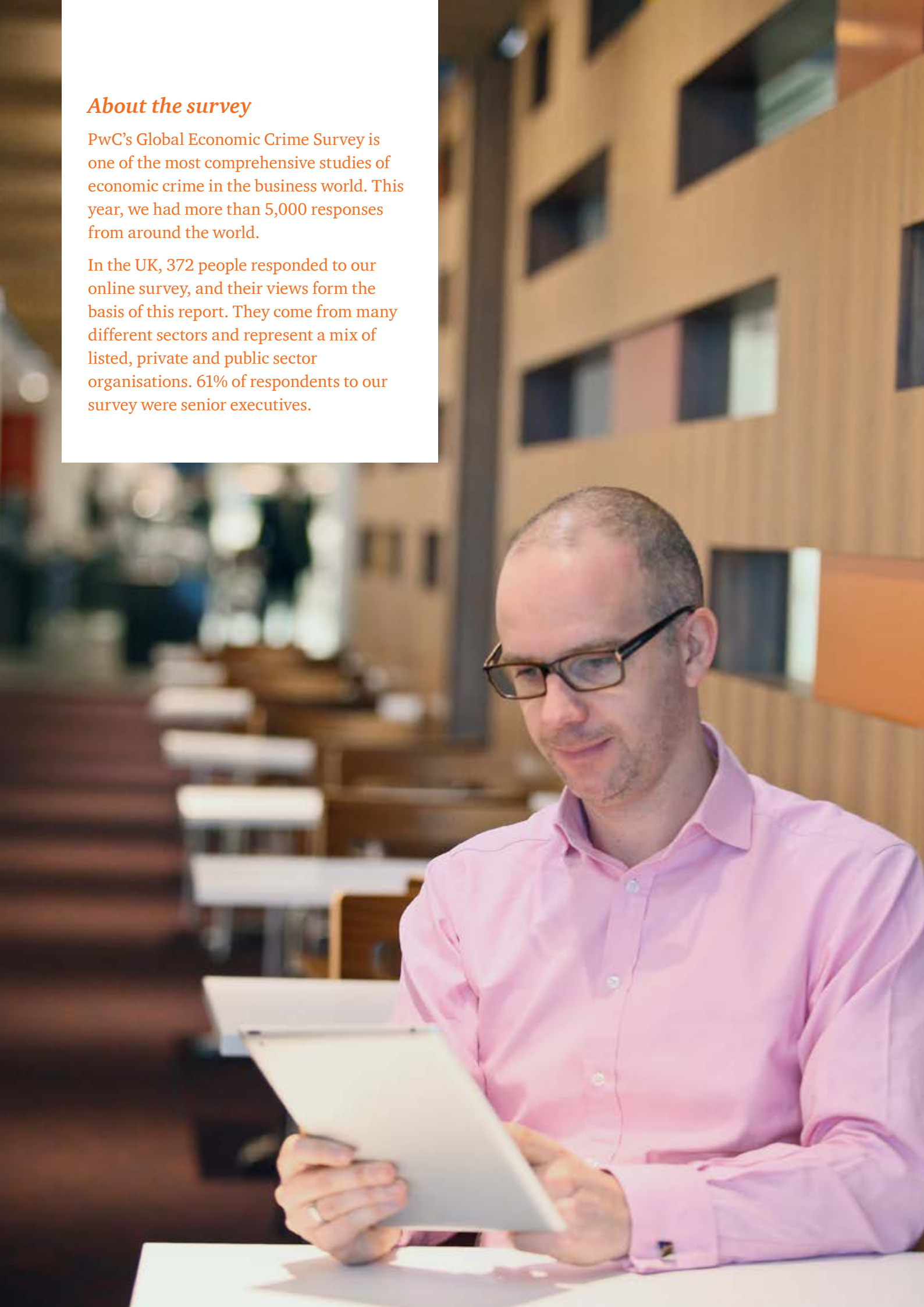
The changing face of fraud
How economic crime can impact your business

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.

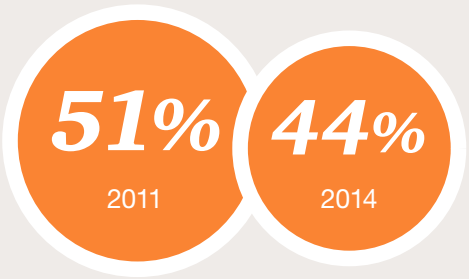
Our survey revealed that most frauds are detected by suspicious transaction monitoring and data analytics – "clever" ways of using the data that you have to identify anomalies. In contrast, we found that whistleblowing mechanisms are rarely used by organisations in the UK, despite most companies having 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.

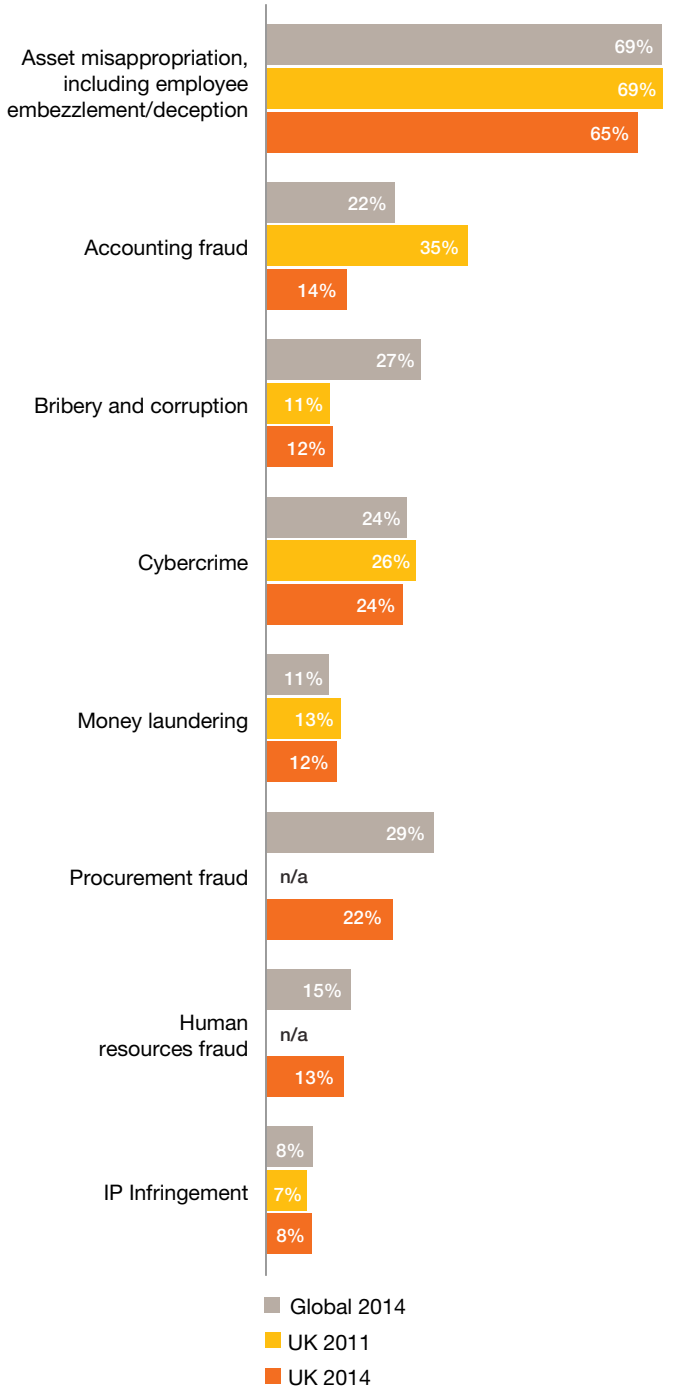
The type of fraud is changing

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

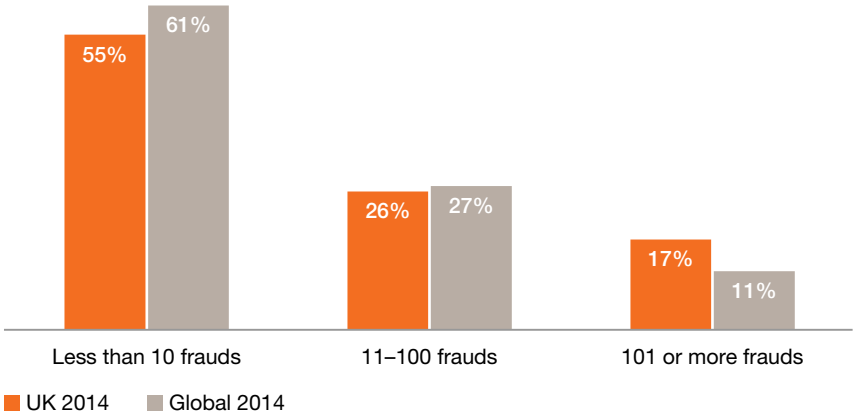
Despite the falling rate of fraud in the UK and the disconnect between the level of economic crime reported by senior executives and those below board level, it seems businesses are more aware of the risks than ever. Fifty-four per cent of respondents felt the number of instances of economic crime had 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

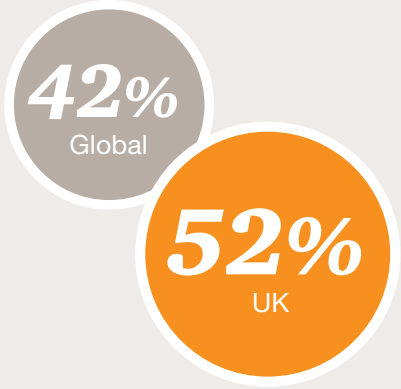
% respondents who reported either a slight increase or a significant increase

Figure 4
More UK organisations reported experiencing 100 or more frauds in the last two years than the global average



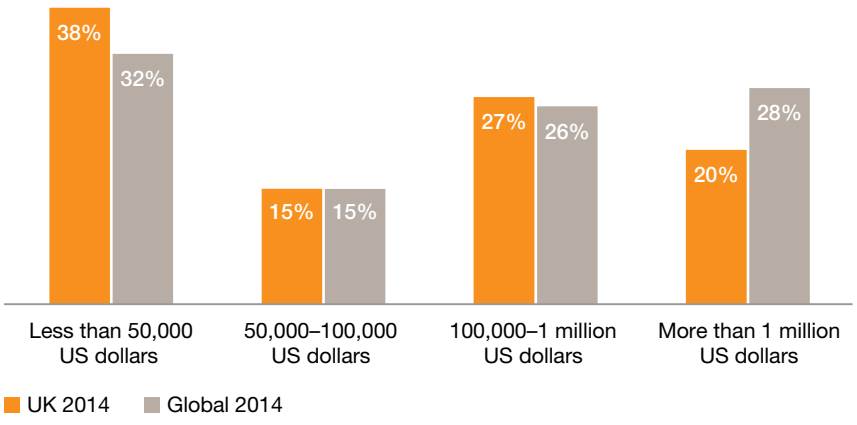
Together, these findings show that UK organisations are more likely to suffer from multiple instances of low-level economic crime than be hit by one multi-million-pound fraud. Whether a business suffers one or a hundred frauds in a year, it makes a significant impact on finances and in other ways: 18% 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

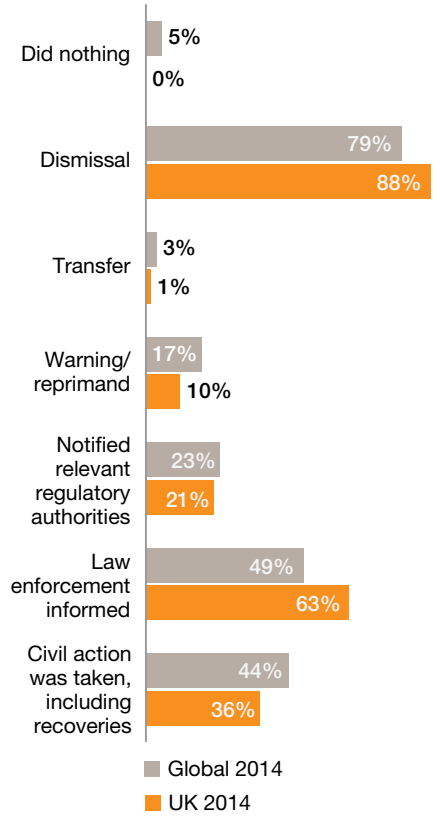
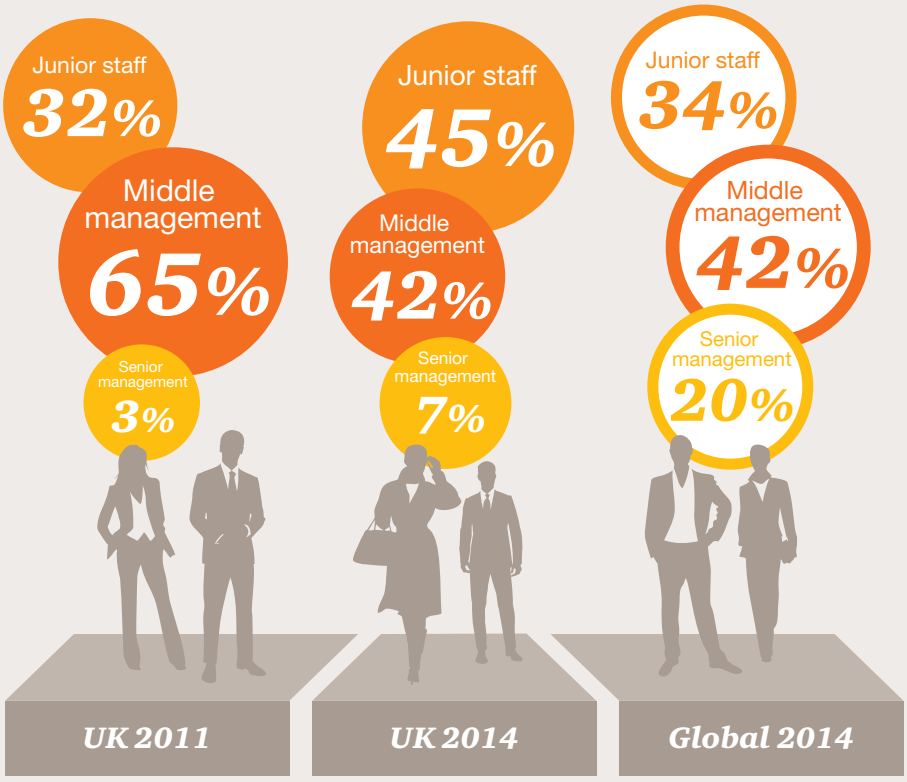
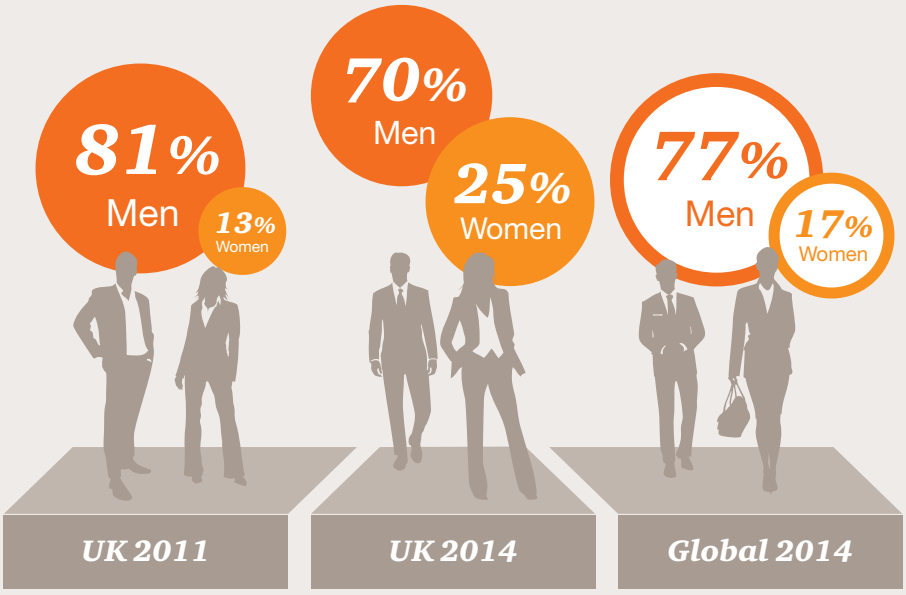


Figure 9
Is there such a thing as a typical 'fraudster'?

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.

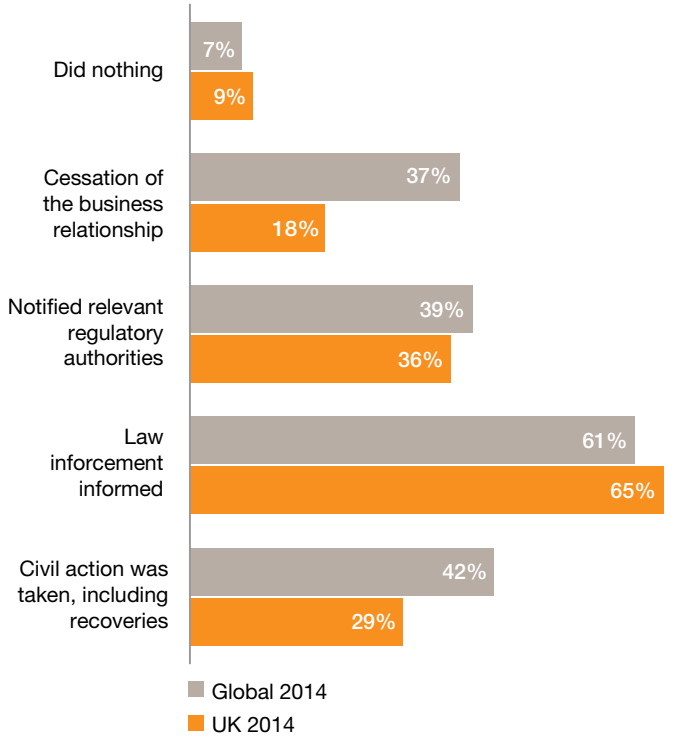
The clearest message from these changes is that it's very difficult, and potentially even dangerous, to try to identify the 'most likely' fraudster within your organisation. It could well be the person you least expect. If they have the opportunity, incentive and pressure, a fraud could be committed 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

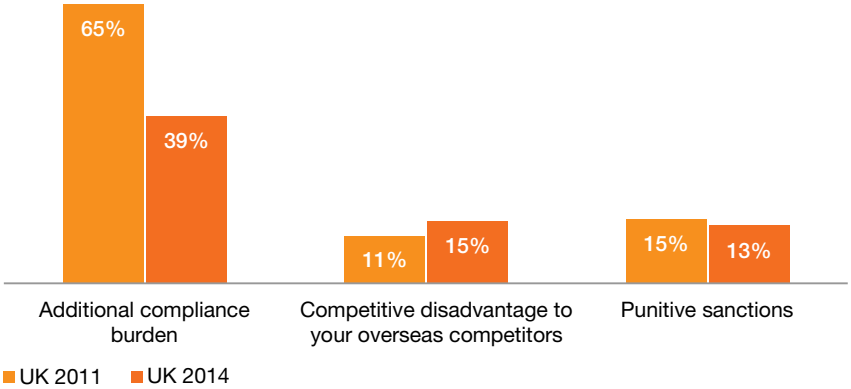
When the UK Bribery Act came into force in July 2011, nearly two-thirds of survey respondents that year said they didn't see any need to update their organisation's existing policies. But our 2014 responses show a shift in this thinking, and the Bribery Act appears to have had more impact than firms 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.

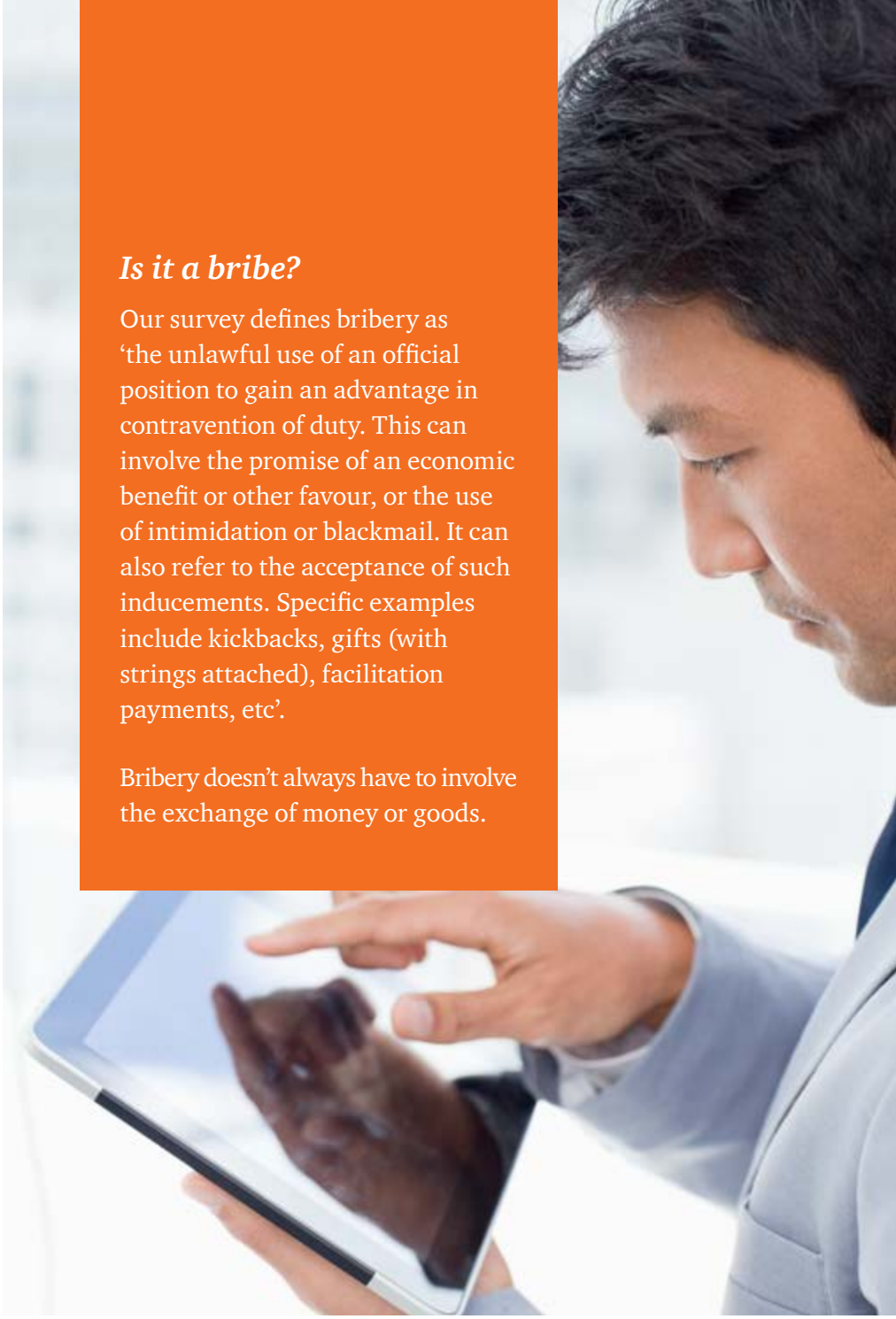


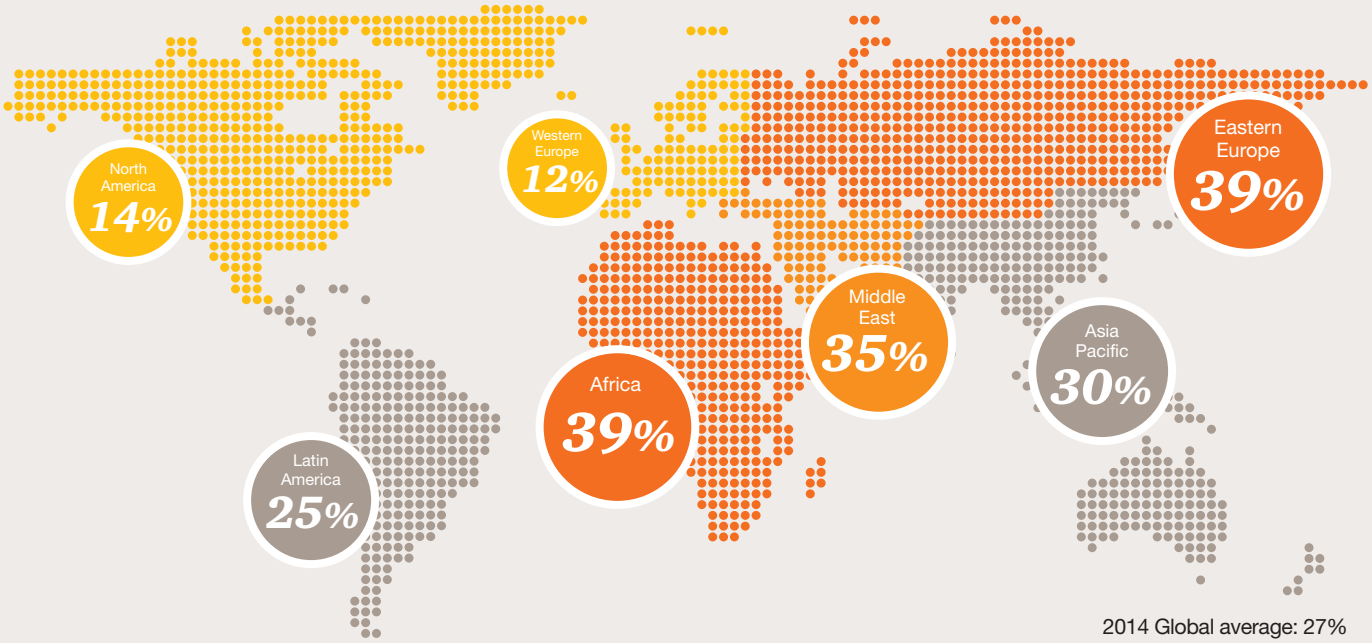
Figure 12
The UK experiences less bribery than the global average

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.

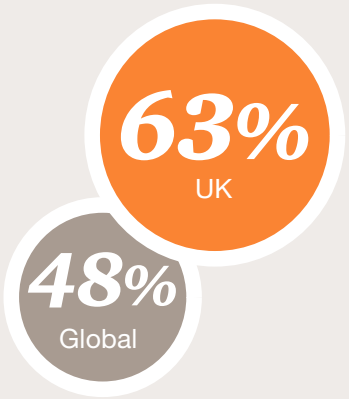
3. **Keep control:** A robust control environment needs a written code of conduct and values-based employee engagement and training (including on compliance-sensitive issues such as gifts and entertainment), as well as a system of controls that monitor suspicious transactions. Organisations are only 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.

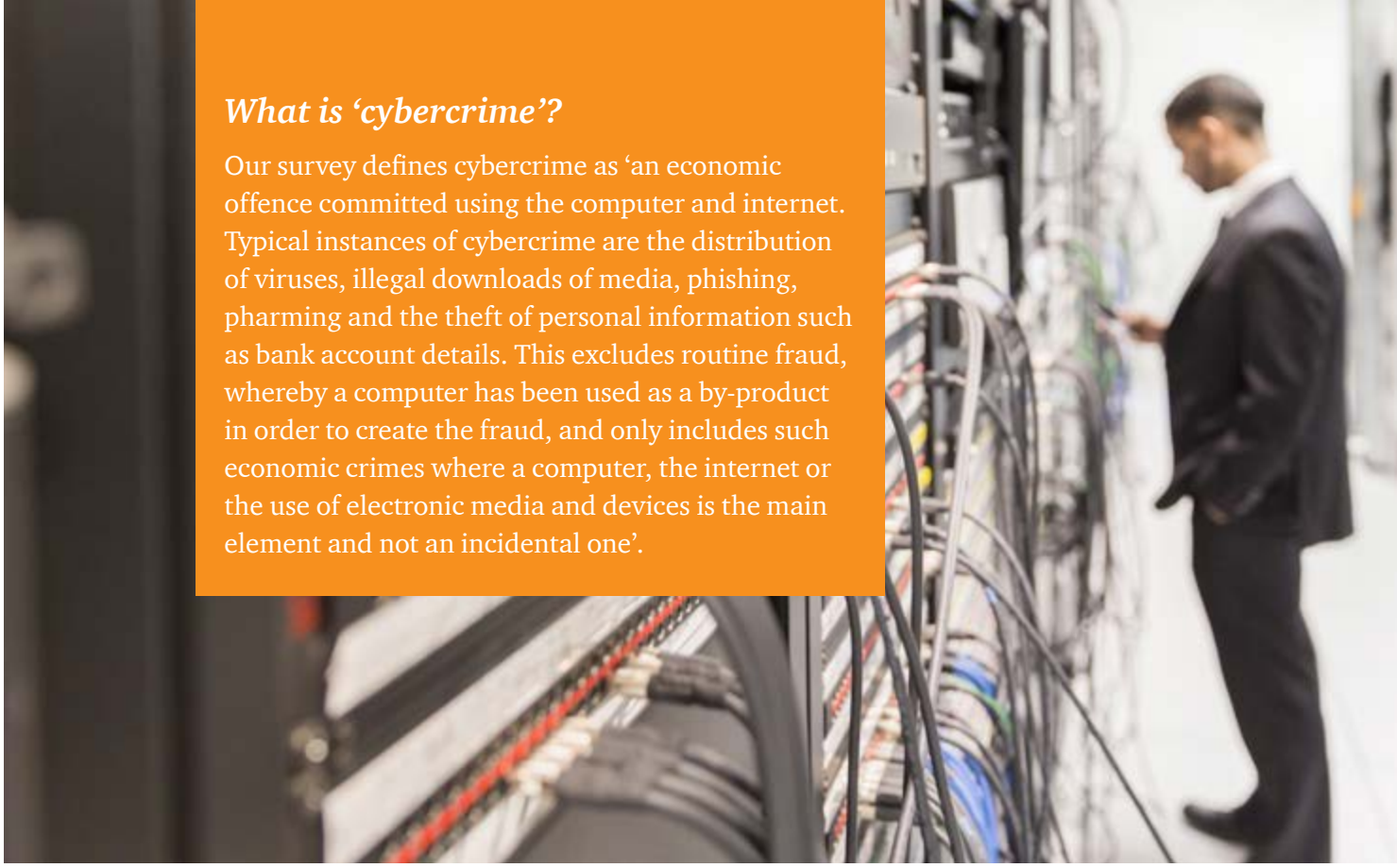
Businesses might not be spotting cybercrime

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.

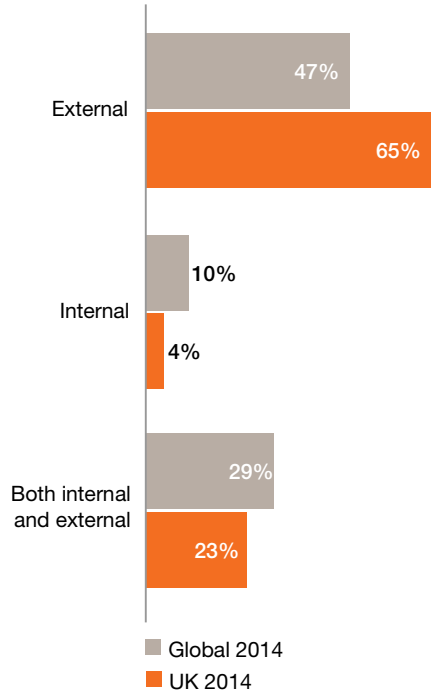
Unsurprisingly, people are most concerned about the impact that a cybercrime would have on their organisation's reputation and the subsequent service disruption. Interestingly, only 58% of our respondents said they were concerned or very concerned about the legal or enforcement costs. This is down from 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.

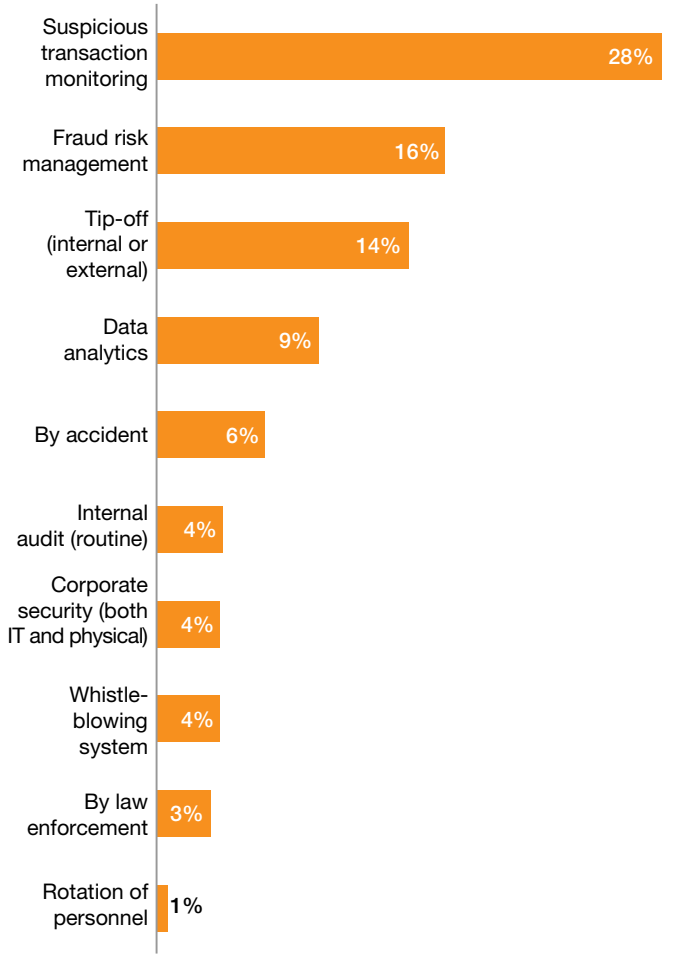
Unsurprisingly, businesses view cybercrime as mainly an external threat, with 65% of respondents feeling that the main source of danger lies outside their organisation. Far fewer respondents in the UK feel the threat is internal, or both internal and external, than the global average and the percentage 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?

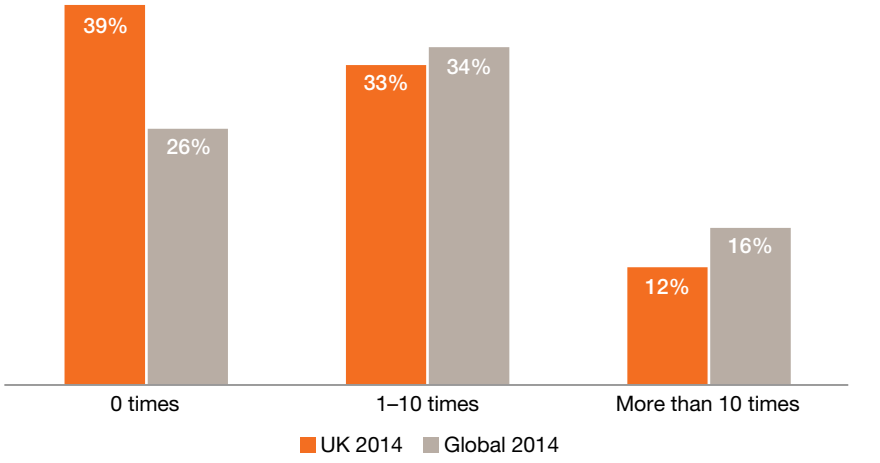
The vast majority of organisations in the UK have invested in whistleblowing mechanisms: 83% of our survey respondents said their company had one, much higher than the global average of 62%. But they're underused. We found that nearly 40% of our respondents reported that their organisation's whistleblowing 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:

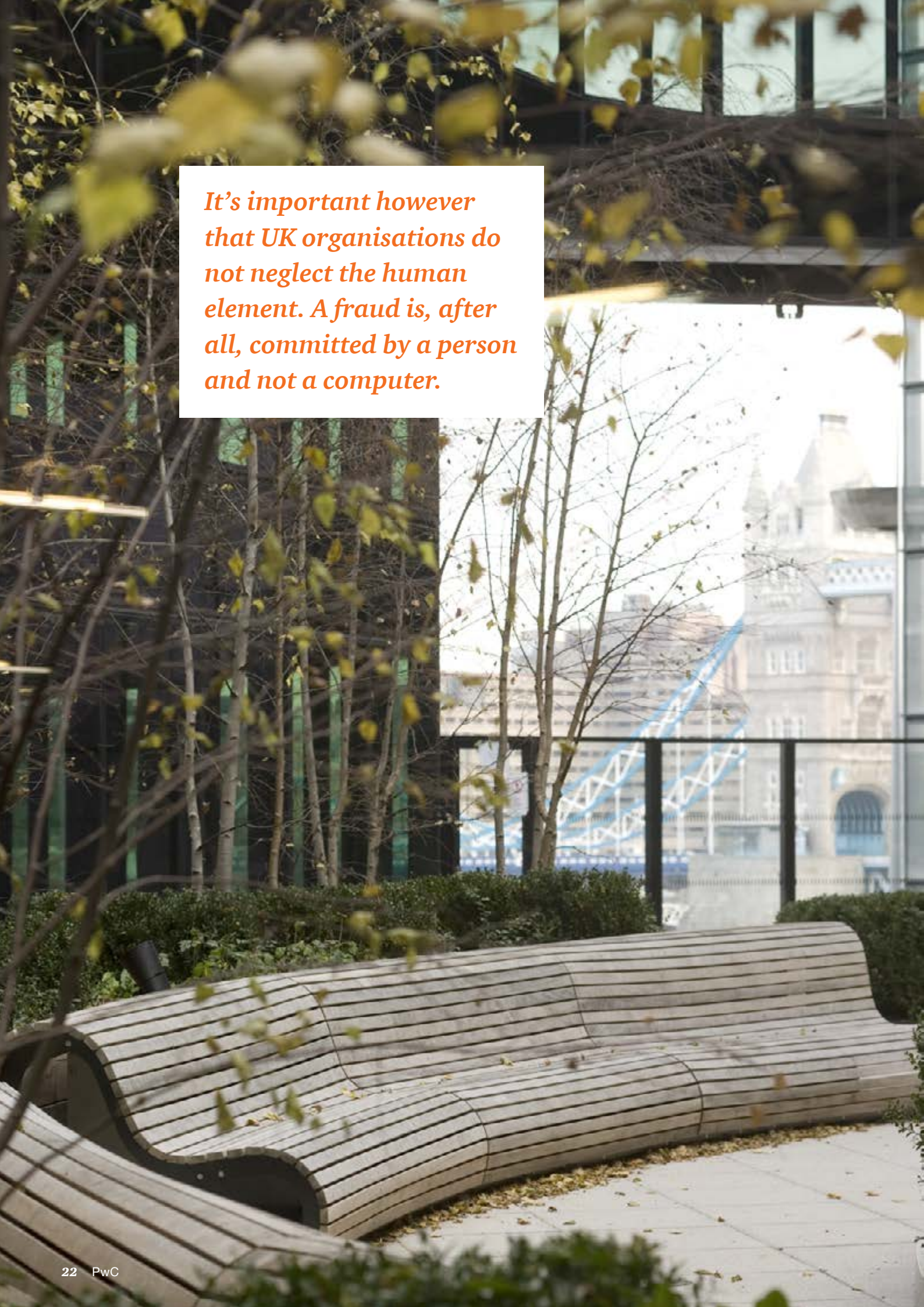
Considers the fraud risks that each business unit faces

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

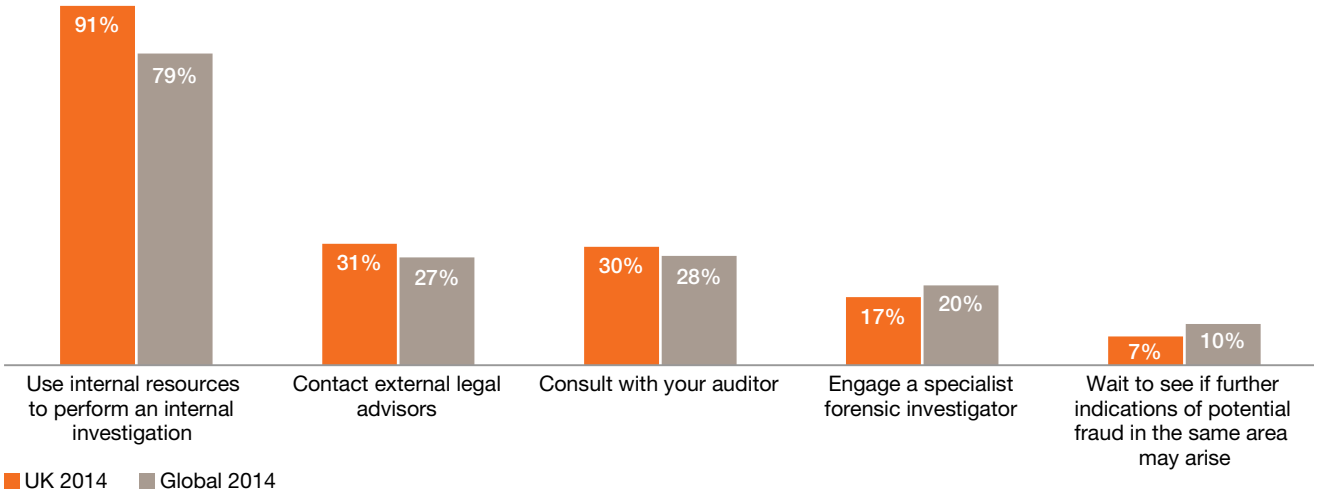


It's important however that UK organisations do not neglect the human element. A fraud is, after all, committed by a person and not a computer.

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

The Design Group 21634 (02/14)