

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.

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

Contents

3 Foreword

4 Highlights

5 Economic crime in 2014

5 The big picture

9 Two kinds of threat

15 Under the eye of enforcement

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

22 Money laundering: A special concern for financial firms

24 Competition law/Antitrust law

26 The eye of enforcement: Future expectations

28 Cybercrime: The risks of a networked world

34 Other high-impact economic crimes

34 Procurement fraud: A growing opportunity, a growing threat

36 Accounting fraud

38 Asset misappropriation

39 The fraudster: Know your adversary

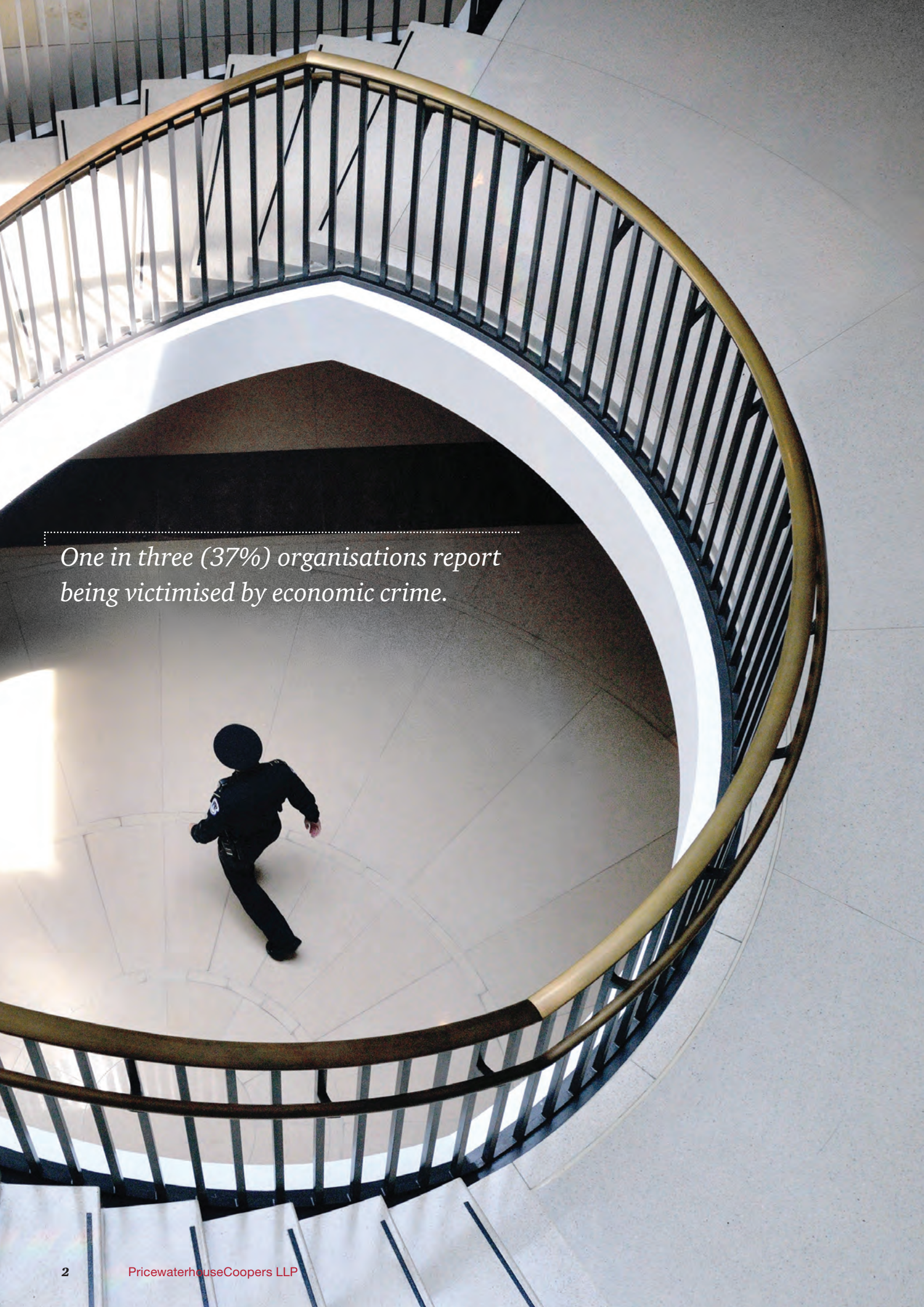
41 To catch a thief

47 Data appendix

47 Detailed regional and industry data

49 Fraudster detail

51 Methodology and acknowledgments



*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.
- 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.
- 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.
- 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

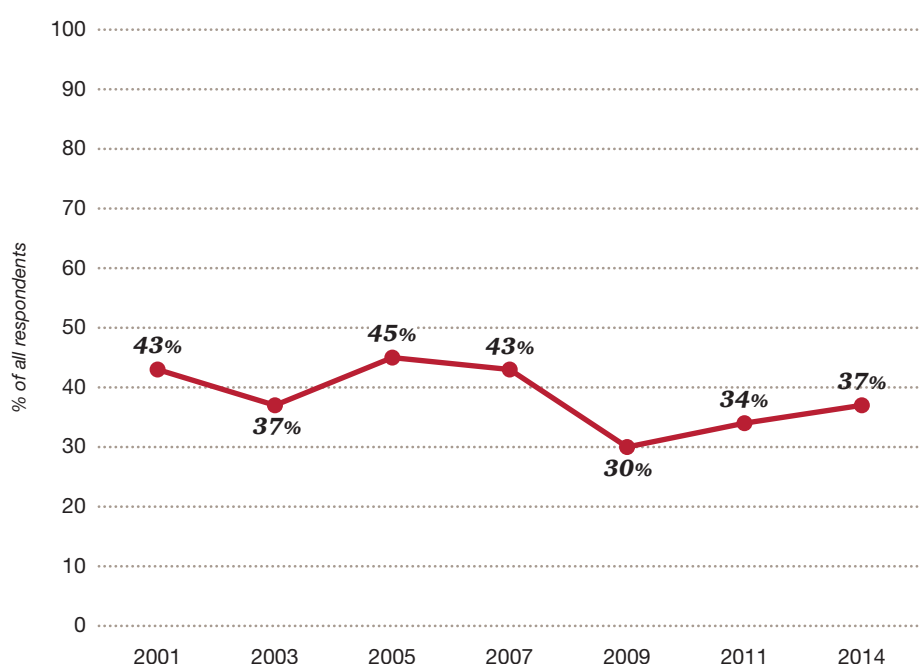
Our 2014 survey respondents included 5,128 representatives from over 95 countries around the world. More than half (54%) of our respondents were employed by organisations with more than 1,000 employees, and over one third (35%) of the survey population represented publicly traded companies.

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



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%

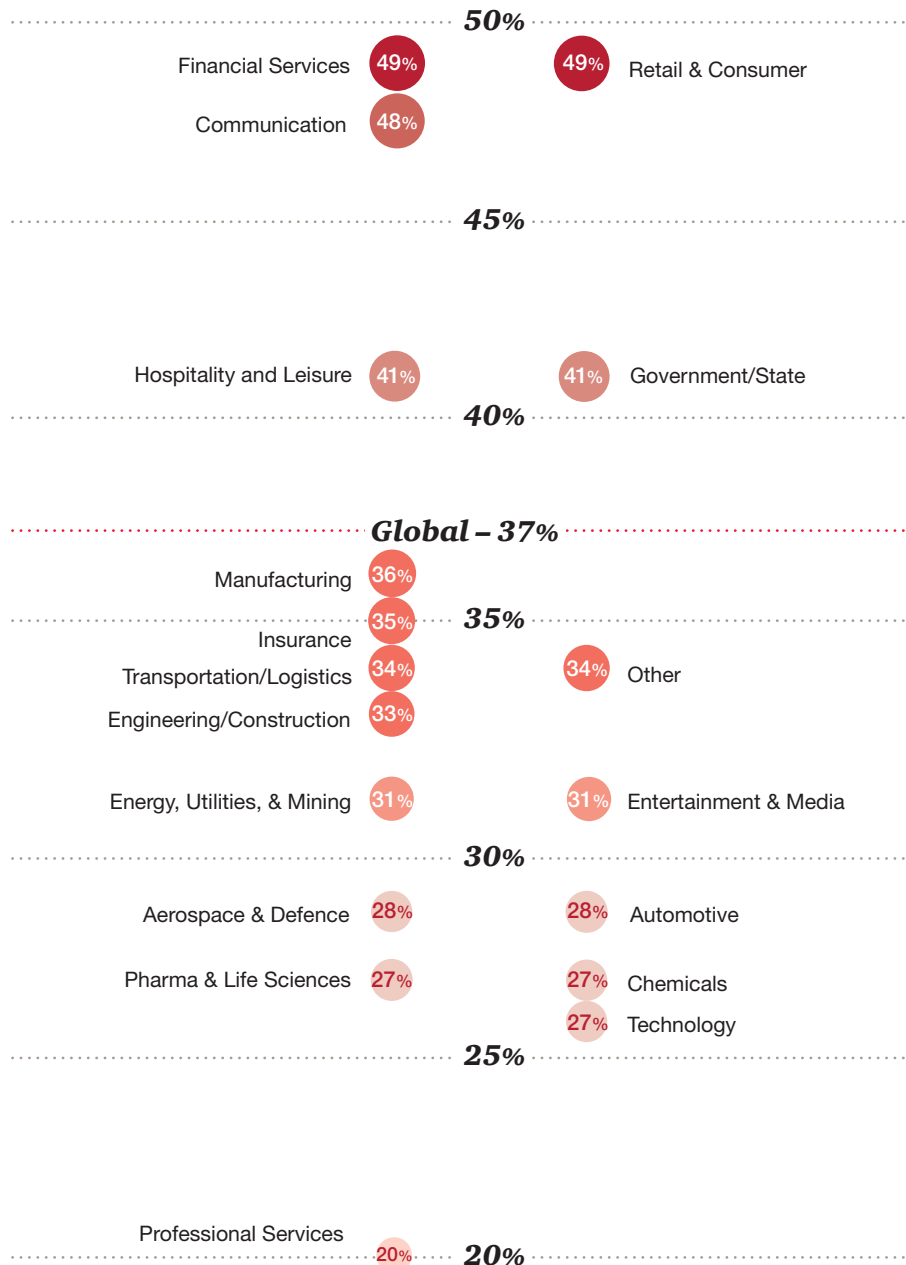
**Emerging Eight include Brazil, China, India, Indonesia, Mexico, Russia, Turkey, and South Africa*

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

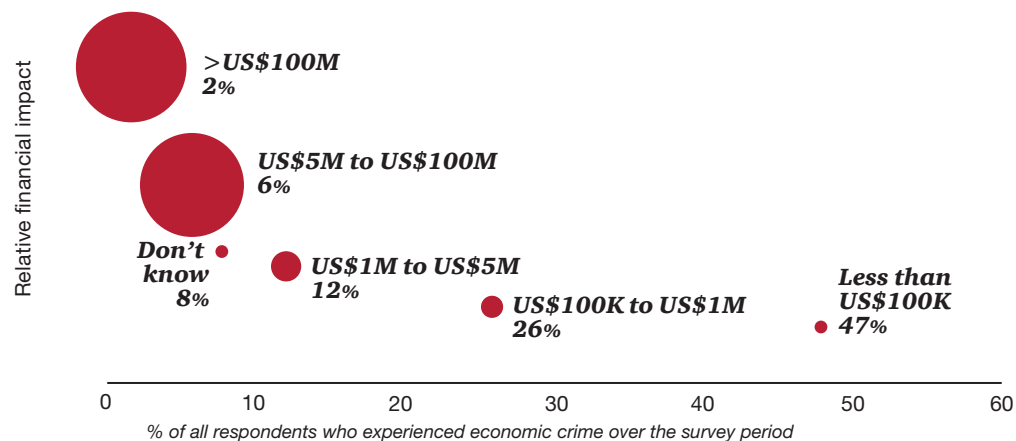
Organisations often don't grasp the true financial impact of an economic crime until after it has happened—sometimes well after. As in previous years, our survey underscores that the cost of fraud—both in financial and non-financial terms—is significant.

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.

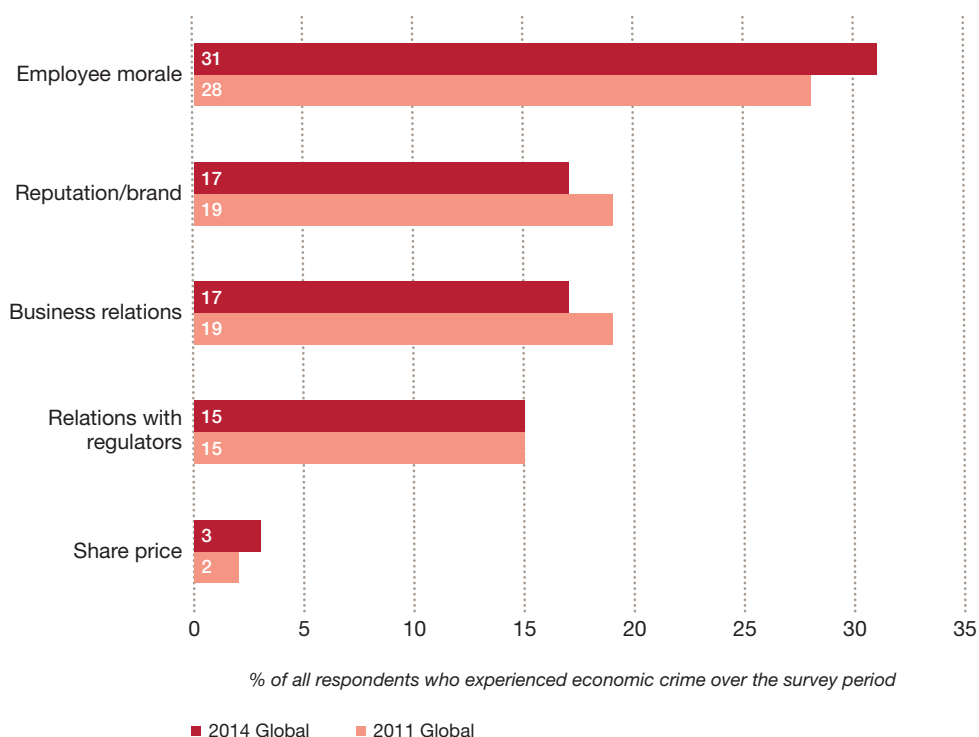
Figure 6: Relative financial impact of economic crime on organisations



Collateral damage: Hard to quantify, hard to ignore

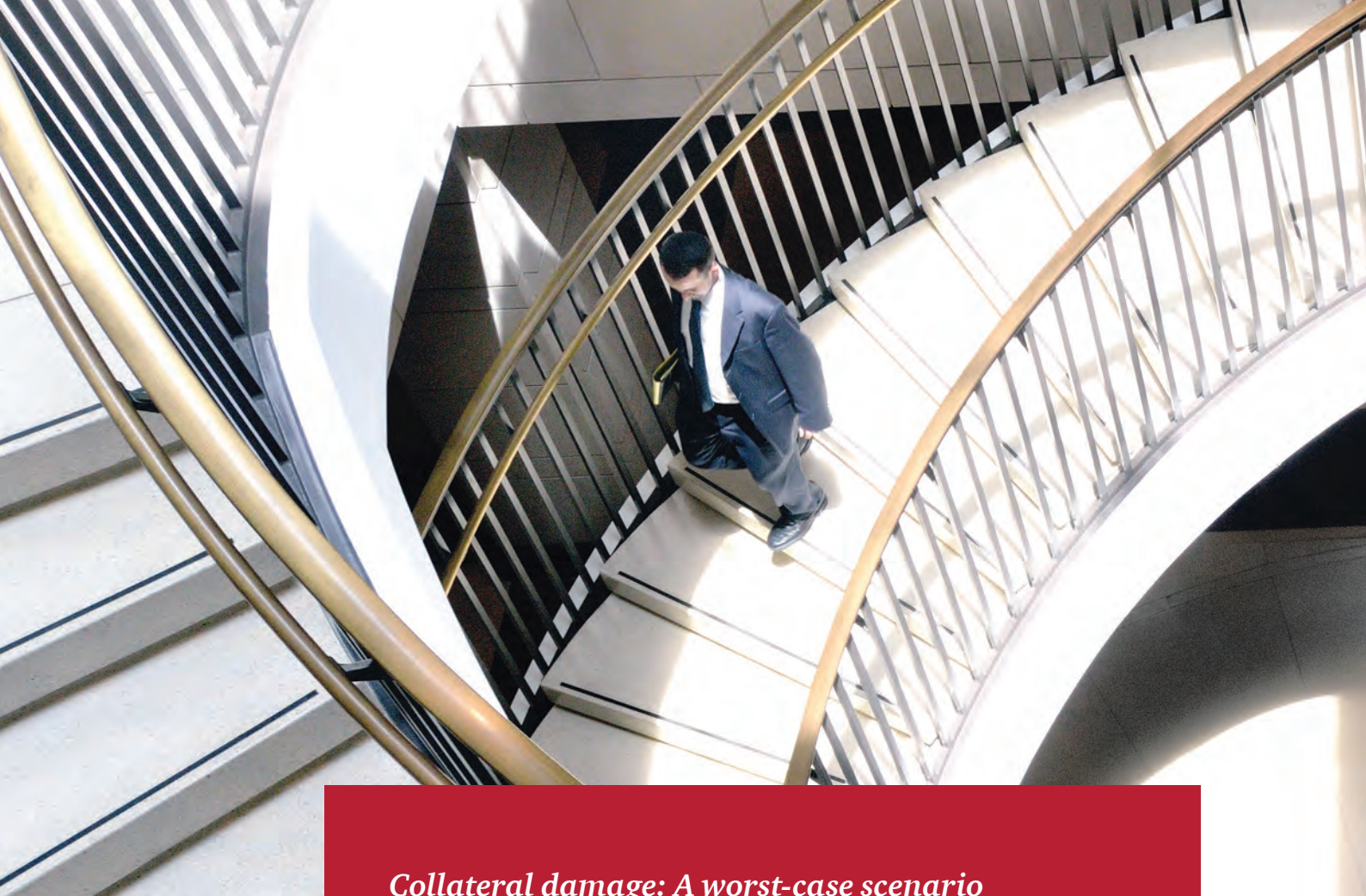
Economic loss is not the only concern that companies face when combating fraud. Our respondents pointed at damage to employee morale, corporate and brand reputation, and business relations as some of the most severe non-financial impacts of economic crime.

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.

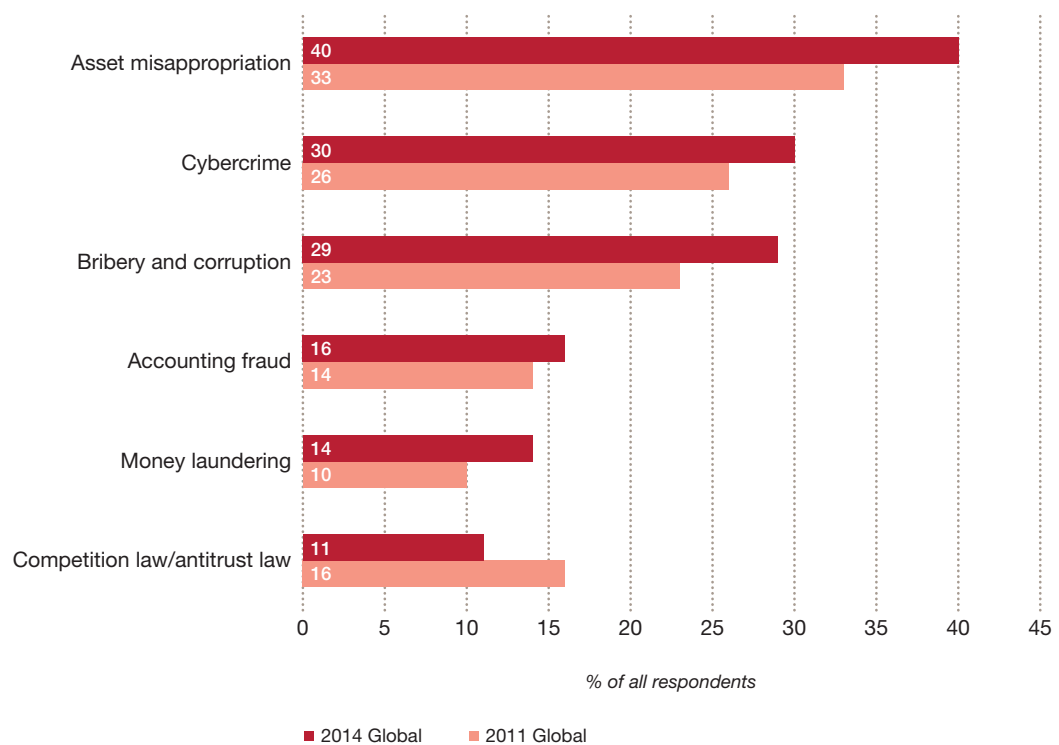
Starting with a report of a single event such as insider trading or financial statement fraud, incidents may appear compartmentalised, involving only one account, division, or customer. Still, in a competitive marketplace, there are often few reasons for customers, counterparties or partners to maintain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

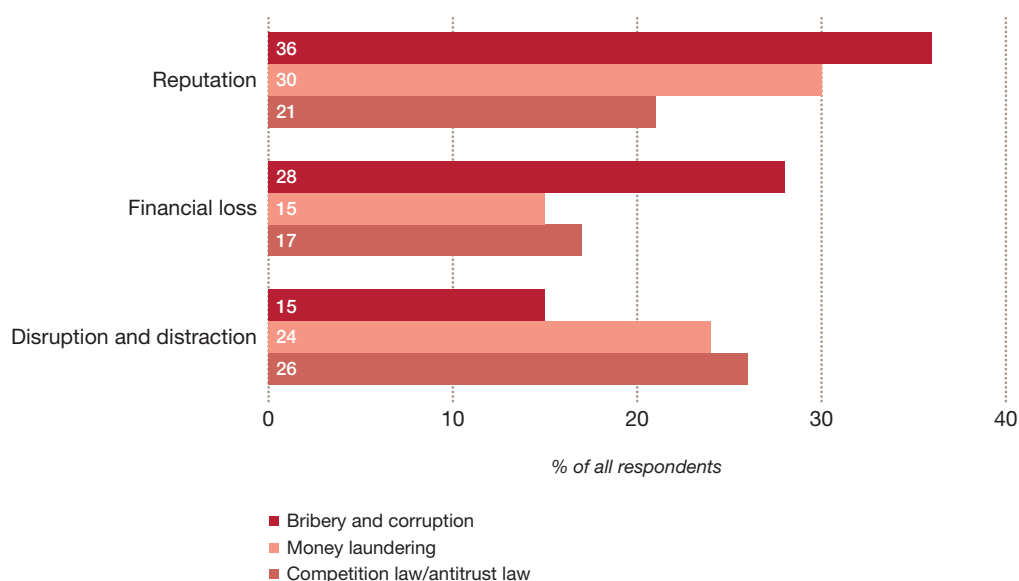
Some types of economic crimes attract significantly more attention from government enforcement agencies than others. For this reason we have decided to dedicate a section of our analysis to an important subset of economic crime—bribery and corruption, money laundering, and anticompetitive behaviour.

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

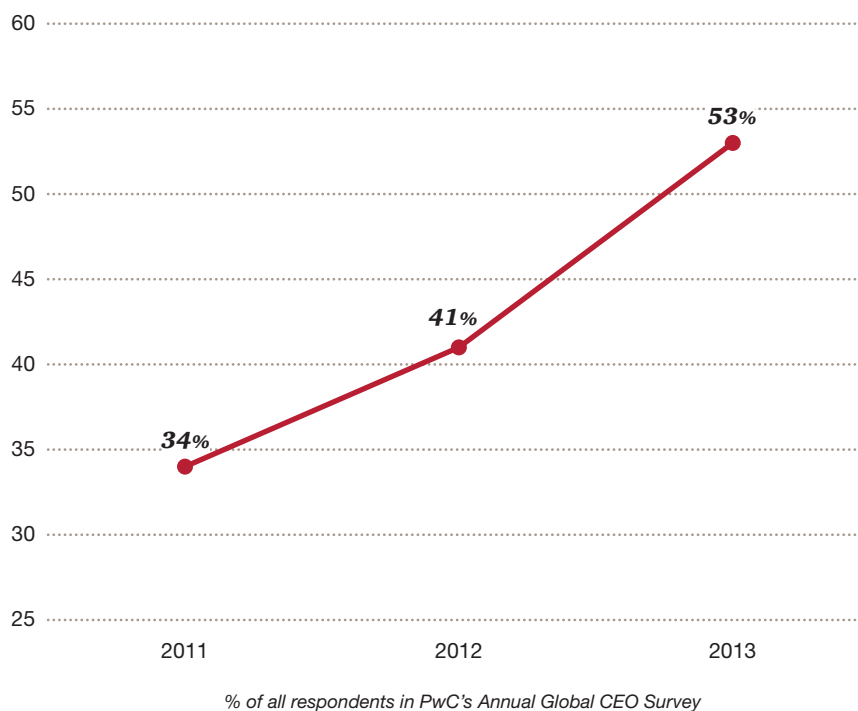


Bribery and corruption: The C-Suite gets the message

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



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.

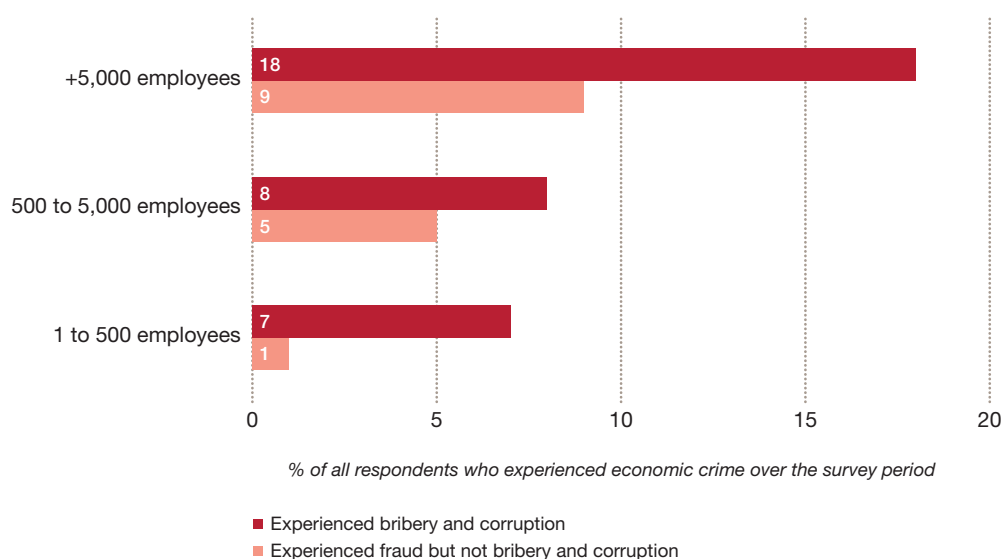
If the territory has a culture that is relatively permissive to bribery and corruption, some of these officials may be predisposed to expect or at least be open to bribes. This exerts pressure on sales and marketing staff, who have been tasked by leadership with bringing a new product to a growing market—pressure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

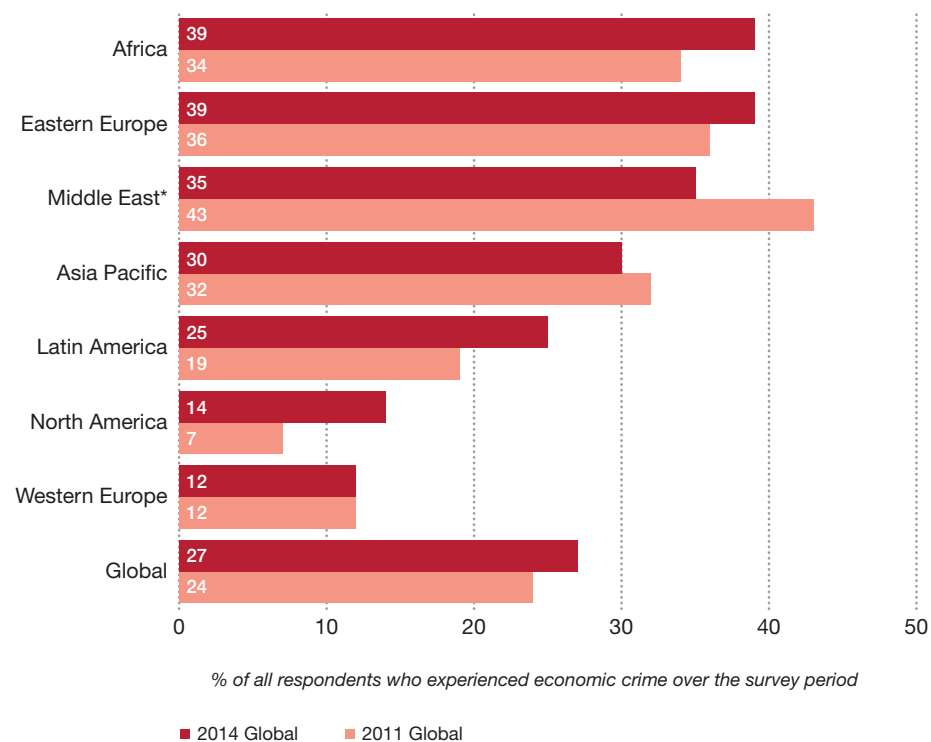
The global economy is generally on the rebound, potentially reinvigorating organisations' appetite for expansion and risk. Our survey results confirm that a large number of organisations operate in territories identified as posing a high corruption risk (50%) and/or plan to pursue opportunities in such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

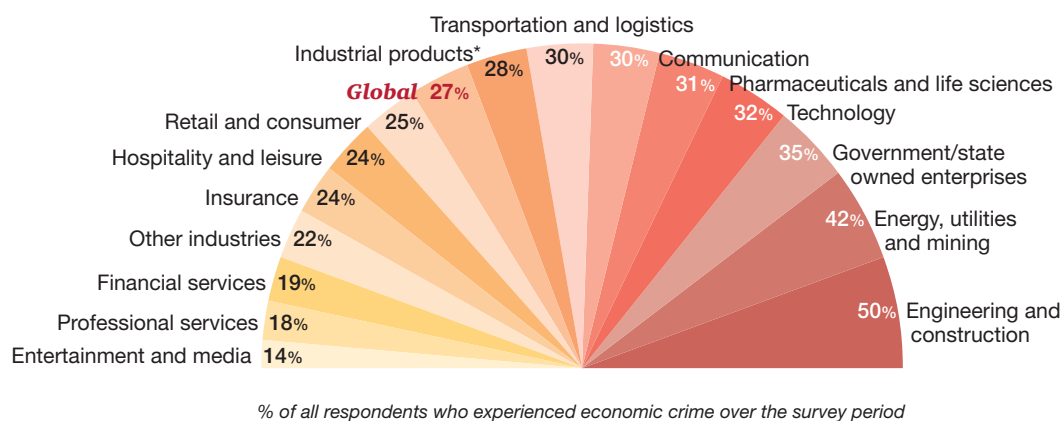
1. Respondents were asked if their organisation had operations or was pursuing operations in high risk areas, with a reference to the 2012 Transparency International Corruption Perception Index ("CPI"). The CPI is compiled annually by Transparency International, a non-profit organisation which tracks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

Figure 12: Reported bribery and corruption, by region



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

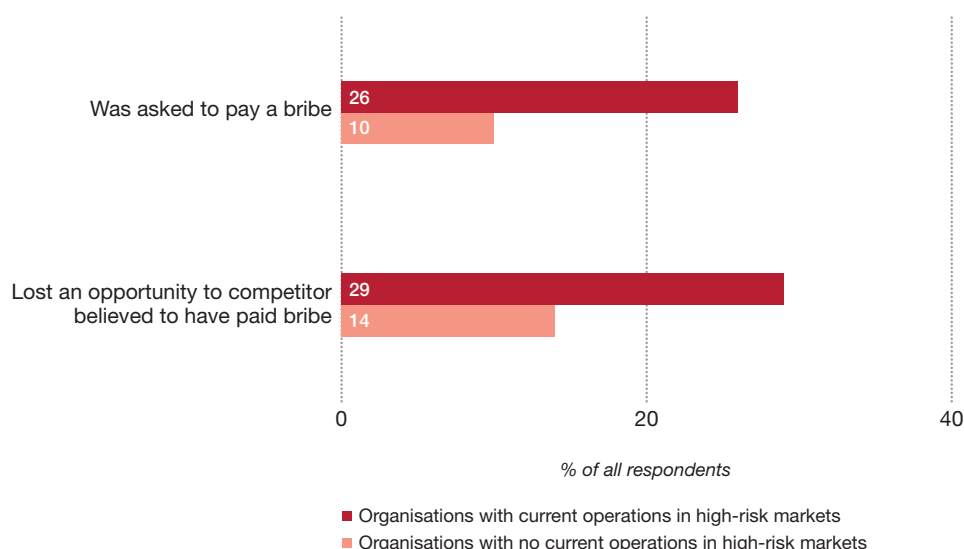
Figure 13: Reported bribery and corruption, by industry



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.

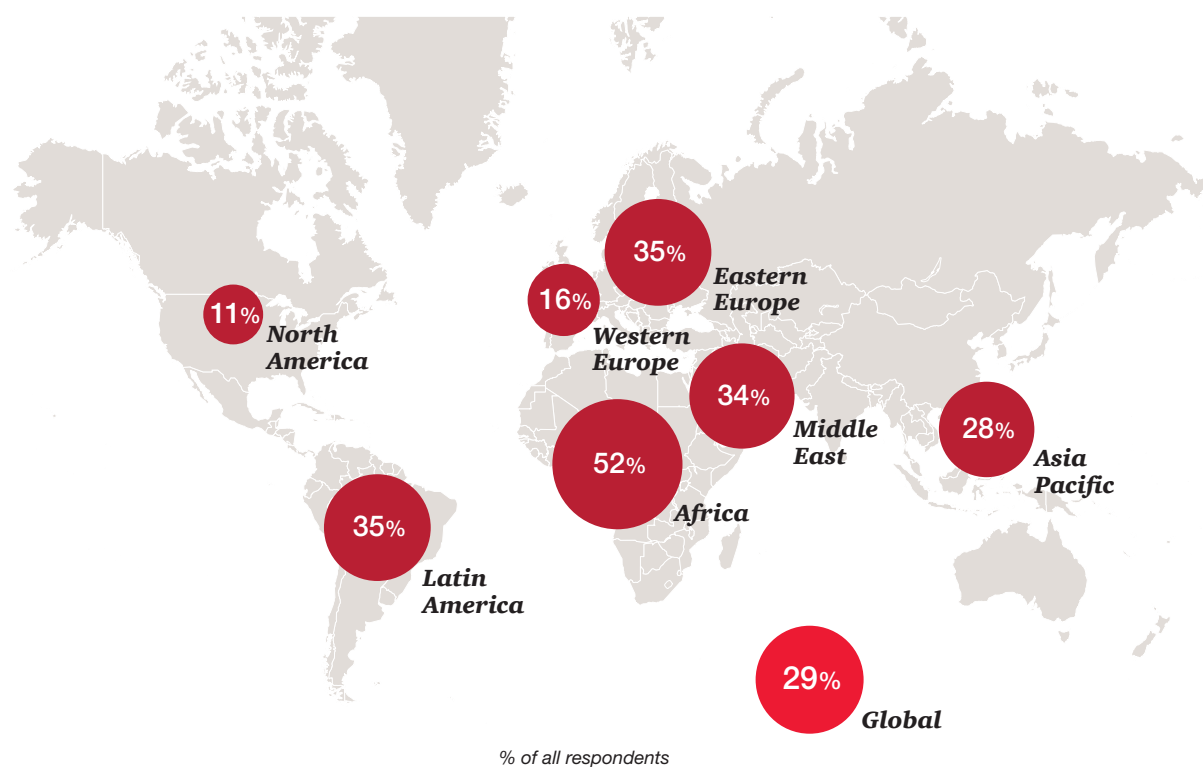
Today's perceptions, tomorrow's predictions

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.

A man in a white shirt and tie is walking down a modern staircase. He is carrying a black suitcase in his right hand and a dark jacket in his left arm. The staircase has a glass railing and a metal handrail. The background shows a large, modern building with a glass facade.

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.

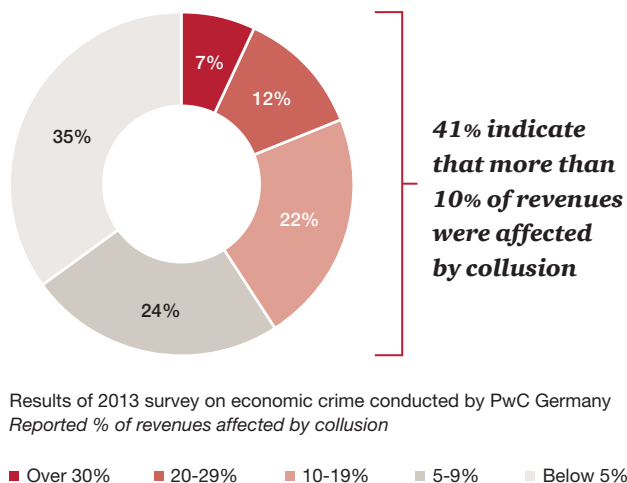
So operating in environments that pose a systemic threat of money laundering to the business processes of financial institutions is a unique challenge. Not only are money laundering schemes numerous and sophisticated, but they create a potentially significant tension between the equally laudable goals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



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 widespread allegations of collusion among banks in reporting LIBOR, the benchmark London Interbank Offered Rate.

European Commission officials became the latest global regulators to take action against multiple global financial institutions after the discovery of widespread rigging of LIBOR—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.

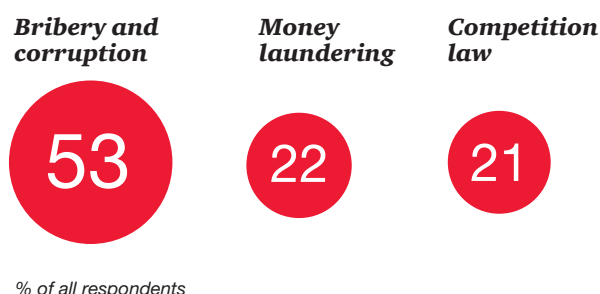
Many observers see the LIBOR case as pointing to a more aggressive future stance by European antitrust authorities in investigating alleged anticompetitive behaviours in any industry.

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

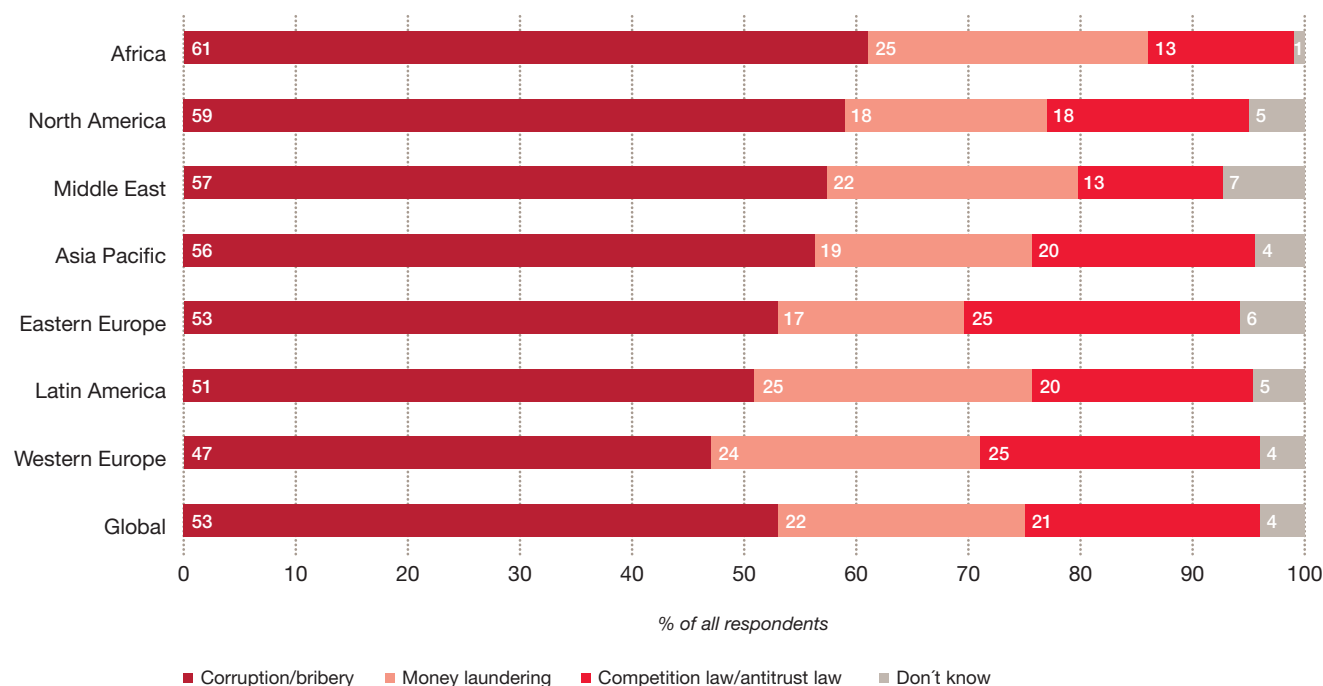


% of all respondents

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.

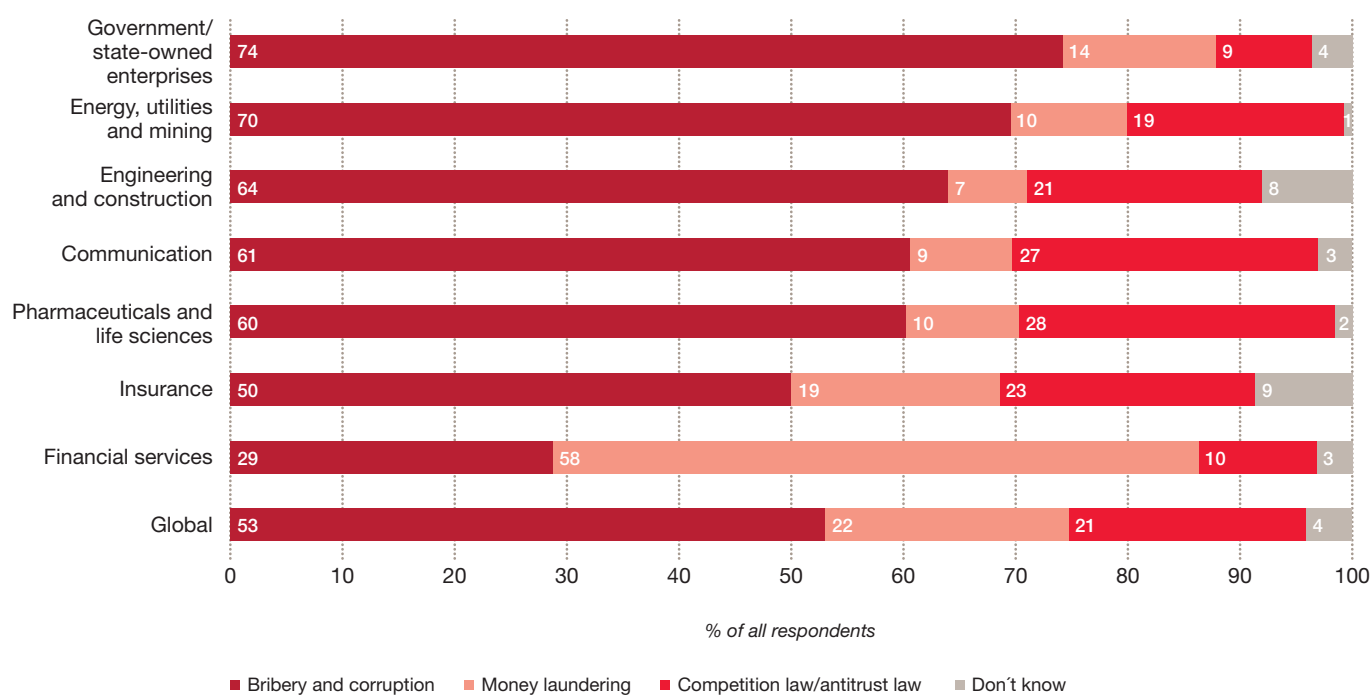
Figure 18: Perceived greatest relative economic crime risk, by region



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.

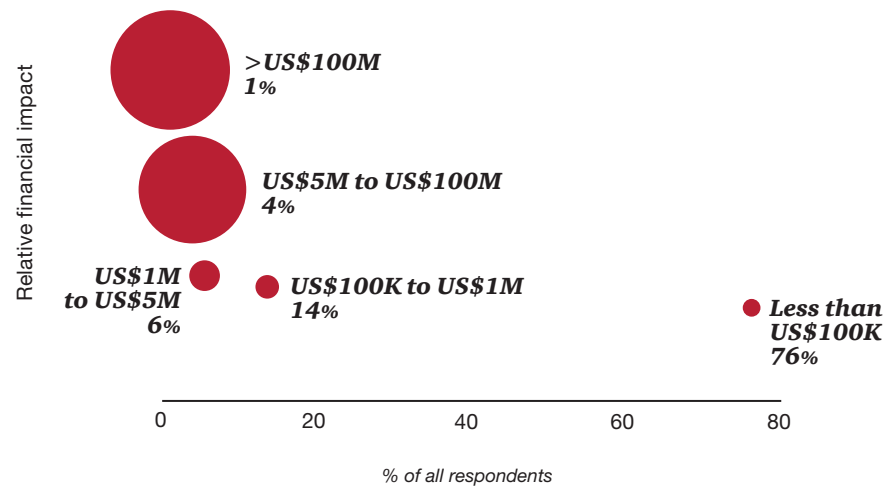
Cybercrime: The risks of a networked world

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

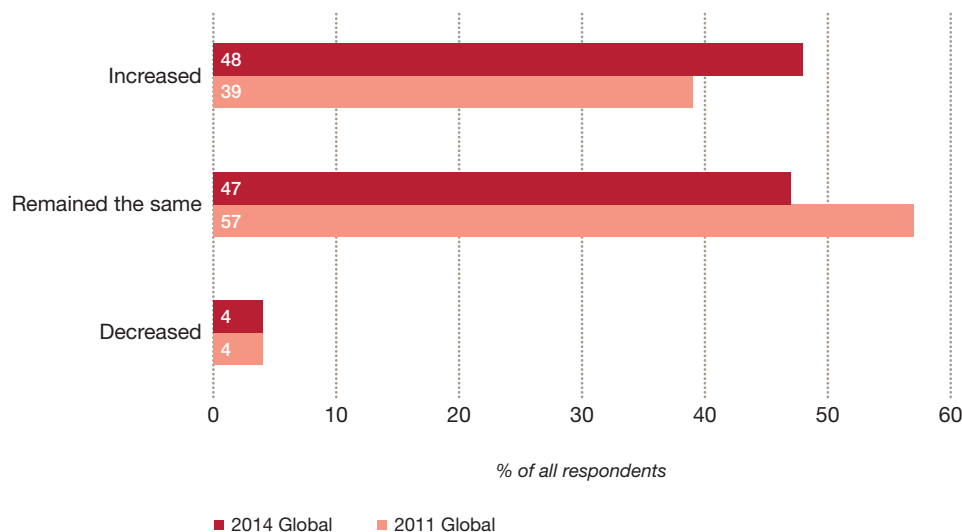


Our 2011 Global Economic Crime Survey was the first in our series to highlight cybercrime as a high-level threat to organisations. This year's survey confirms the significant, continuing impact of this crime on business, with now one in four of respondents reporting they have experienced a cybercrime—and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

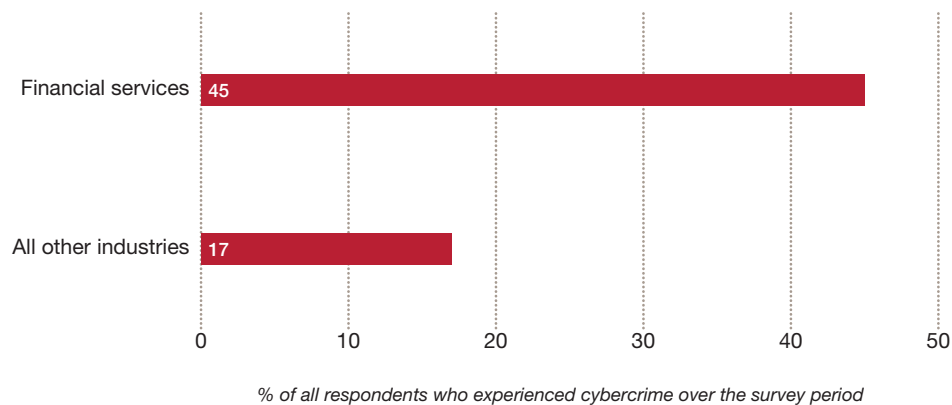
The bottom line is that much of the damage caused by these kinds of attacks is not disclosed, either because it is not known, because it is difficult to quantify, or because it is not shared. Naturally, this poses risks in a global business ecosystem that is increasingly reliant on both technology and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



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.

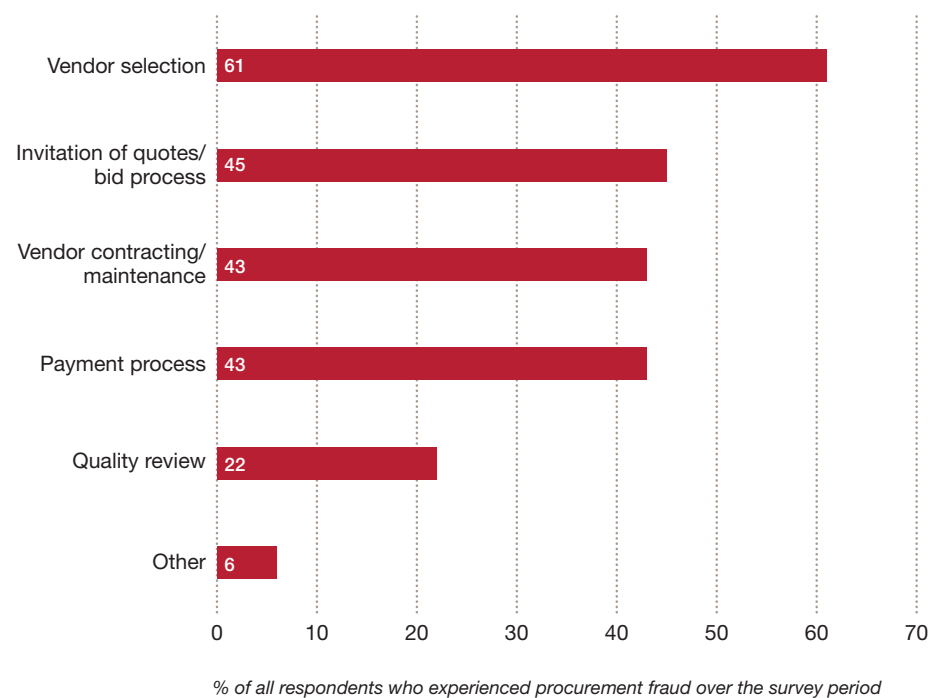
First, there has been an increase in more-competitive public tender processes from governments and state-owned businesses, unleashing the possibility of fraudulent activity on the part of agents and other third parties. No doubt, in past surveys procurement-related kickbacks, bid-rigging, or similar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



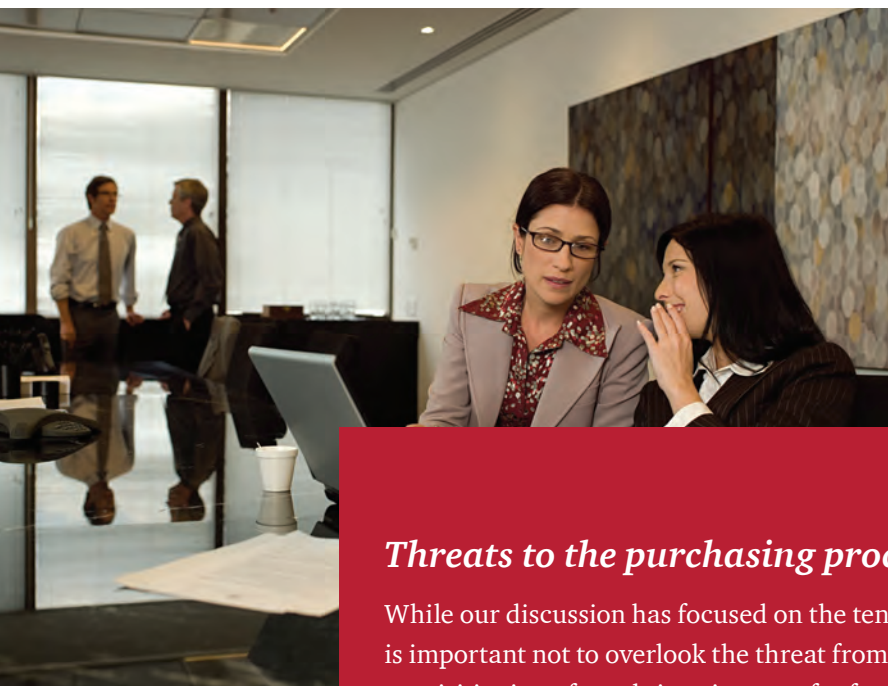
It's worth noting that procurement frauds are not only investigated and enforced at the sovereign level. In recent years, the World Bank has taken a more active stance against fraud in general, with 79 cases opened in 2012. As the institution commonly funds infrastructure projects in developing countries,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

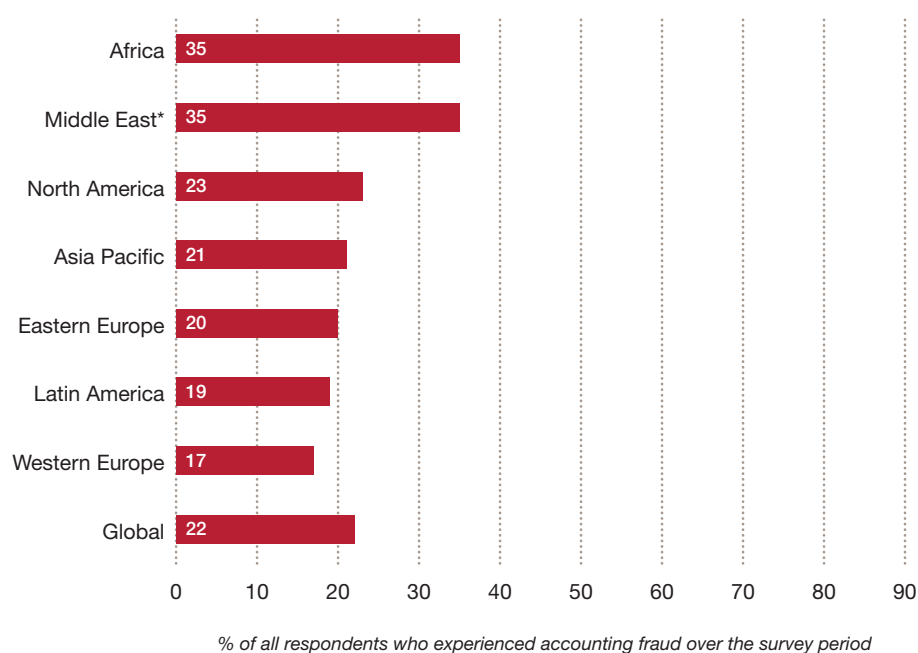
Financial statements are a fundamental barometer of a business—and a traditional starting point for analyses relating to credit decisions, contract awards, and capital raising in public markets. Accounting fraud—which includes misleading or falsely prepared financial statements—can dupe banks, lessors,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



*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.

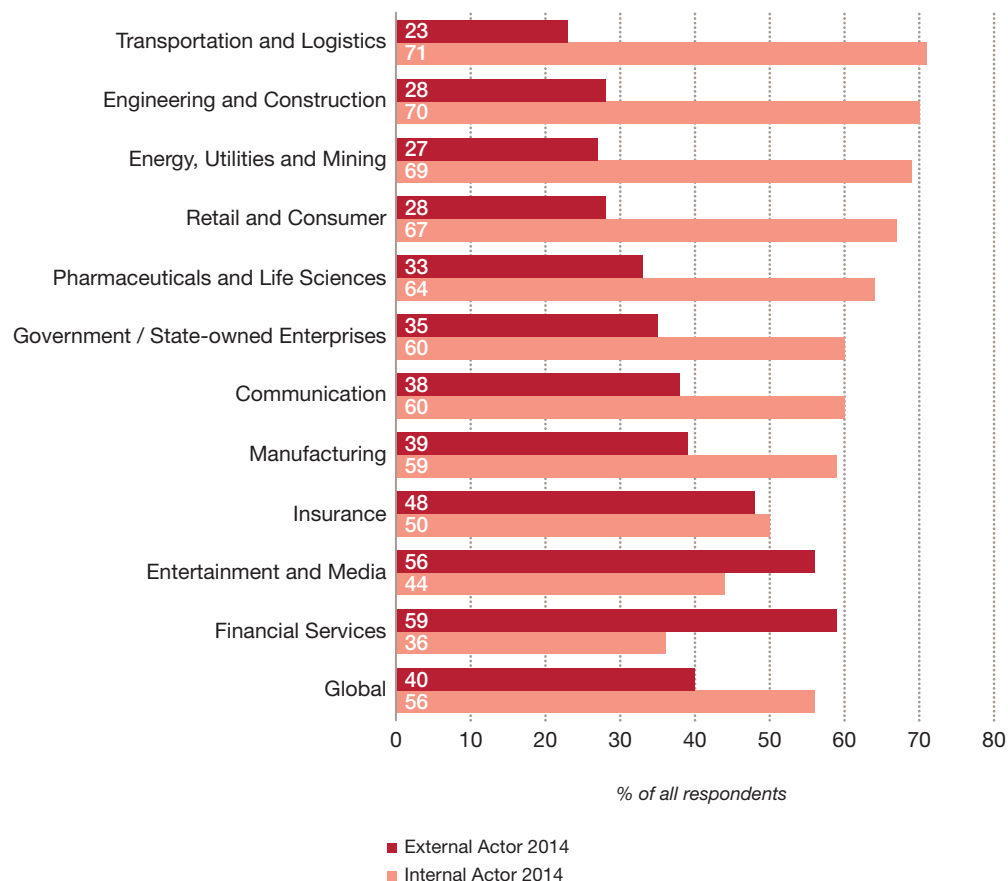
But dig a little into the data, and some sharp contrasts begin to emerge at the sector level.

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.

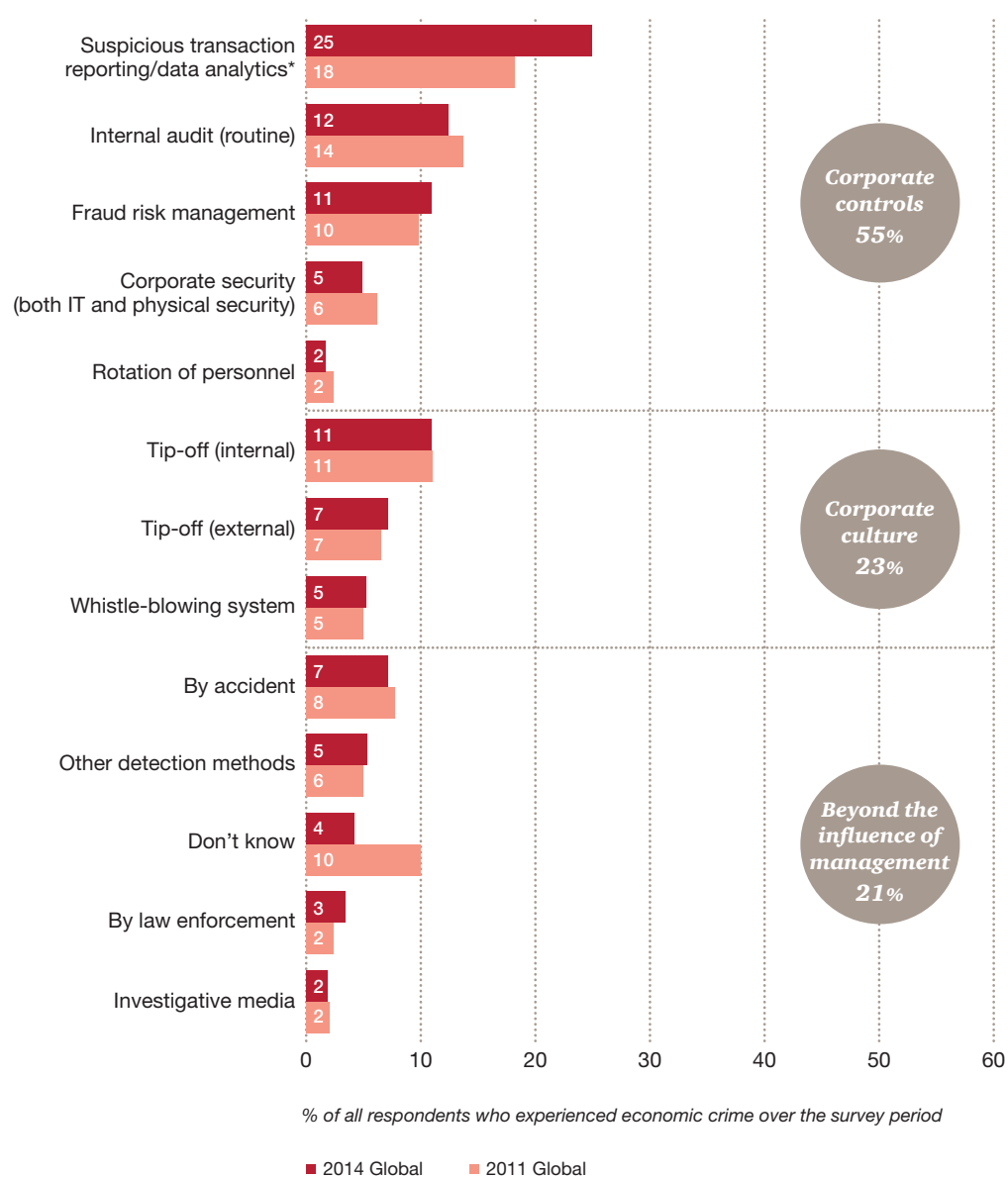
Presumably, there is a silver lining to having most of one’s fraud losses attributable to internal players—you have a better opportunity to mitigate these risks through improved internal policies, processes and controls when the fraudster is someone employed by the company. Mitigating the actions of 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	34	46	50	55
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

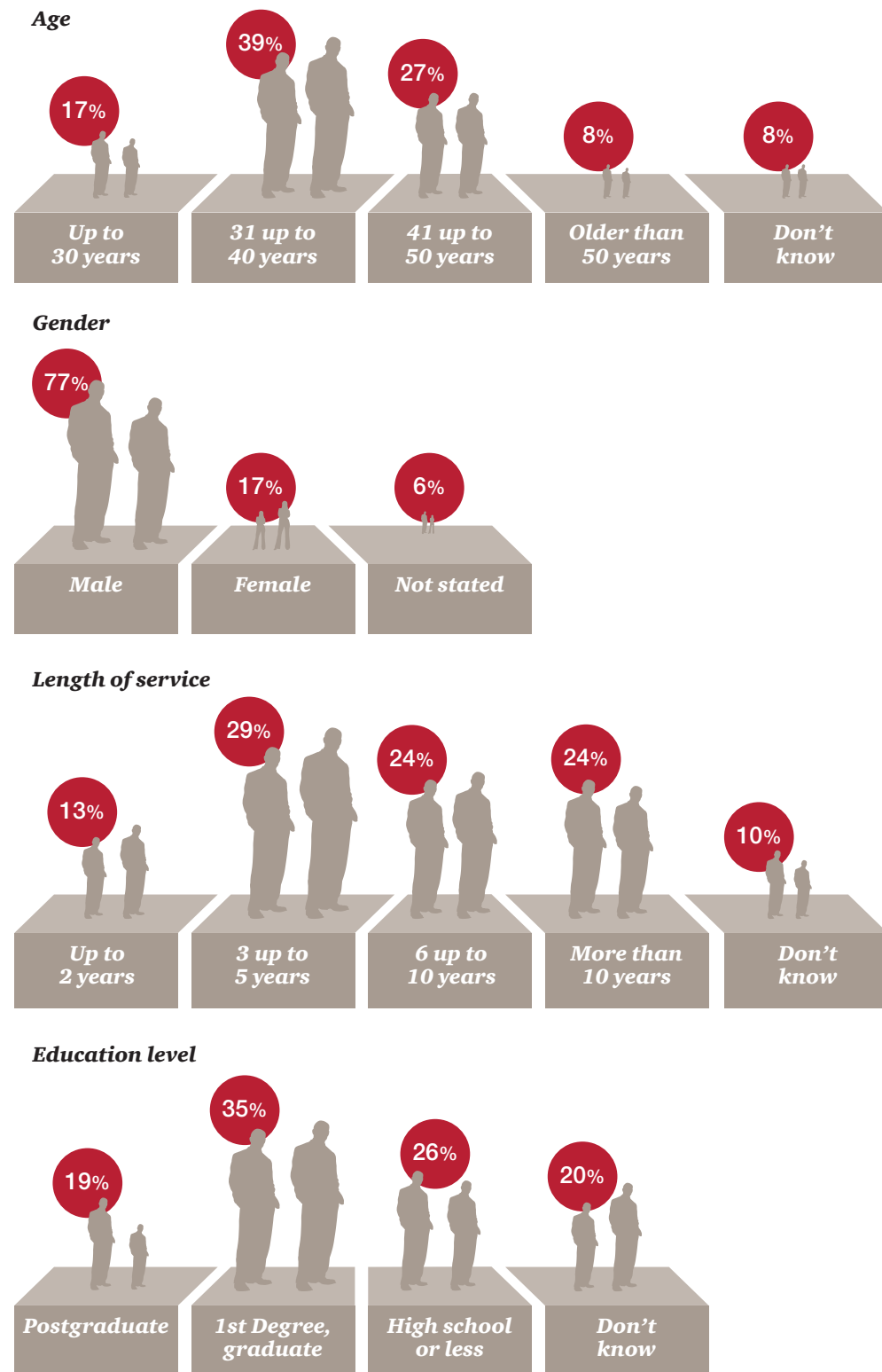
Practitioners commonly refer to a “Fraud Triangle”—the three elements that are often present when a perpetrator commits fraud: pressure, opportunity and rationalisation.

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

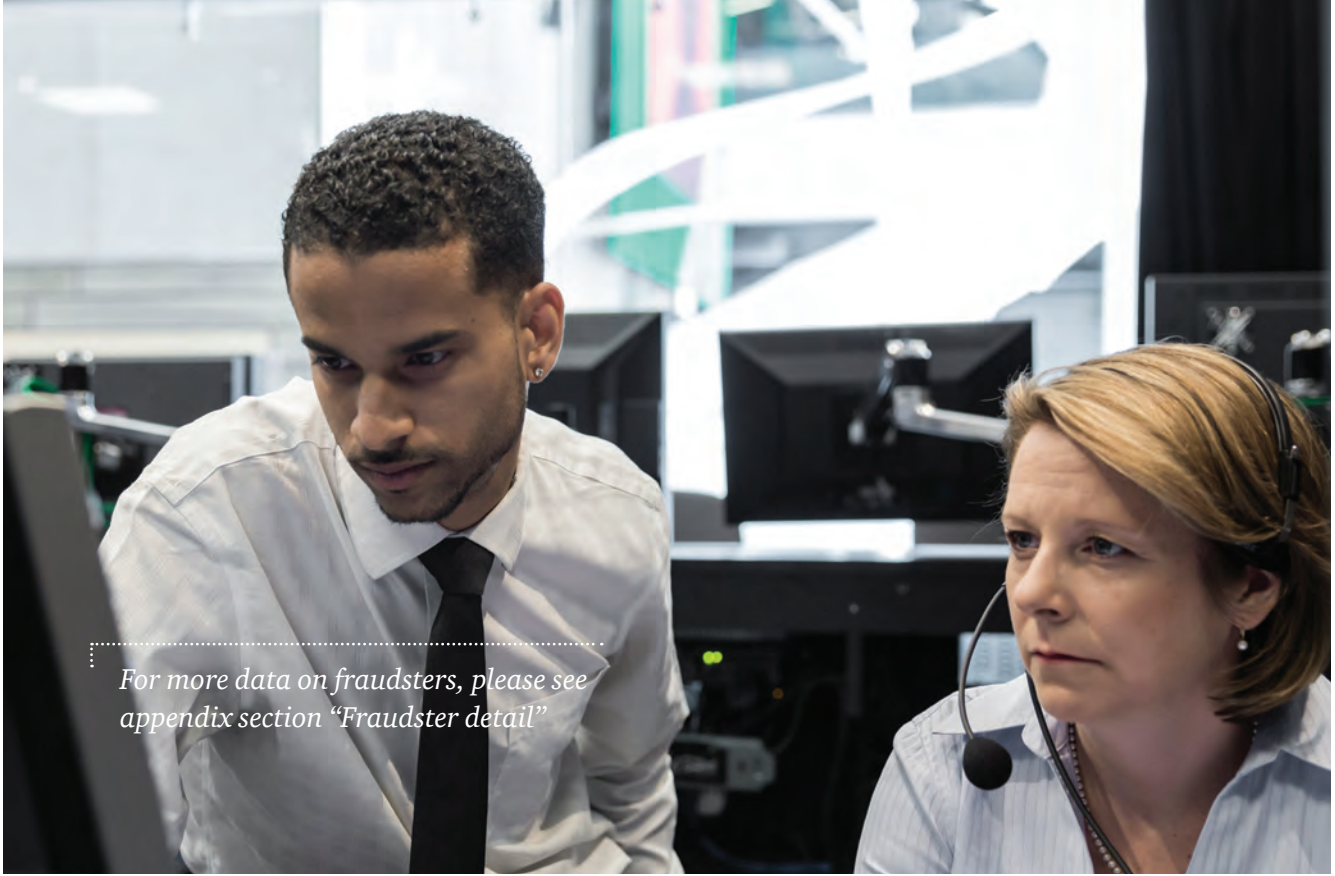
● 2014 Global

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.

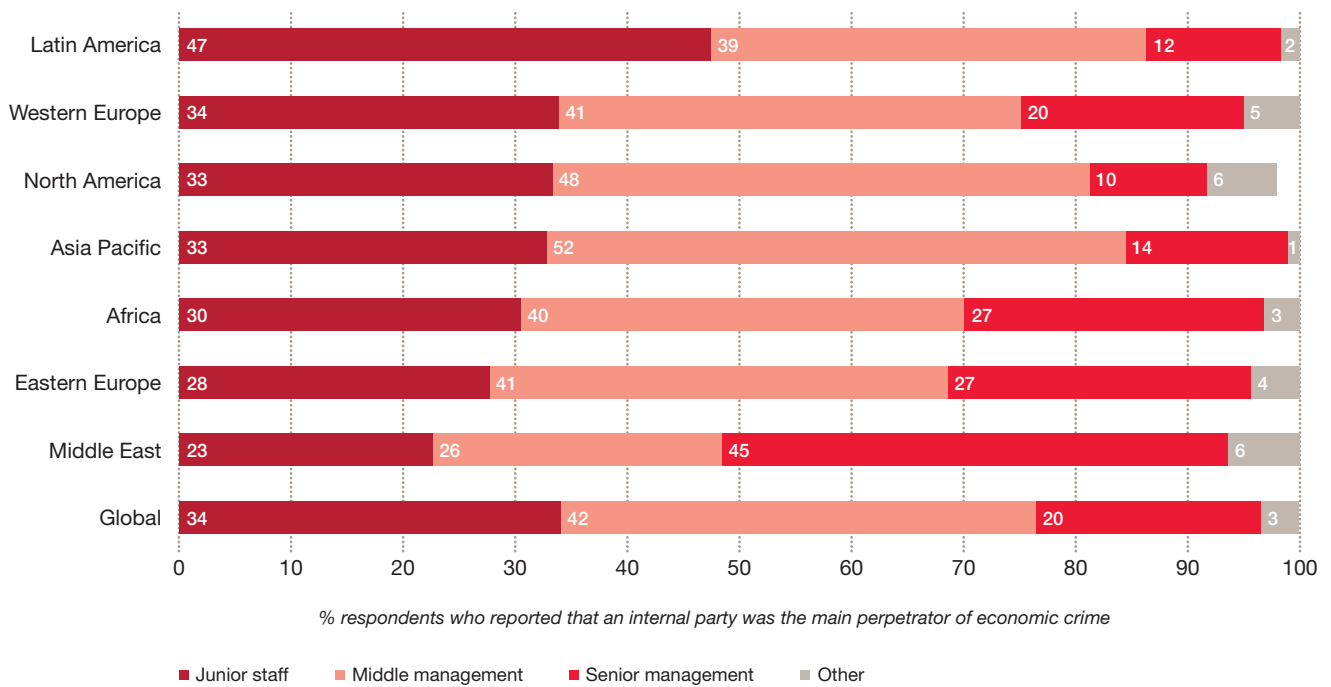
Consider the senior private banker who assures the wire transfer operators that he'll handle the client call-back procedure to confirm instructions for payments. Or the boss who says she'll take care of getting the documentation needed to support the payment. Or even the division manager who budgets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

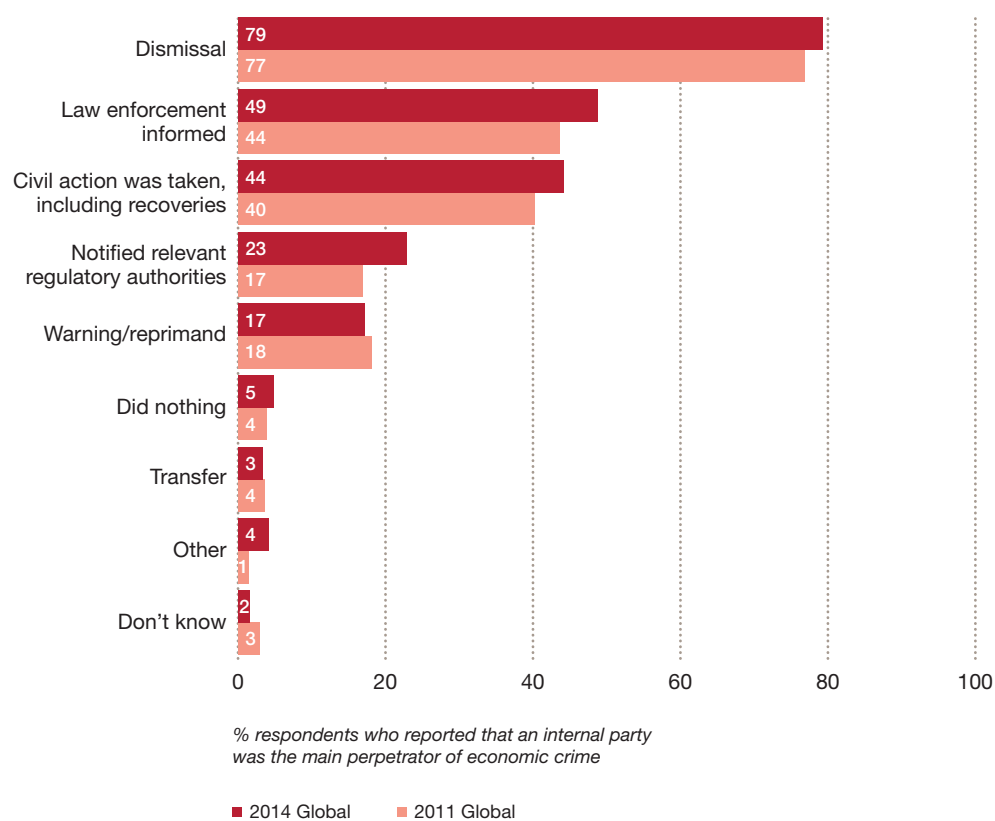


Figure 34: Profile of external perpetrator

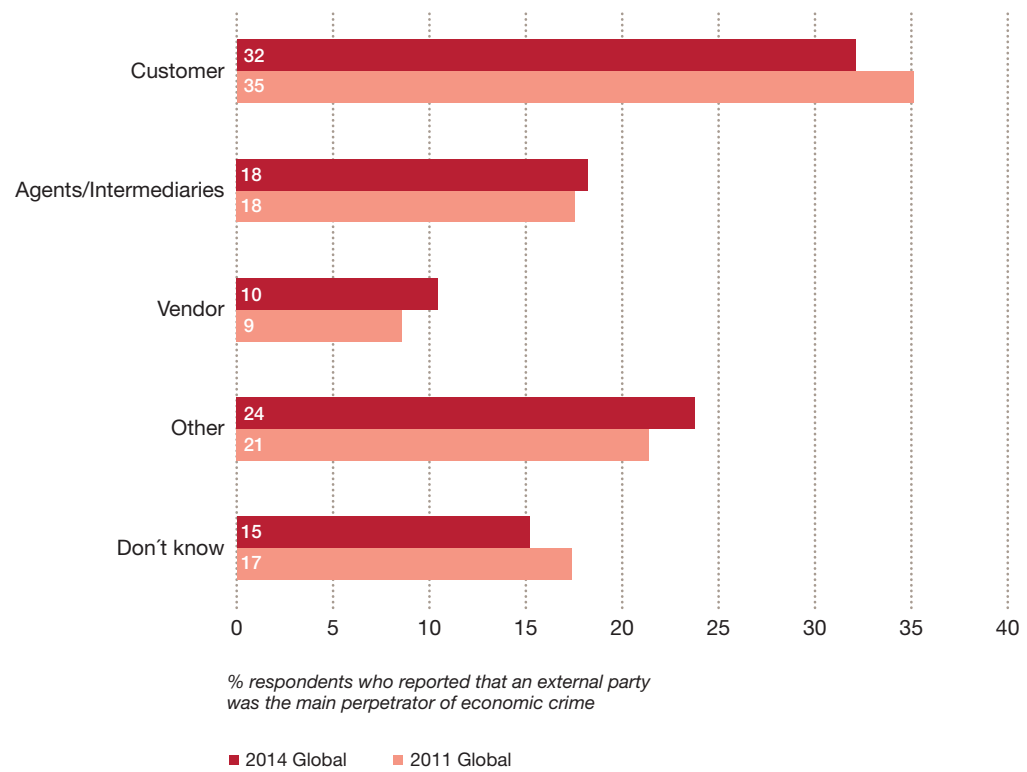
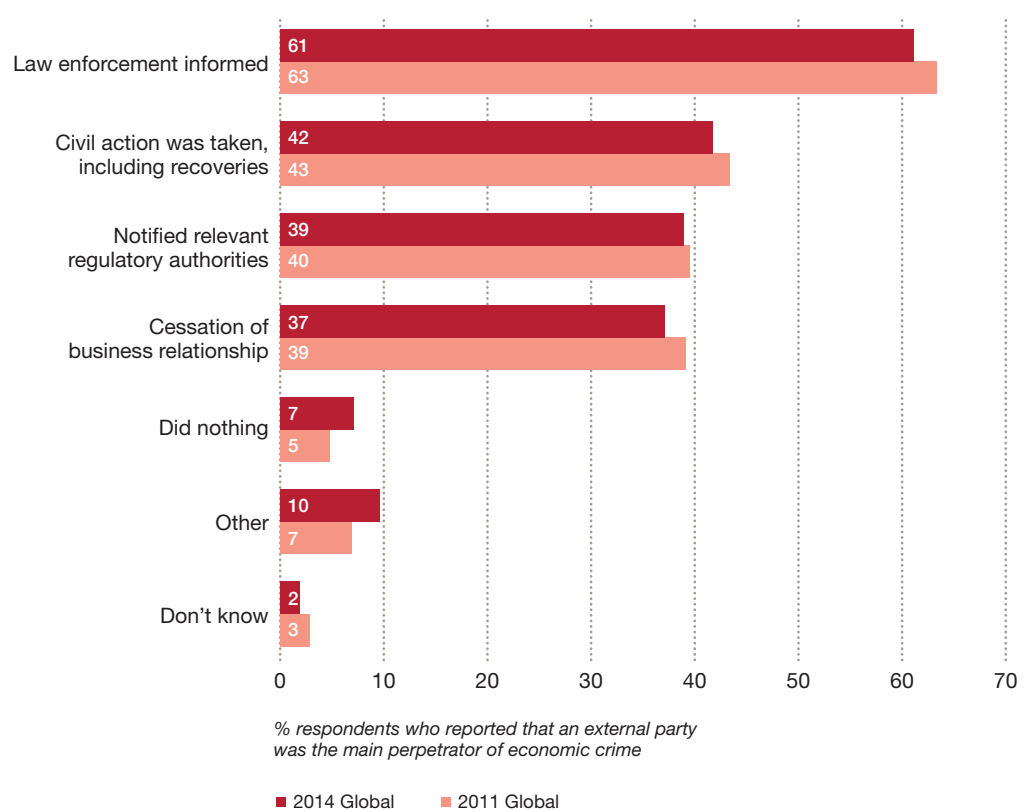


Figure 35: Actions taken against external perpetrator



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	Territory	2014	2011
Asia Pacific	906	669	Middle East²	232	128
Australia	79	79	Unspecified Middle East Countries	N/A	127
China including Hong Kong ¹	N/A	22	Bahrain	2	N/A
Hong Kong / Macau	116	N/A	Egypt	7	N/A
China (excluding Hong Kong)	85	N/A	Jordan	9	N/A
India	115	106	Lebanon	8	N/A
Indonesia	4	84	Oman	1	N/A
Japan	75	73	Qatar	12	N/A
Malaysia	110	93	Saudi Arabia	74	N/A
New Zealand	82	93	Sudan ³	1	1
Papua New Guinea	81	1	Syria	1	N/A
Singapore	82	18	UAE	117	N/A
Taiwan	0	2	Western Europe	1,555	1,317
Thailand	76	79	Andorra	0	1
Vietnam	1	19	Austria	6	8
Africa	604	259	Belgium	68	84
Algeria	2	0	Cyprus	88	5
Angola	22	1	Denmark	118	116
Botswana	5	1	Finland	34	61
Cameroon	6	0	France	131	112
Democratic Republic of Congo	1	0	Germany ⁴	10	38
Ghana	3	29	Greece	11	92
Guinea	2	0	Ireland	78	80
Ivory Coast	3	0	Israel	31	-
Kenya	124	91	Italy	101	127
Lesotho	1	0	Luxembourg	12	3
Liberia	0	5	Netherlands	75	41
Malawi	1	0	Norway	92	67
Morocco	17	0	Portugal	75	0
Mozambique	4	0	Spain	79	85
Namibia	26	2	Sweden	91	79
Nigeria	82	3	Switzerland	83	140
Sierra Leone	1	0	UK ⁵	372	178
South Africa	134	123	North America	215	209
Swaziland	4	1	Canada	100	53
Tanzania	12	0	USA	115	156
Tunisia	17	2			
Uganda	12	0			
Zambia	83	1			
Zimbabwe	42	0			

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	Territory	2014	2011
Central & Eastern Europe	877	804	Latin America	711	483
Bulgaria	79	58	Argentina	82	77
Croatia	0	1	Bahamas	2	0
Czech Republic	94	84	Barbados	1	0
Estonia	0	1	Bolivia	0	3
Hungary	91	85	Brazil	132	115
Kazakhstan	1	0	Chile	75	1
Lithuania	1	7	Colombia	1	1
Moldavia	0	1	Cuba	2	0
Montenegro	0	1	Dominican Republic	1	0
Poland	94	79	Ecuador	22	11
Romania	77	76	Mexico	211	174
Russia	111	126	Peru	82	17
Serbia	52	14	Venezuela	100	84
Slovakia	76	84			
Slovenia	33	48			
Turkey	78	55			
Ukraine	90	84			
			No primary country specified	28	8
			Total	5,128	3,877

Figure 37: Participating industry groups

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

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.

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.

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.

Contacts and contributors

Survey Leadership and Editorial Board

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

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

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

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

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

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

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

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

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

Survey Management Team

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

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

Forensic Services Leaders

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

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

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

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

Survey Marketing Team

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

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

www.pwc.com/crimesurvey

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

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

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

Designed by US Studio CMD NY-14-0348