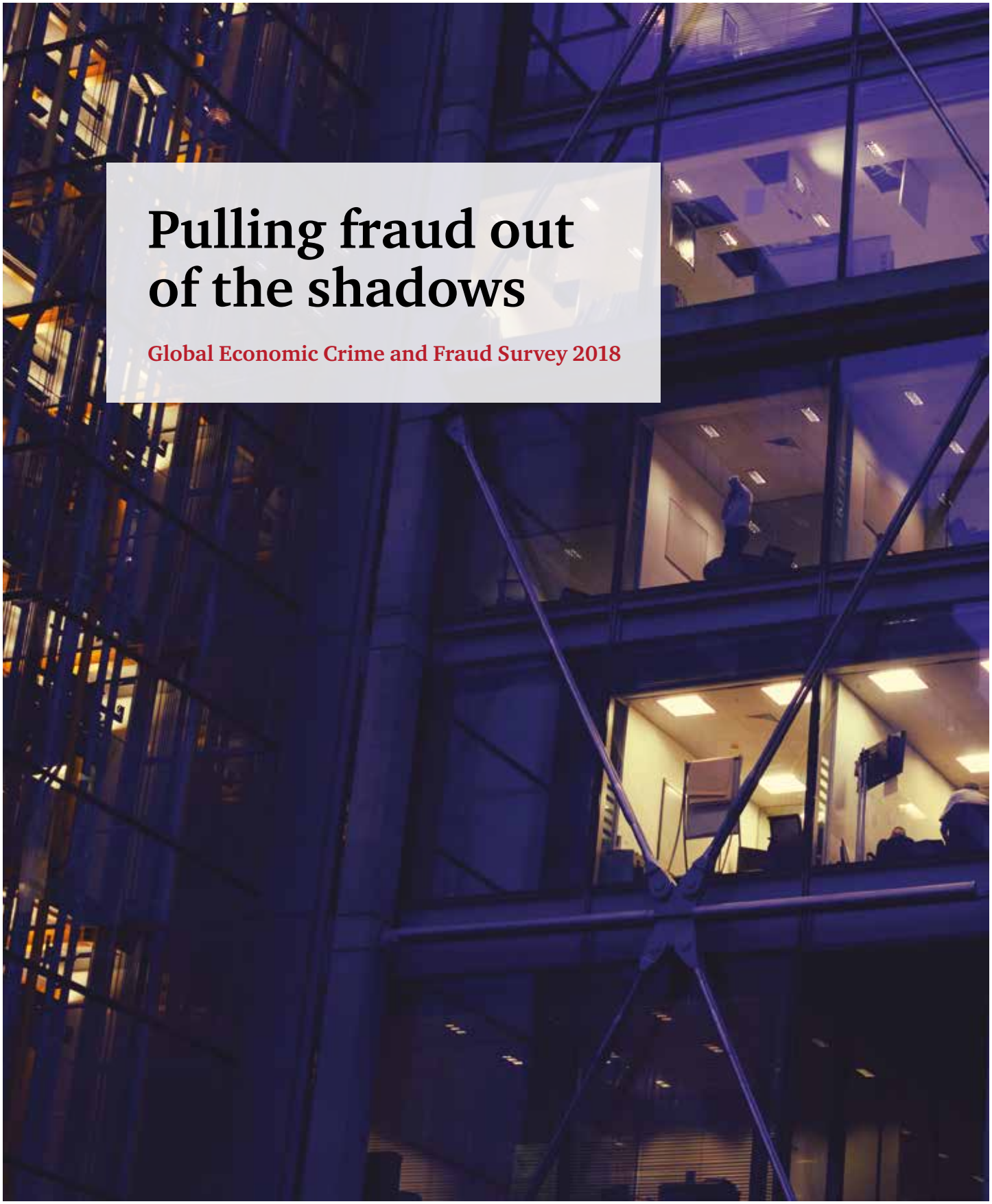


Pulling fraud out of the shadows

Global Economic Crime and Fraud Survey 2018

pwc

www.pwc.com/fraudsurvey

Executive Summary

Didier Lavion
Principal, Global Economic Crime and Fraud Survey Leader, PwC US

In PwC's 2018 Global Economic Crime and Fraud Survey, only 49% of global organisations said they'd been a victim of fraud and economic crime. However, we know this number should be much higher. So, what about the other 51%?

The reality is, too few companies are fully aware of the fraud risks they face. That's why this year's Global Economic Crime and Fraud Survey, gathering valuable data from more than 7,200 respondents across 123 different territories, aims to pull fraud out from the shadows – and shed much-needed light on some of the most important strategic challenges confronting every organisation.

The biggest competitor you didn't know you had

Today, fighting fraud has moved front and centre to become a core business issue. Long gone are the days when it was viewed as an isolated incident of bad behaviour, a costly nuisance, or a mere compliance issue. That's because the scale and impact of fraud has grown so significantly in today's digitally enabled world. Indeed, it can almost be seen as a big business in its own right – one that is tech-enabled, innovative, opportunistic and pervasive. Think of it as the biggest competitor you didn't know you had.

It's not hard to see how we got here. On the one hand, technology has advanced in leaps and bounds, helping fraudsters become more strategic in their goals and more sophisticated in their methods. On the other hand, regulatory regimes in much of the world have become far more robust, with enforcement intensifying, often in cross-border cooperation. Moreover, in the face of well-publicised corruption and other corporate scandals, public expectations around the world are converging around common standards of transparency and accountability.

More and more companies, organisations and nation states are now recognising that corruption and fraud are holding them back from competing on the global stage – and have simply become too costly to ignore.

A perfect storm of risks

In this era of unparalleled public scrutiny, today's organisations face a perfect storm of fraud-related risks – internal, external, regulatory and reputational. The time is therefore right for them to adopt a new, more holistic view of fraud. One that recognises the true shape of the threat: not merely a cost of doing business, but a shadow industry which can impact every territory, every sector and every function. Since it hides in the shadows, a lack of fraud-awareness within an organisation is highly dangerous.

So, the important question is not: is your organisation the victim of fraud? Rather it's: are you aware of how fraud is touching your organisation? Are you fighting it blindfolded, or with eyes wide open?

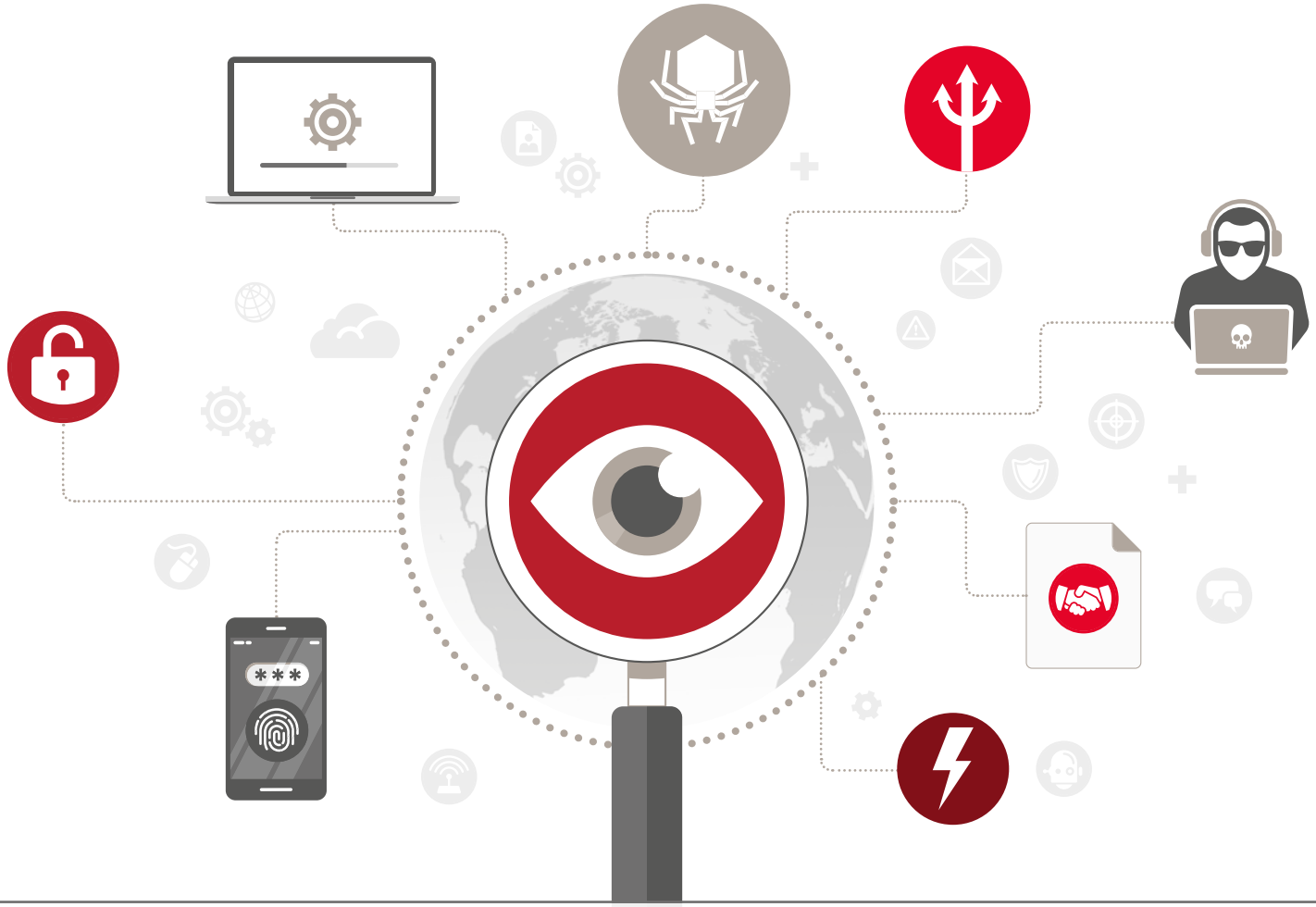
The fraud you don't see is as important as the fraud you do

PwC's 2018 Global Economic Crime and Fraud Survey shows that, while there is growing awareness of the perils of economic crime, too few companies are fully aware of the individual risks they face. This report sets out to plug that awareness gap. In it, we explore not only the visible fraud that companies say they are facing, but also the blind spots that stop them seeing the big picture – and what they can and should do about them.

So, what does our survey tell us about the steps your organisation can take today to fight fraud more effectively?

Four steps to fight fraud

Recognise fraud when you see it

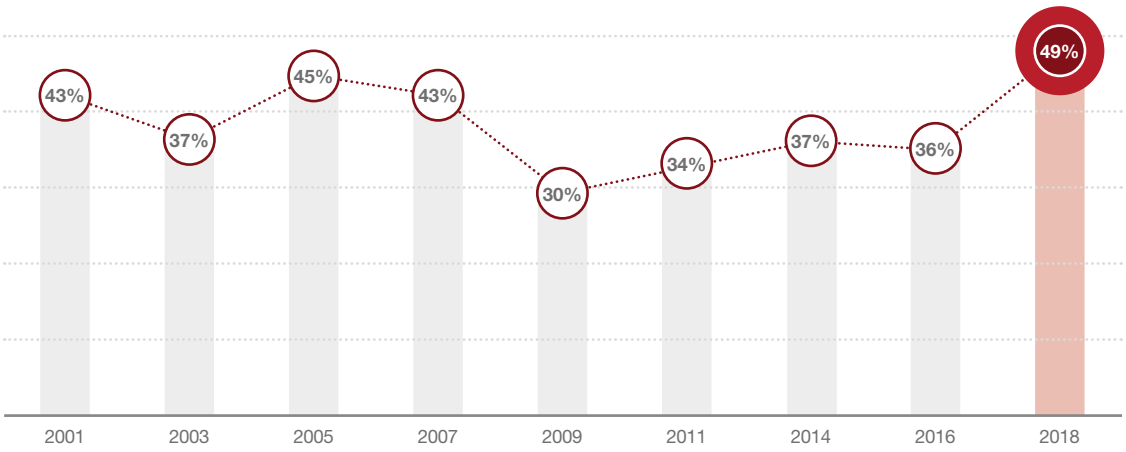


Is fraud really on the rise – or just our awareness of it?

This year, 49% of respondents to our Global Economic Crime and Fraud Survey said their companies had been victims of fraud or economic crime, up from 36% in 2016. This rise can be explained by a combination of growing global awareness of fraud, a larger number of survey responses, and greater clarity about what 'fraud' actually means. But every organisation – no matter how vigilant – is vulnerable to blind spots. And because those blind spots usually only become apparent with hindsight, throwing light onto them as early as possible can vastly enhance fraud-fighting efforts.

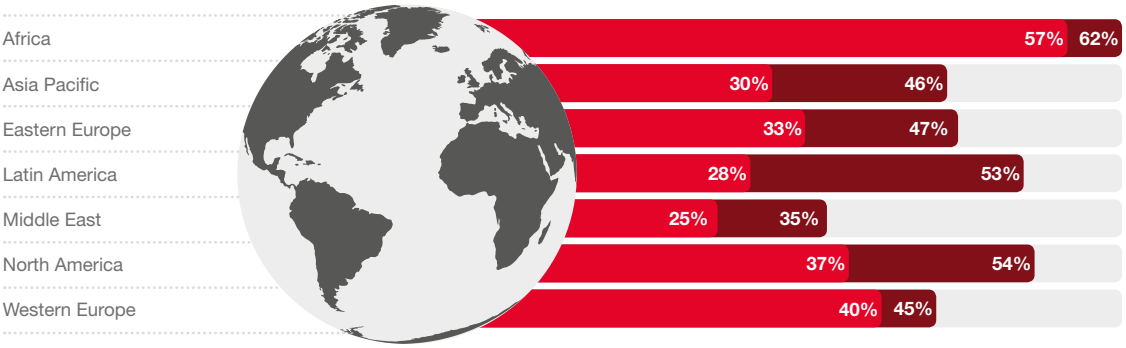
Companies today face a perfect storm of fraud risk – internal, external, regulatory and reputational

Exhibit 1: The reported rate of economic crime is on the rise



Q. Has your organisation experienced any fraud and/or economic crime within the last 24 months?
Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 2: The reported rate of economic crime has increased across all territories



Q. Has your organisation experienced any fraud and/or economic crime within the last 24 months?
Source: PwC's 2018 Global Economic Crime and Fraud Survey

Just as the reported rate of economic crime has increased since 2016, so has the amount that companies are spending to fight it:

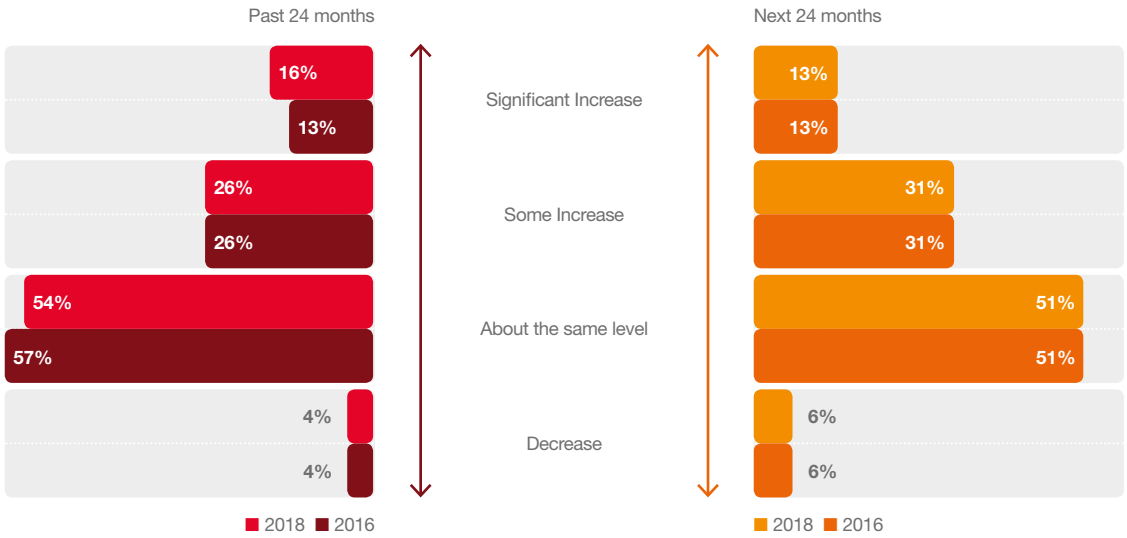
- 42% of respondents said their companies had increased spending on combatting fraud and economic crime over the past two years (up from 39% in 2016).
- 44% of respondents said they plan to boost spending over the next two years.

Where is this money being spent? Organisations are using ever-more powerful technology and data analytics tools to fight fraud. And, in addition to these technology-based controls, many are also expanding whistle-blower programmes and taking steps to keep leadership in the loop.

But do these measures represent a genuine shift to more proactive approaches to fraud and corruption? Or are they just a rear-guard action, driven principally by enhanced anti-bribery/anti-corruption legislation and increasingly globalised forms of enforcement? In other words, are we still missing something vital in the fight against fraud?

Our survey results strongly suggest we are.

Exhibit 3: Organisations continue to increase spending on combatting fraud



Q. How has/is your organisation adjusting the amount of funds used to combat fraud and/or economic crime?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

59%

of CEOs agree or strongly agree that organisations are currently experiencing increased pressure to hold individual leaders accountable for any organisational misconduct

Source: PwC's 21st CEO Survey

71%

of CEOs measure trust between their workforce and their organisation's senior leadership

Source: PwC's 21st CEO Survey

Fraud risk assessments are the first step in preventing fraud before it takes root

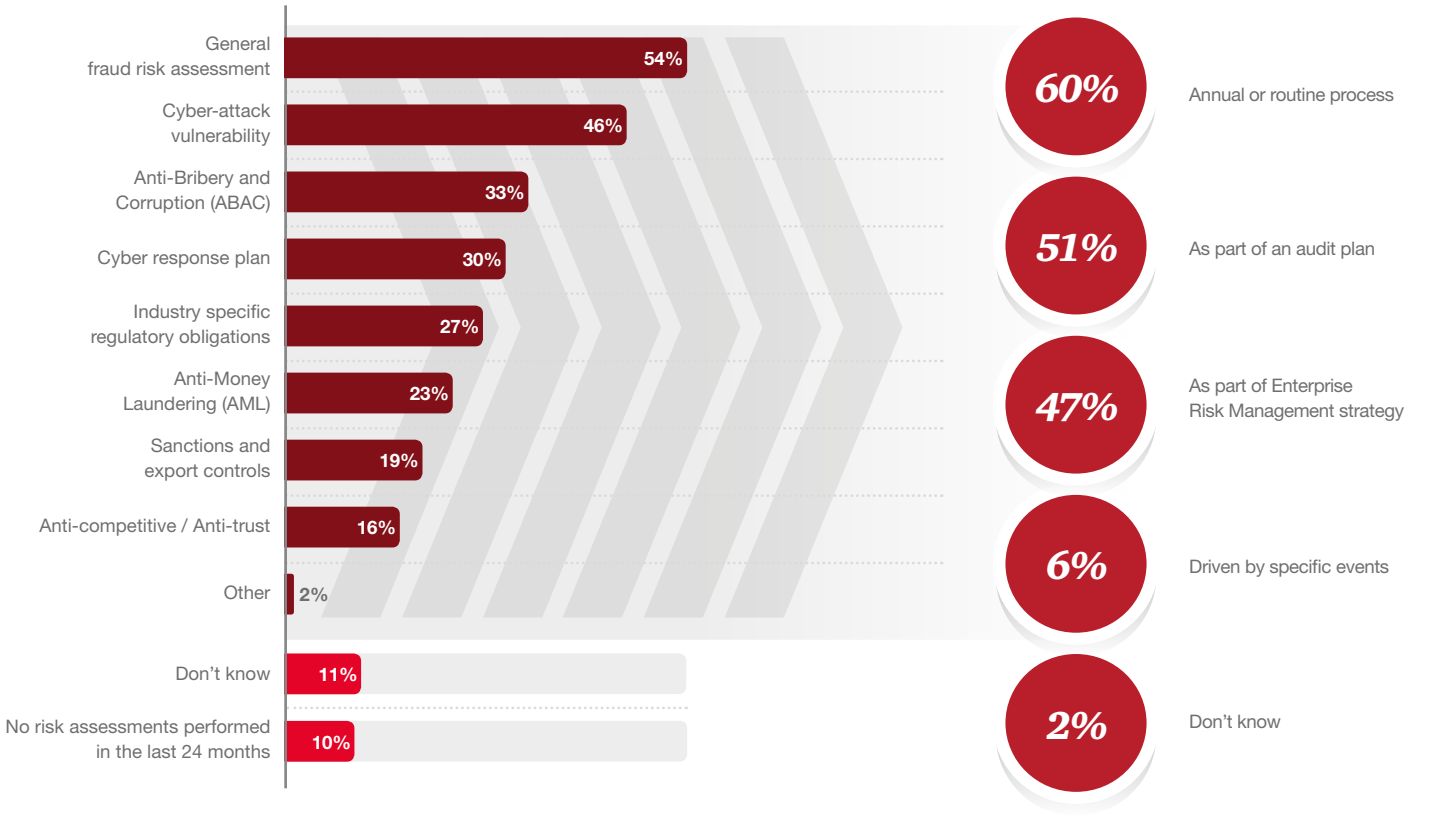
Despite the increase in spending, many organisations are still addressing fraud prevention by using a reactive, defensive approach:

- **Only 54% of global organisations said they have conducted a general fraud or economic crime risk assessment in the past 2 years.**
- Less than half said they had conducted a cybercrime risk assessment.
- Fewer than a third said their company performed risk assessments in the critical areas of anti-bribery and corruption, anti-money laundering, or sanctions and export controls.
- **One in ten respondents had not performed any risk assessments at all in the past 2 years.**

However, the rules of the game are changing profoundly and irreversibly. Public tolerance for corporate and/or personal misbehaviour is vanishing. Not only is sensitivity to corporate misconduct at an all-time high, some corporations and leaders are also now being held to account for past behaviour, conducted when the 'unspoken rules' of doing business might have been thought to be different. PwC's 21st CEO Survey underscores this theme: in it, chief executives cite trust and leadership accountability as two of the most significant threats to business growth.

This points to a heightened risk when fraud or economic crime spills into public view – and a greater need for organisations to take a lead in preventing fraud before it can take root. Fraud risk assessments can help organisations do so by identifying the specific frauds they need to look for. Moreover, these assessments are increasingly looked on favourably by regulators in enforcement actions.

Exhibit 4: Less than half of all organisations have performed targeted risk assessments in the last 2 years



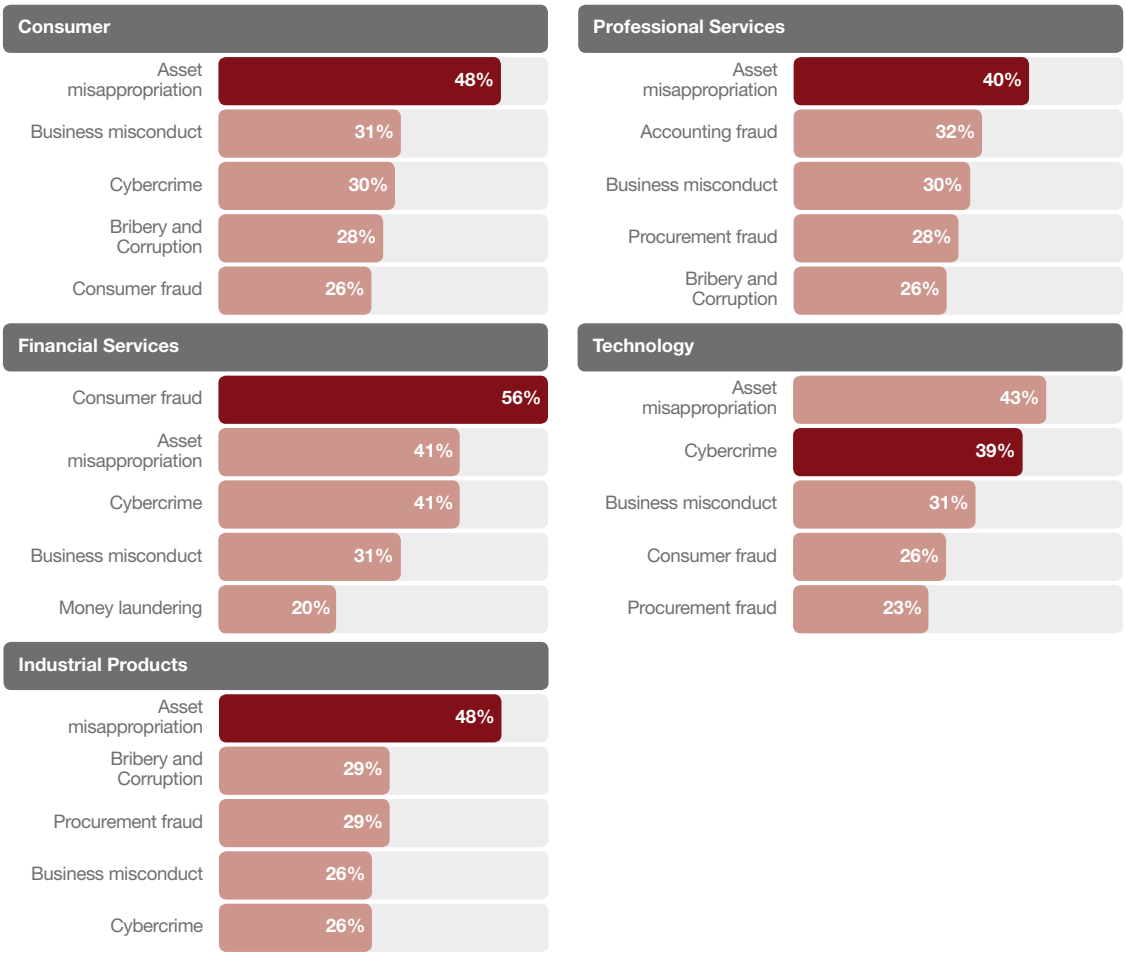
Q. In the last 24 months, has your organisation performed a risk assessment on any of the following areas?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Q. What prompted your organisation to perform a risk assessment?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 5: Asset misappropriation, consumer fraud and cybercrime were the most frequently reported frauds across industries



Q. What type of fraud and/or economic crime has your organisation experienced in your country within the last 24 months?
Source: PwC's 2018 Global Economic Crime and Fraud Survey

Conduct risk: the 'hidden risk' behind many internal frauds

Two types of fraud – consumer fraud and business misconduct – have grown in prominence to such an extent that this year's survey is measuring them as separate threats for the first time. Of the respondents who indicated their companies had experienced fraud in the last two years, 29% said they had suffered from consumer fraud and 28% said they had suffered from business misconduct (making these, respectively, the 3rd and 4th most frequently reported frauds this year, behind asset misappropriation at 45% and cybercrime at 31%). It should be noted that the significant decrease in reported incidents of asset misappropriation (down from 64% in 2016) is at least partly explained by the inclusion of these new frauds in the survey.

These methodological changes reflect the growing recognition of a broad category of internal fraud risk: "conduct risk". This is the risk that employee actions will imperil the delivery of fair customer outcomes or market integrity. And, unlike operational breakdowns or external threats (which can often be checked by internal controls), conduct risk requires a more holistic response – and a shift in attitude.

At present, many companies treat compliance, ethics and enterprise risk management as separate functions – sometimes they even exist in separate siloes within an organisation. But, like all organisational silos, this means these functions rarely add up to a strategic whole. The parts of an organisation that investigate fraud, the parts that manage the risk of fraud, and the parts that report fraud to the board or regulators become disjointed.

When that happens, operational gaps can emerge and fraud can too easily be brushed under the carpet or seen as someone else's problem – to the detriment of the overall effectiveness of fraud prevention, financial performance and regulatory outcomes.

A more innovative approach is to reframe these functions as components of conduct risk. It enables a company to better measure and manage compliance, ethics and risk management horizontally and embed them in its strategic decision-making process. It also means fraud and ethical breaches can be approached more dispassionately, with less emotion, as a fact of life that every organisation has to deal with. Moreover, adopting this more systemic – and realistic – stance towards conduct risk can enable cost efficiencies between ethics, fraud and anti-corruption compliance programmes. It is an important step in breaking down the silos between key anti-fraud functions – and pulling fraud out of the shadows.

Looking for fraud in the right places

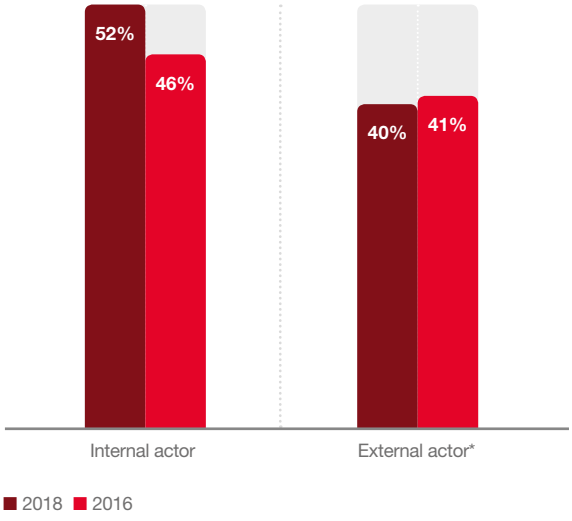
Our survey revealed a significant increase in the share of economic crime committed by internal actors (from 46% in 2016 to 52% in 2018) and a dramatic increase in the proportion of those crimes attributed to senior management (from 16% in 2016 to 24% in 2018). Indeed, internal actors were a third more likely than external actors to be the perpetrators of the most disruptive frauds.

However, one of a company's biggest fraud blind spots – and biggest threats – is often not to do with its employees, but rather the people it does business with. These are the third parties with whom companies have regular and profitable relationships: agents, vendors, shared service providers and customers. In other words, the people and organisations with whom a certain degree of mutual trust is expected, but who may actually be stealing from the company.

24%

of reported internal frauds were committed by senior management

Exhibit 6: Internal actors are the main perpetrators of fraud

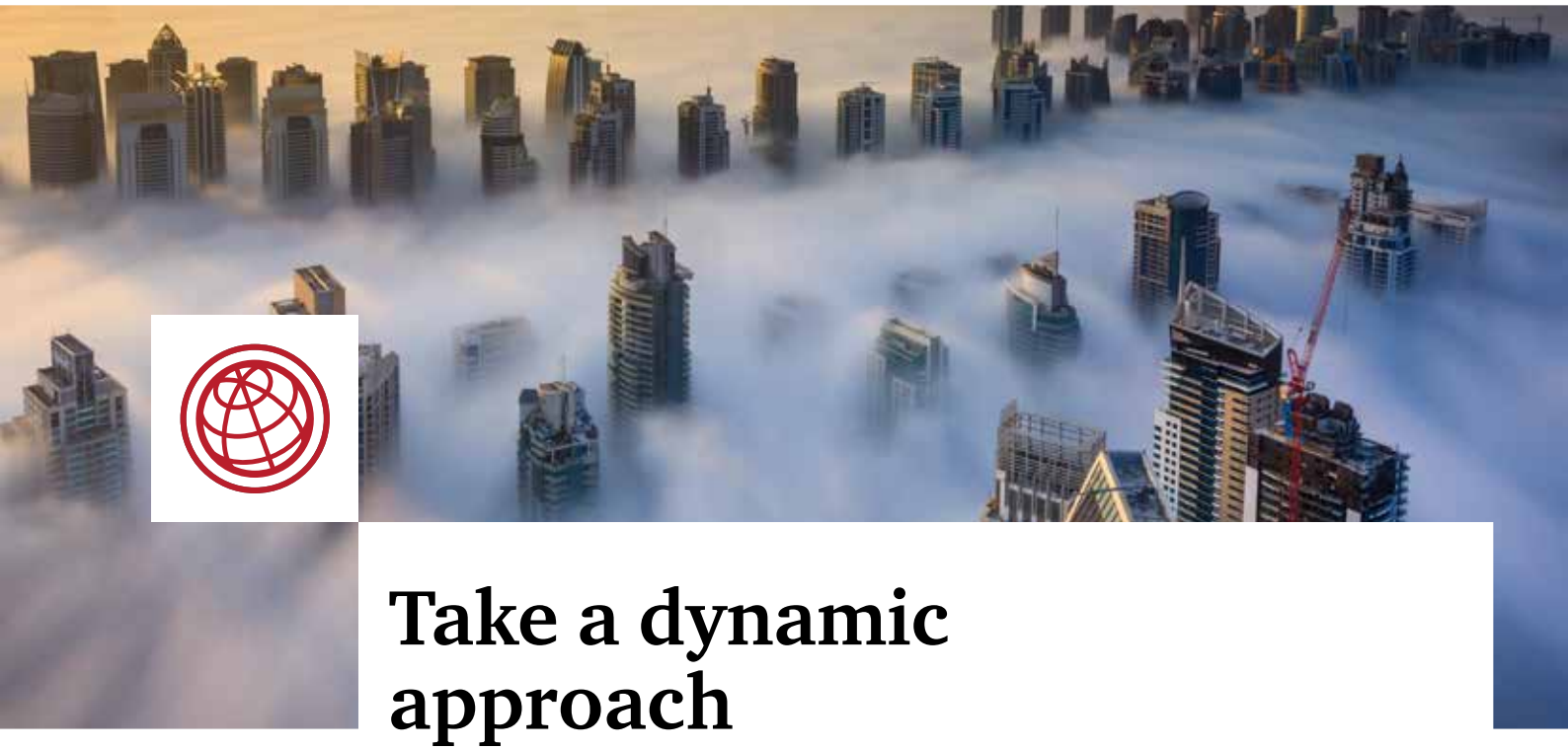


***68%**

of external actors committing the fraud are 'frenemies' of the organisation – agents, vendors, shared service providers and customers

Q. Who was the main perpetrator of the most disruptive fraud?

Source: PwC's 2018 Global Economic Crime and Fraud Survey



Take a dynamic approach

Chief executives are accountable

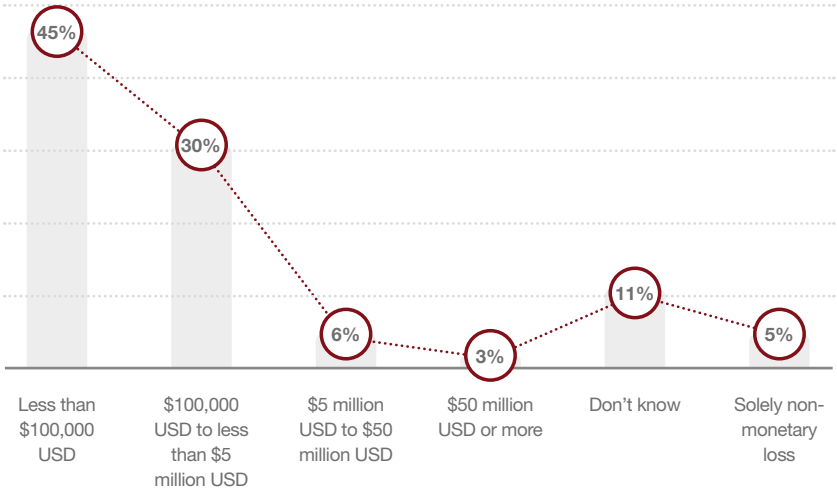
Our survey underscores that the direct monetary cost of fraud and its aftermath can be substantial. But when secondary costs (such as investigations and other interventions) are included, the true picture of overall cost can be much higher.

46%

of respondents said their organisation spent the same or more on investigations and other interventions than was directly lost to fraud itself

When the financial costs of fraud hit the bottom line of a business, it is only natural for the board and shareholders to require explanations from senior management. In today's world, however, a leader's responsibility doesn't stop there. In fact, that's just the beginning.

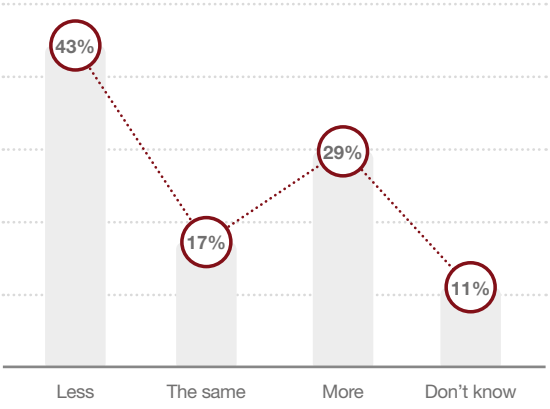
Exhibit 7: Direct monetary losses due to fraud can be substantial



Q. In financial terms, approximately, how much do you think your organisation may have directly lost through the most disruptive crime over the last 24 months?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 8: The amount spent on investigations and other interventions as a result of fraud is significant



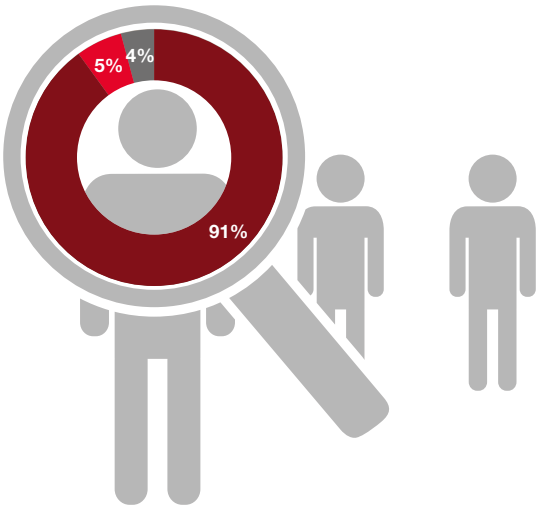
Q. As a result of the most disruptive crime experienced in the last 24 months, was the amount spent by your organisation on investigations and/or other interventions, more, less or the same as that which was lost through this crime?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

A chief executive is increasingly seen as the personal embodiment of an organisation – with their finger on the pulse of every facet of its culture and operations at all times. So, when ethical or compliance breakdowns happen, these individuals are often held personally responsible – both by the public and, increasingly, by regulators. Whether merited or not, one thing is clear: the C-suite can no longer claim ignorance as an excuse.

Our survey shows that in nine in every ten cases, the most serious incidents of fraud have been brought to the attention of senior management. In addition, 17% of respondents indicated that the CEO has primary responsibility for their organisation's ethics and compliance programme. This puts a sharp spotlight on how the front office is managing the crisis – and the extent to which they are (or are not) adjusting their risk profiles accordingly.

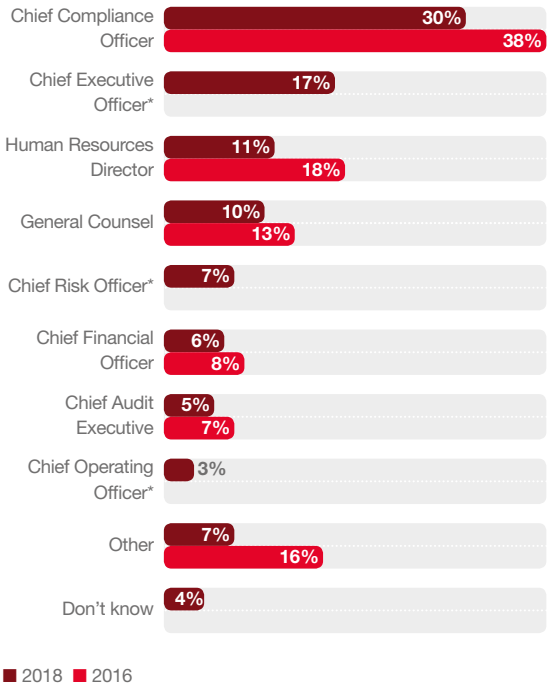
Exhibit 9: Organisations are reporting serious frauds to senior management



Q. Was the most disruptive incident you indicated brought to the attention of your board level executives or to senior leaders charged with governance?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 10: Primary accountability for ethics and compliance programmes resides with the C-suite



* New option in 2018.

Q. Who has primary responsibility for the business ethics and compliance programme in your organisation?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Whereas traditionally fraud prevention and detection would have been the domain of the organisation's second line of defence – risk management, legal, compliance, etc. – today's enterprises are increasingly embedding their newly reinforced fraud prevention measures into the fabric of their first line of defence.

This is likely to be just the beginning of a significant shift, where first-line fraud prevention and detection capabilities continue to mature and strengthen. As they do so, they will enable the second line of defence to shift to a more traditional second-line approach: governance and oversight and setting risk tolerance, frameworks and policies.

In a world where the boundaries between industries, technologies and regulatory bodies continue to blur – and where fraudsters are looking for soft spots to attack beyond their traditional, highly protected financial services targets – this is an important development.

Bad news travels fast: reputational risk now outstrips regulatory risk

A pronounced shift in the way the world looks at fraud and corruption has taken place over the past few years. And our survey data reflects this now deep-seated demand for accountability, from both the public and from regulators, across the private and public sectors.

This is not a phenomenon limited to developed markets, either. Across vastly different cultures, in every region of the world, there are signs of convergence around standards of transparency and expectations of conduct. Nation states in which the rule of law and levels of transparency have traditionally been weak have seen public outrage in the streets, politicians and business leaders jailed, and in some cases even governments toppled.

For an organisation on the receiving end, perhaps with only fragmented information about what has happened, this represents a serious reputational risk. It can find itself punished from all quarters for its perceived inability to respond appropriately – well before the board has a plan for what to do.

Your reputation is subject to no jurisdiction, law or due process

Exhibit 11: Fraud detection moves up to the first line of defence

1

Executive management

The CEO and executives are responsible for management of risk and are held accountable by the Board.

2

Risk functions

The CRO and the risk function are not responsible for managing risk; that is management's job.

3

Internal audit

The Internal Auditor is responsible for independent assurance and is accountable to the Audit and Risk Committee.

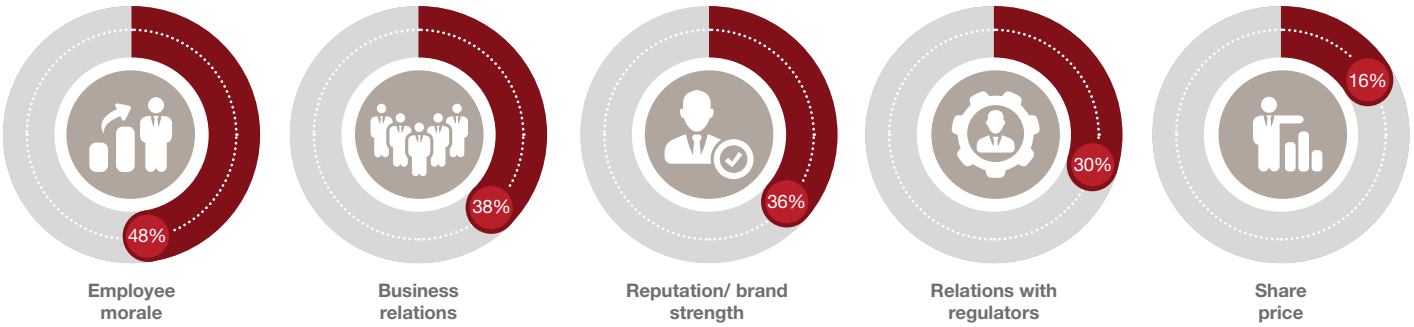
That's because, in this era of radical transparency, companies often don't get to decide when an issue becomes a crisis. Rather, that's down to the jury of public opinion. Moreover, society's rules can change much faster than regulators' – and there is little public tolerance for those who break them. Regulators, by definition, operate within a limited jurisdiction and in accordance with well-defined rules. A company's brand reputation, on the other hand, is subject to no fixed jurisdiction, law or due process.

The executives we surveyed consistently ranked reputational harm at or near the top of negative impacts from various forms of economic crime, with public perception (reputation/brand strength, business relations and share price) taking the hardest hit – a level of impact that has increased since 2016.

Regulatory compliance remains as critical as ever – if not more so. Across the board, regulations and reporting requirements, touching both legal and ethical behaviour, continue to expand. Scrutiny and enforcement are also on the rise globally, and cross-border regulatory cooperation is becoming increasingly routine.

In our survey, 54% of respondents involved in money movement (and/or any of the following lines of business: financial institutions, mutual funds, money service businesses, broker dealers, insurance companies, or dealers in precious metals, stones or jewels) indicated they had experienced an Anti-Money Laundering (AML) regulatory enforcement or inspection in the last two years (up by 4 percentage points from 2016). And an identical proportion (54%) expect recent changes in the geopolitical regulatory environment to have a greater impact on their organisations over the next two years.

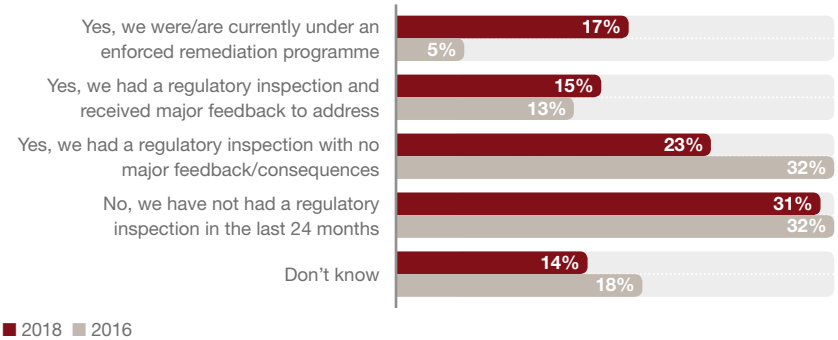
Exhibit 12: Fraud and economic crime impact all elements of the business



Q. What was the level of impact of the most disruptive fraud/economic crime experienced on the following aspects of your business operations?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 13: The number of regulatory enforcements and inspections continues to rise



*Organisations involved in money movement and/or any of these lines of business are: Financial Institution, Mutual Funds, Money Service Business, Broker Dealer, Insurance Company, Dealers in Precious Metals, Stones or Jewels.

Q. Has your organisation experienced any regulatory enforcement/inspection in relation to AML in the last 24 months?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

54%

said they expect changes in the regulatory environment to have an increased impact on their organisation in the next 2 years

Is there a correlation between economic development and fraud?*

Our survey reveals some interesting nuances about global approaches to fraud, which could offer valuable pointers for nation states as they continue on the path of economic development.

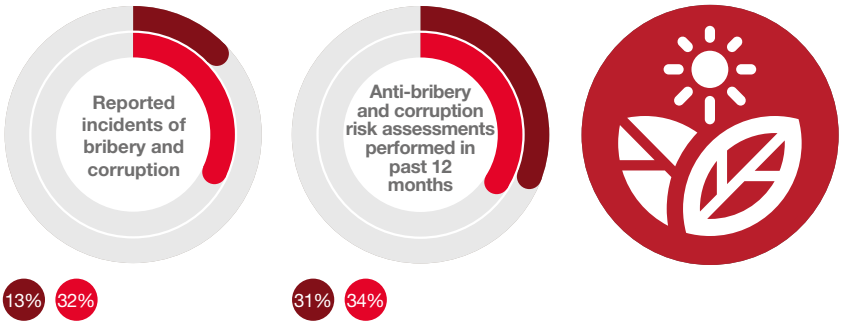
In developing territories, 58% of companies involved in money movement (and/or any of the following lines of business: financial institutions, mutual funds, money service businesses, broker dealers, insurance companies, or dealers in precious metals, stones or jewels) told us they had experienced anti-money laundering (AML) regulatory enforcement or inspection in the last two years. The equivalent figure in developed territories was just 48%.

In developing territories, 15% of companies told us they expect to significantly increase funding for anti-fraud investments in the next 24 months. The equivalent figure in developed territories was just 9%.

In developing territories, respondents told us that economic crime is more often committed by internal actors (59%). The equivalent figure in developed territories was just 39%.

* Our grouping of developed and developing territories was based on the United Nations Conference on Trade and Development classifications. For the purposes of this survey, transitioning territories were treated as developing territories.

Exhibit 14: Developing territories continue to be challenged by corruption risk



Source: PwC's 2018 Global Economic Crime and Fraud Survey

Organisations in developing territories are almost three times as likely to experience corruption as those in developed territories. However, only one third perform risk assessments on anti-bribery and corruption measures, nearly equal to those performed by those in developed territories.

83%

of CEOs report experiencing no negative impact on revenue growth after a well-managed crisis

Source: PwC's CEO Pulse on Crisis

"Instead of tone at the top, organisations should be focused on action at the top"

Tania Fabiani, Partner, PwC US

Learn to leverage the small shocks… and emerge stronger

In any organisation, the occasional breakdown or mishap is unavoidable. And our data suggests that there is plenty of upside to learning how to leverage the small shocks. In fact, they can be a blessing in disguise – an opportunity to test systems and make improvements.

The maturation of a process – for companies as well as countries – happens in part by weathering storms. When a crisis or unplanned event is well managed, 83% of CEOs report experiencing no negative impact on revenue growth. Beyond revenue, how the C-Suite deals with what can become a crisis has a high likelihood of becoming the measure by which it will be judged.

It is natural for a relatively inexperienced company to have a knee-jerk response to a crisis that blindsides it. However, the more a company learns to react to micro-disruptions effectively, the better prepared it is for responding to mega-crises. It acquires a form of 'muscle memory' enabling it to be more proactive in its approach, leveraging mature ethics and compliance programmes and a battle-tested front office.

Harness the protective power of technology

Finding the technology sweet spot

When it comes to fraud, technology is a double-edged sword. It is both a potential threat and a potential protector. Thus, as companies come to view fraud as first and foremost a business problem which could seriously hamper growth, many have made a strategic shift in their approach to technology. These companies are making a business case for robust new investments in areas such as detection, authentication and the reduction of customer friction.

29%

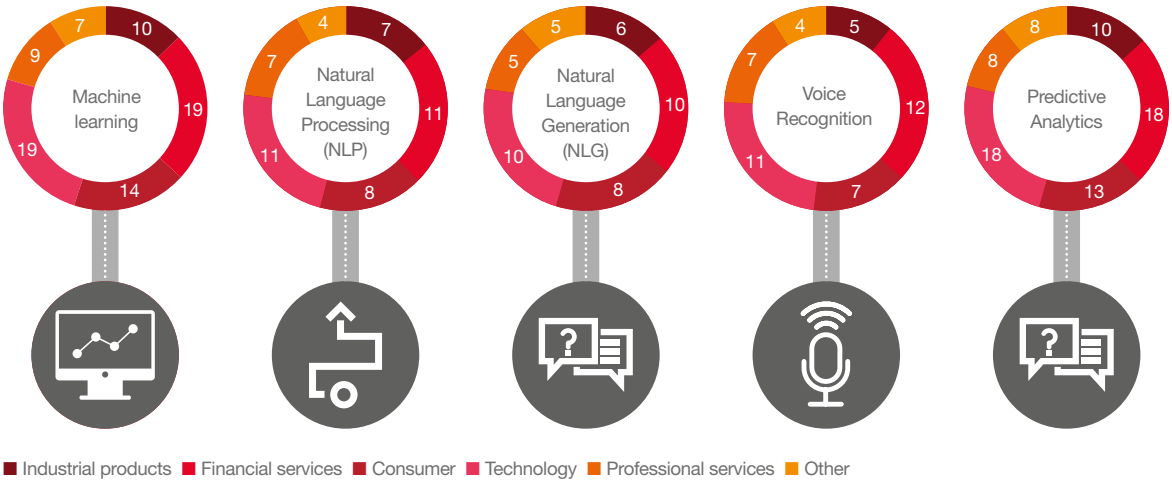
of companies said they spent at least twice as much on investigating and preventing fraud as was lost through the most disruptive economic crimes

42%

of companies said they have increased funds used to combat fraud and/or economic crime

Today, organisations have access to a wealth of innovative and sophisticated technologies with which to defend themselves against fraud, aimed at monitoring, analysing, learning and predicting human behaviour. These include machine learning, predictive analytics and other artificial intelligence techniques. And our survey shows companies are using these technologies, to varying degrees, depending on the industry sector. Technology is expensive to buy and to adopt across a large organisation – prohibitively so, for some. And the decision about what to purchase, and when, is a delicate one. Some invest in emerging or disruptive technologies that they don't use optimally, for instance. Others adopt technology too late and find themselves behind the curve.

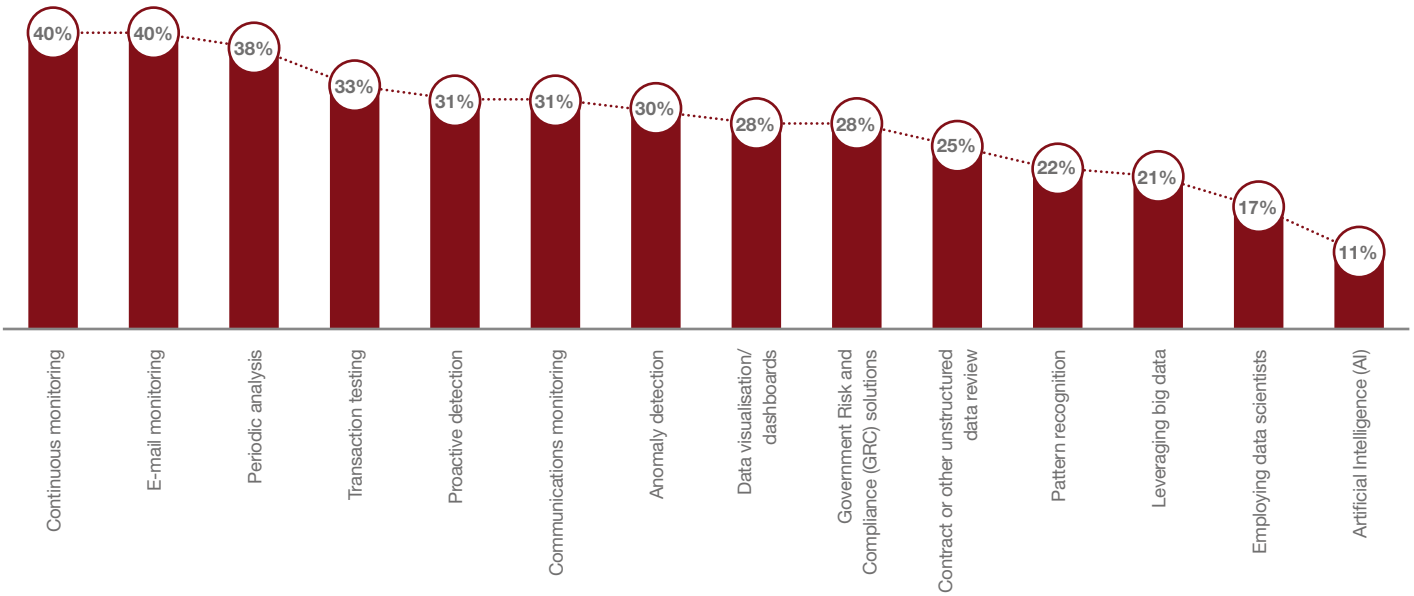
Exhibit 15: The Financial Services and Technology industries are finding the most value in Artificial Intelligence (AI) and Advanced Analytics



Q. To what degree is your organisation using and finding value from Artificial Intelligence or Advanced Analytics to combat/monitor for fraud and other economic crimes? (% of respondents who said their organisation uses and derives value)

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 16: Organisations are beginning to derive value from alternative and disruptive technologies in combatting fraud



Q. To what degree is your organisation using and finding value from the following alternative/disruptive technologies and techniques in your control environment to help combat fraud and/or economic crime? (% of respondents who said their organisation uses and derives value)

Source: PwC's 2018 Global Economic Crime and Fraud Survey

The use of innovative technologies to combat fraud is now a worldwide phenomenon. Indeed, our survey shows that companies in developing territories are actually investing in advanced technologies at a faster rate than those in developed territories. We found 27% of companies in developing territories said they currently use or plan to implement artificial intelligence to combat fraud, while just 22% of companies in developed territories said the same. For those developing territories, this approach could represent an effective means of catching up in an area in which other nations have already sunk considerable infrastructure costs.

In the end, the ubiquity of technology creates a double challenge for all organisations: how to find the sweet spot between a technology's effectiveness and its cost while remaining ahead of the fraudsters.

What is customer friction?

As a customer, it can be reassuring – at first – to know a company is continuously monitoring fraud in the services it provides. But if that monitoring leads to frequent or repetitive alerts, that reassurance can quickly turn to irritation.

This is known as customer friction. And it is a growing challenge for organisations as they seek to strike the right balance between acting appropriately to fraud red flags and being overzealous in alerting their customers.

That is not an easy balance to strike – and the margin for error is small. Be too passive and the organisation risks missing a fraudulent transaction, with all the financial and reputational fallout that follows. But be too proactive, and they risk alienating, or even losing, their customer base.

When it comes to new technology adoption, the developing world is now accelerating ahead of the developed world.'

Philip Upton, Partner, PwC US

34%

of respondents said they thought their organisation's use of technology to combat fraud and/or economic crime was producing too many false positives

Customers aren't just one consideration of your business – they are your business

Customers are the lifeblood of any business. But, as business models continue to evolve through the digital revolution, many of those customers are being exposed to payment fraud for the first time. How an organisation handles that fraud will profoundly affect its outcomes. Here are some of the characteristics and challenges of today's digital fraud:

New digital products are creating new attack surfaces

To bring products to market, companies once followed an established B2B process involving resellers, distributors and retailers. On today's innovative B2C digital platforms, there is a much wider attack surface – and much more room for fraud to break through.

Industry lines are blurring

Non-financial services companies are venturing into payment systems. These relative newcomers sometimes lack the anti-fraud and anti-money laundering experience and know-how of traditional financial services companies, making them, and their third-party ecosystems, susceptible to both fraud and regulatory risk.

The technical sophistication of external fraudsters continues to grow

Digital fraud attacks are becoming more and more sophisticated, thorough and devastating. Single ransomware attacks can cripple organisations and fraudsters manage to move billions of dollars between bank accounts every day.

You can change your credit card number, but you can't change your date of birth

The knowledge-based authentication tools long used to control fraud are outdated and new techniques – such as digital device ID and voice biometrics – are now necessary to protect customers' assets. But most companies are yet to adopt them. This is important because a major data theft is nothing like the loss of a replaceable asset like cash. Rather, what is lost is an individual's unique, deeply personal, permanent identity markers (such as date of birth or social security number). Because this is the very data that knowledge-based authentication tools use to verify identity and prevent fraud, its theft opens the door for fraudsters to take over a person's identity.

Cybercrime: a disconnect between ends and means

Cybercrime has long passed beyond infancy and adolescence. Today's cybercriminals are as savvy and professional as the businesses they attack. This maturity calls for a new perspective on the multifaceted nature of cyber threats and accompanying frauds.

Often, the first sign an organisation gets that something systemic is amiss is the detection of a cyber-enabled attack, such as phishing, malware or a traditional brute force attack. The increasing frequency, sophistication and lethality of these attacks are spurring companies to look for ways to pre-empt them. This approach has the added benefit of enabling a deeper focus on fraud prevention.

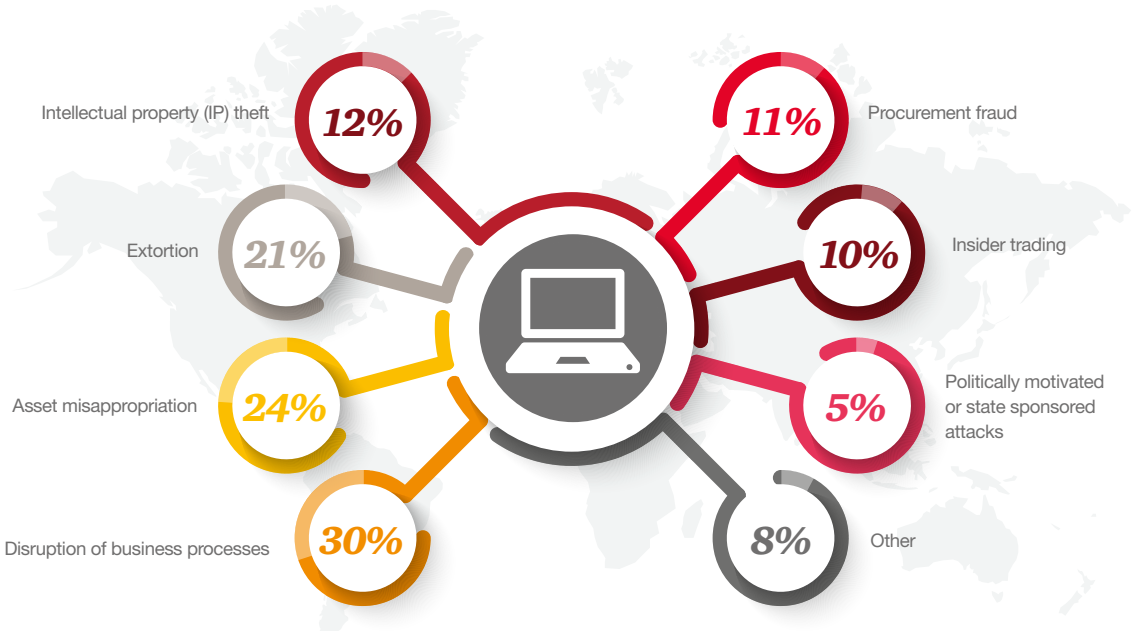
Although it can be difficult for companies to accurately measure the financial impact of cyber-attacks, 14% of survey respondents who said cybercrime was the most disruptive fraud told us they lost over $US1 million as a result, with 1% indicating they lost over $US100 million.

Cybercrime was more than twice as likely than any other fraud to be identified as the most disruptive and serious economic crime expected to impact organisations in the next two years (26% of respondents said they expected a cyber-attack in the next two years and that it would be the most disruptive; 12% said they expected bribery and corruption to be most disruptive; while 11% said the same about asset misappropriation). In fact, cyber-attacks have become so pervasive that measuring their occurrences and impacts is becoming less strategically useful than focusing on the mechanism that the fraudsters used in each case.

41%

of executives surveyed said they spent at least twice as much on investigations and related interventions as was lost to cybercrime

Exhibit 17: Types of fraud that organisations were a victim of through a cyber-attack



Q. Which of the following types of fraud and/or economic crime was your organisation victim of through a cyber-attack?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

While all digital fraud is fraud, not all fraud is digital. It can therefore be helpful to distinguish two forms of cybercrime:

(1) As digital theft (the stolen goods, not the smashed door). This type of attack could include stealing cash, personal information, and intellectual property, and could involve extortion, ransomware, or a host of other crimes.

(2) As digital fraud. This type of attack is in many ways the more long-lasting and disruptive, because the fraudster penetrates an open door (typically, but not always, a customer- or employee-facing access point) and uses the company's own business processes to attack it. To combat this type of fraud, the organisation must use digital methods – both as a vaccine and as a remedy.

Exhibit 18: Cyber-attack techniques used against organisations

36% Malware

33% Phishing

13% Network scanning

10% Yes, but unsure of technique

8% Brute force attack

7% Man in the middle

3% Other technique

Q. In the last 24 months, has your organisation been targeted by cyber-attacks using any of the following techniques?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Over a third of all respondents have been targeted by cyber-attacks, through both malware and phishing. Most of these attacks, which can severely disrupt business processes, also lead to substantive losses to companies: 24% of respondents who were attacked suffered asset misappropriation and 21% were digitally extorted.

Beyond compensating customers… where'd the money go?

While keeping customers happy is the first order of business, there are deeper dimensions to fraud prevention. These involve the fraud underworld, and the regulation and enforcement regimes whose mission is to control it.

In the case of identity theft, for instance, a bank or merchant will cover the loss to the customer and absolve them of further responsibility if, say, a fraudster opens a credit card in her name and runs up a significant balance. Until now, the system of remedying such external frauds has worked in this way, and all parties – banks, merchants, consumers and regulators – have accepted it as part of the cost of doing business together.

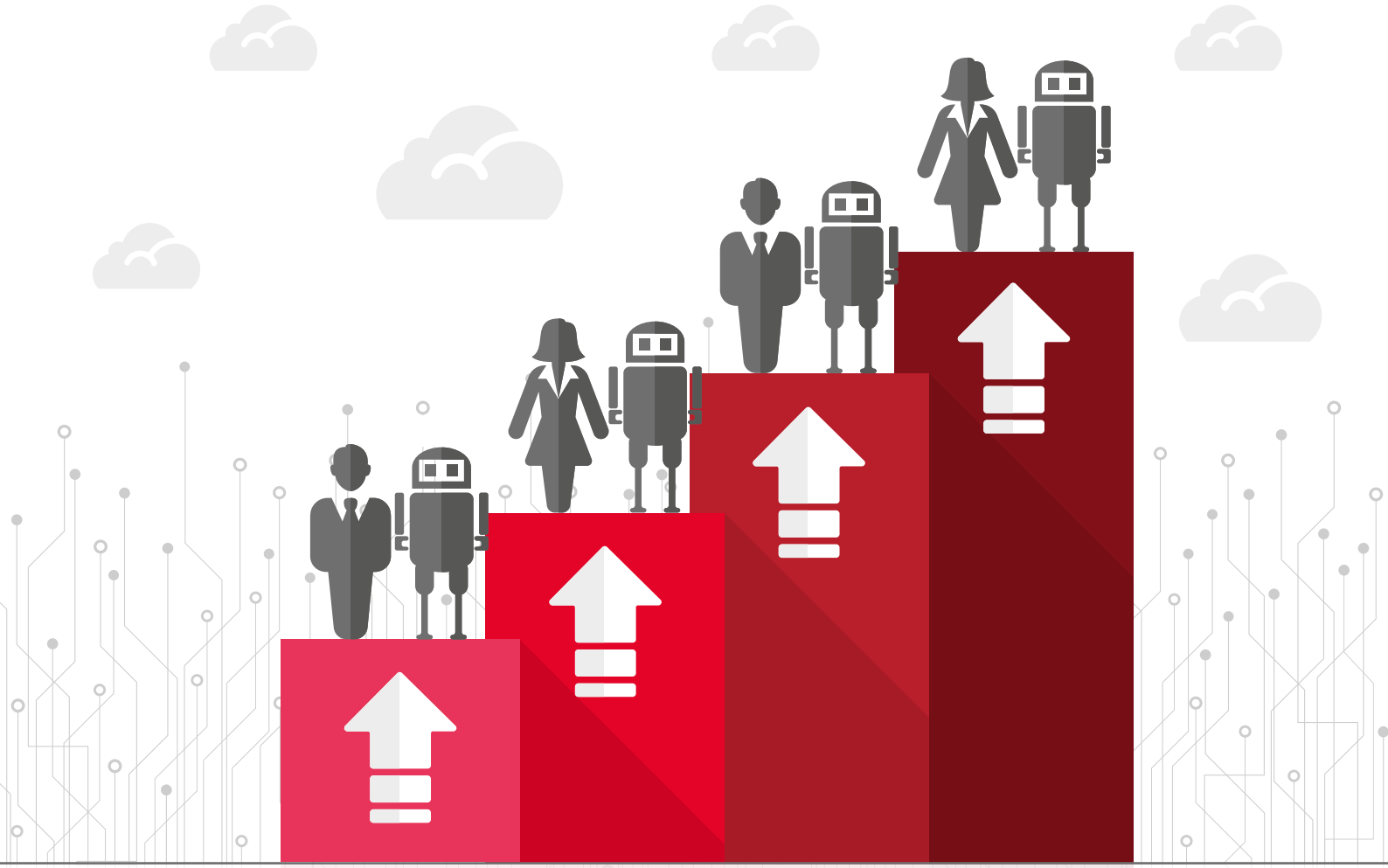
While these fraudulent activities can be detected by the transaction monitoring systems built in response to the United States' Bank Secrecy Act (BSA) and similar rules in other countries, it is likely that both banks and money services businesses (MSBs) are missing the manner in which these transactions manifest themselves in the system. This has been shown in recent regulatory enforcement around lack of detection by businesses in the context of human trafficking, for example.

Non-financial companies may not have the same regulatory obligations as their financial counterparts, but they could still find themselves falling foul of the law. Regulators and law enforcement are now looking beyond the primary impact of a crime – for example, trafficking in counterfeit goods – to examine which illicit activities the stolen assets went to finance. As part of their remit, they are scrutinising non-financial services companies' compliance and anti-fraud measures for signs that they may be, consciously or not, aiding and abetting criminal activities.

The business case

The business case for investment in anti-fraud technology goes beyond protecting the organisation from reputational, regulatory and/or financial damage. It also includes reducing the cost of fraud prevention through efficiencies and enabling an organisation to safely build and sell new products and services on a digital platform. Furthermore, it enables a business to fine-tune a fraud programme to reduce customer friction – allowing customers to interact more freely with its platform and its product.

Invest in people, not just machines



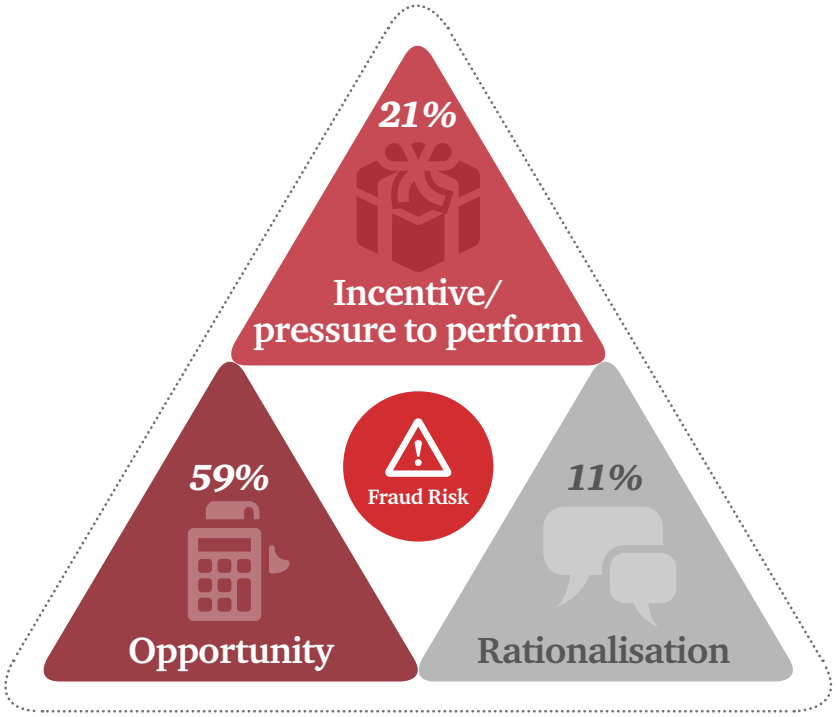
A small investment in people can pay huge dividends

Confronted with the seeming intractability of dealing with fraud, many organisations decide to pour ever more resources into technology. Yet these investments invariably reach a point of diminishing returns, particularly in combatting internal fraud. So, while technology is clearly a vital tool in the fight against fraud, it can only ever be part of the solution.

This is because fraud is the result of a complex mix of conditions and human motivations. The most critical factor in a decision to commit fraud is ultimately human behaviour – and this offers the best opportunity for combatting it. There is a powerful method for understanding and preventing the three principal drivers of internal fraud – the fraud triangle.

The fraud triangle starts with an incentive (generally a pressure to perform from within the organisation) followed by an opportunity, and finally a process of internal rationalisation. Since all three of these drivers must be present for an act of fraud to occur, each of them should be addressed individually.

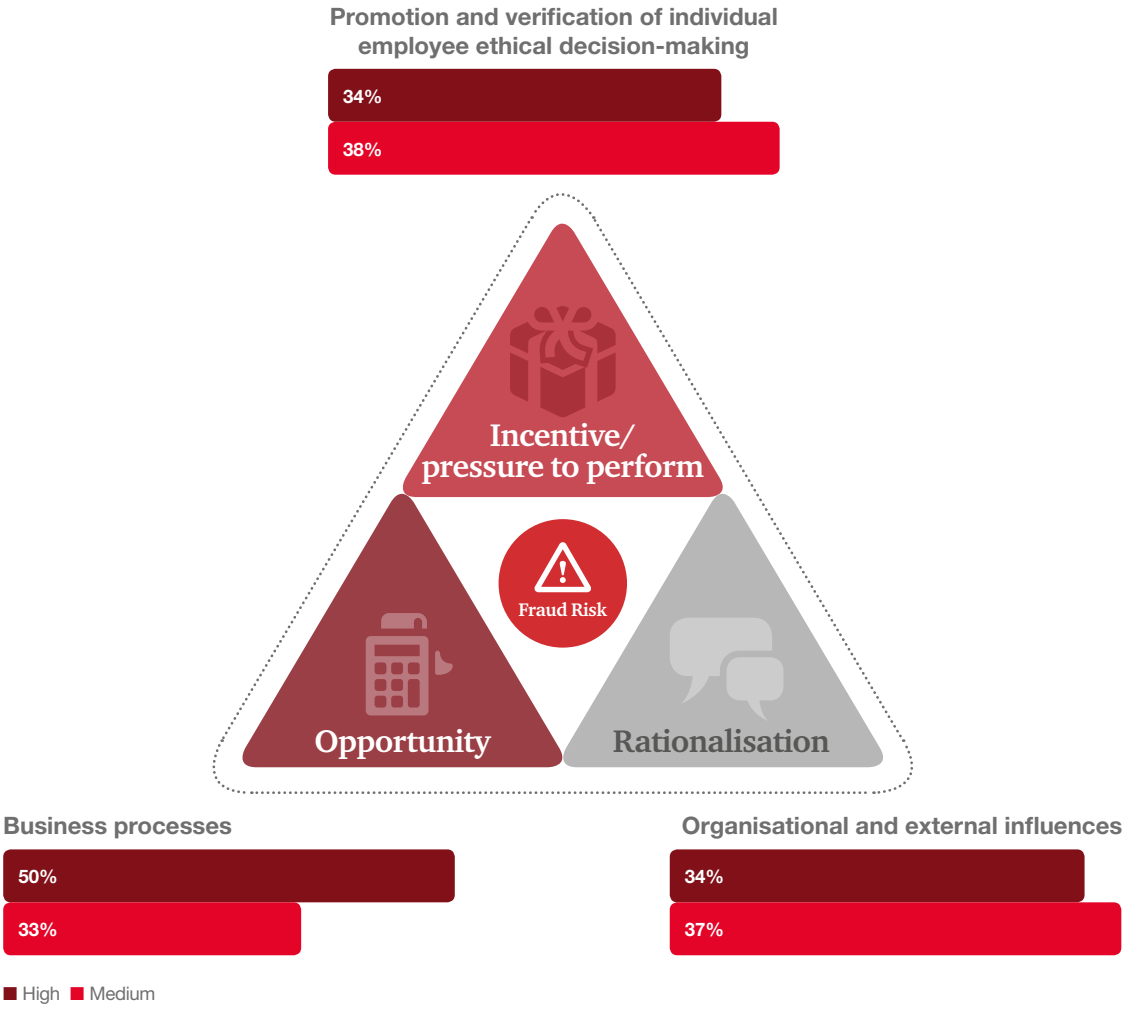
Exhibit 19: The fraud triangle: what makes an employee commit fraud?



Q. To what extent did each of the following factors contribute to the incident of fraud and/or economic crime committed by internal actors? (% of respondents who ranked the factor as the leading contributing factor to internal fraud)

Source: Global Economic Crime and Fraud Survey 2018.

Exhibit 20: The level of organisational effort required to combat internal fraud



Q. What level of effort does your organisation apply to the following categories in order to combat fraud and/or economic crime internally?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Preventing the opportunity: controls

Most organisations' anti-fraud efforts in recent years have been focused on reducing the opportunities for fraudulent acts: 50% of survey respondents said they expend a high degree of effort in building up business processes, such as internal controls, that target opportunities to commit fraud. And, while 59% of respondents ranked opportunity as the leading contributor to the most disruptive frauds committed by internal actors, this was 10 percentage points lower than the equivalent figure in 2016 (69%). This is evidence that technology has a key role to play – and, more to the point, that companies are generally employing it effectively.

Unfortunately, companies are putting significantly less effort into measures to counteract incentives and rationalisation, with only 34% indicating they spent a high level of effort targeting these factors. Our survey highlights the result of these choices: 21% of respondents ranked incentives/ pressure as the leading contributing factor of the most disruptive fraud committed by internal actors, twice the amount reported in 2016 (11% identified rationalisation as the leading motivating factor – the same proportion as in 2016).

This under-emphasis on cultural/ethical measures points to a potential blind spot, and indeed may be one reason why internal fraud is so resilient. Because fraud is the result of the intersection of human choices with system failures, it is important to be wary of the false sense of security that internal controls, even well-designed ones, can bring.

Indeed, there is a fundamental flaw with the belief that internal technology-driven controls alone can catch fraud: it assumes that management will always behave ethically. In fact, experience shows that virtually every significant internal fraud is a result of management circumventing or overriding those controls. Our survey backs this up: it reveals that the share of reported serious internal fraud committed by senior management has risen dramatically – by 50% – over the past two years (from 16% of respondents in 2016 to 24% in 2018). To overcome this structural problem, organisations need to create controls that actually account for management override or collusion in targeted areas.

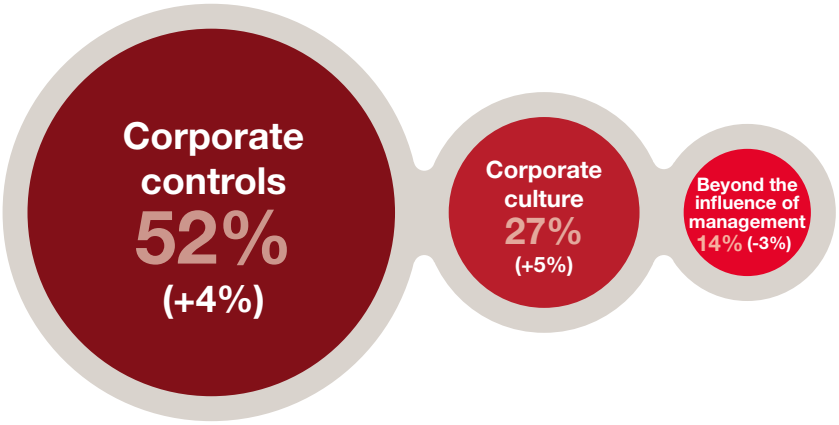
Preventing the incentive: openness

Corporate-sized frauds are generally connected to corporate pressures – and the pressure to commit fraud can arise at any level of the organisation. Our survey shows that 28% of organisations that experienced fraud in the last two years suffered business conduct/misconduct fraud (incentive abuse), and 16% of global organisations with offices in other territories experienced business conduct/misconduct fraud in those other territories. Meanwhile, 24% of respondents indicated that senior management was responsible for the most disruptive crime experienced.

It is important not to over-emphasise financial incentives when considering what drives a person to commit fraud. Fear and embarrassment about having made a mistake may be equally important. Thus, the incentives coming from the top of the organisation must be examined: to what extent do they align with regulations and with 'doing the right thing'?

In addition, short-term bespoke controls can serve as useful checks on whether aggressive sales programmes are leading to fraudulent behaviour. A well-publicised open-door or hotline policy can also provide a valuable early-warning system of potential problems in an organisation.

Exhibit 21: Just over half of the most disruptive frauds were detected by corporate controls



Includes		Includes		Includes	
Internal audit (routine)	14%	Tip off (internal)	13%	By accident	8%
Fraud risk	13%	Tip off (external)	7%	By law enforcement	4%
Suspicious activity monitoring	13%	Whistleblowing hotline	7%	Investigative media	2%
Corporate security	5%				
Data analytics	4%				
Rotation of personnel	1%				

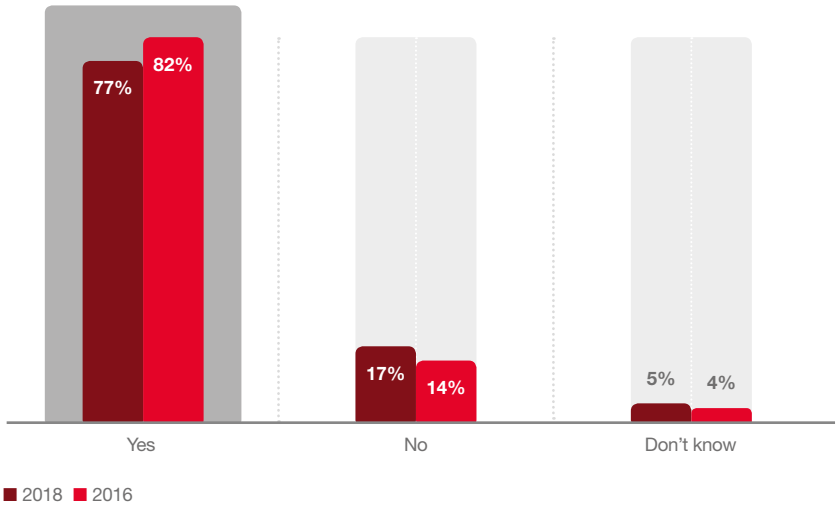
Q. How was the most disruptive fraud and/or economic crime initially detected?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Fraud can occur with the best of intentions

Fraud needn't necessarily be a malicious or selfish act. From a legal point of view, there are actually two kinds of fraud – fraud committed for personal gain (such as embezzlement, or false reporting intended to boost compensation) and fraud committed for "corporate motives" (such as the survival of the company, or the protection of the workforce). The latter could occur with the best of intentions set on increasing the company's success. For example, what might start as a sales strategy designed to increase market share and profitability (to the benefit of employees) might ultimately morph into fraudulent sales tactics. Either way, the result is the same: the executive suite will be held responsible.

Exhibit 22: Fewer companies report having ethics and compliance programmes



Q. Do you have a formal business ethics and compliance programme in your organisation?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Preventing rationalisation: culture

While incentives and opportunities can be influenced and managed, preventing the rationalisation of a fraudulent act is more of a challenge. This is a process that occurs entirely within the human mind and is thus far harder to influence.

One of the peculiarities of internal fraud is that those who commit it often see it as a victimless crime and cannot visualise any person who will be directly harmed by their actions. This helps explain why nearly three-quarters of survey respondents told us that an internal actor was the main perpetrator of the following most disruptive economic crimes, including human resources fraud (81%), asset misappropriation (75%), insider trading (75%), accounting fraud (74%) and procurement fraud (73%).

The first step in preventing rationalisation is to focus on the environment that governs employee behaviour – the organisational culture. Surveys, focus groups and in-depth interviews should therefore be used to assess the strengths and weaknesses of that culture. Consistent training is also key. If people clearly understand what constitutes an unacceptable action – and why – rationalising fraudulent activity will be harder.

However, our survey found a decreasing number of organisations investing in the kind of training that can make a material difference to fraud prevention. The percentage of respondents who indicated they have a formal business ethics and compliance programme has dropped from 82% to 77% since our 2016 survey. And only 58% of companies with such a programme indicated that programme has specific policies targeting general fraud.

The task of detecting and preventing economic crime or fraud is undoubtedly a complex one. It means finding the right blend of technological and people-focused measures, guided by a clear understanding of the motivations behind fraudulent acts and the circumstances in which they occur. Organisations need not resign themselves to the belief that technology is the only solution, or that a certain amount of fraud is simply part of the cost of doing business. Rather, by establishing a culture of honesty and openness from the top down, they can imbue their organisations with a spirit of open accountability – and pull fraud out of the shadows.

Conclusion

Be prepared. Face the fraud. Emerge stronger.

Our survey shows that many companies are under-prepared to face fraud, for both internal and external reasons. This is why shining a light on an organisation's fraud blind spots, and sharing a clear understanding of what constitutes fraud – and what needs to be done to prevent it – is so important.

Doing so can also unlock significant opportunities. It can help make positive structural improvements across the organisation – which can make the business stronger and more strategic in both good times and bad. That includes removing siloes in functions like compliance, ethics, risk management and legal – and enabling a culture that is more positive, cohesive and resilient.

It's true that the value proposition of an up-to-date fraud programme can be hard to quantify, making it sometimes difficult to secure the investments needed. But the opportunity cost – financial, legal, regulatory and reputational – of failing to establish a culture of compliance and transparency can be far greater.

Not only has the threat of economic crime intensified in recent years, the rules and expectations of all stakeholders – from regulators and the public to social media and employees – have also changed, irrevocably. Today, transparency and adherence to the rule of law are more critical than they have ever been.

And that's a good thing, because in the court of public opinion, where reputations can be won and lost overnight, a business will be held accountable tomorrow for what happens today. Therefore, how it responds when a fraudulent event or compliance issue arises will be as important for the company as the event itself.

Understanding this principle gives a business the opportunity to get ahead of fast-moving events, and to demonstrate to both internal and external stakeholders that it is on top of the issues. Not only are there considerable reputational benefits to 'owning' transparency, in an atmosphere of zero-tolerance, doing so can actually enhance the job security of senior management – while attracting the next generation of leaders to the organisation.

An unplanned event can quickly spiral into a crisis if not well managed. But with the right mechanisms in place – a culture of cohesion and openness and a sophisticated control environment – a company will be well positioned to absorb the shocks, build 'muscle memory', and emerge stronger. The imperatives are clear: place transparency at the heart of corporate purpose, use it to unite strategy, governance, risk management and compliance, and find yourself better positioned to transform a potentially serious business problem into an opportunity to come out ahead.

Contacts

Want to know more about what you can do in the fight against fraud? Contact one of our subject matter experts

Survey Leadership

Didier Lavion
Principal
PwC US
+1 (646) 818 7263
didier.lavion@pwc.com

Forensic Services Leaders

Kristin Rivera
Global Forensics Leader
PwC US
+1 (415) 498 6566
kristin.d.rivera@pwc.com

Dinesh Anand
Partner
PwC India
+91 (124) 330 6005
dinesh.anand@pwc.com

Dyan Decker
Partner
PwC US
+1 (646) 313 3636
dyan.a.decker@pwc.com

John Donker
Partner
PwC Hong Kong
+852 2289 2411
john.donker@hk.pwc.com

Ian Elliott
Partner
PwC UK
+44 (0) 771 191 2415
ian.elliott@pwc.com

Trevor Hills
Partner
PwC South Africa
+27 (11) 797 5526
trevor.hills@pwc.com

Leonardo Lopes
Partner
PwC Brazil
+55 (11) 3674 2562
leonardo.lopes@pwc.com

Richard Major
Partner
PwC Singapore
+65 6236 3058
richard.j.major@sg.pwc.com

Domenic Marino
Partner
PwC Canada
+1 (416) 941 8265
domenic.marino@pwc.com

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

Sirshar Qureshi
Partner
PwC Czech Republic
+420 251 151 235
sirshar.qureshi@pwc.com

Nick Robinson
Partner
PwC United Arab Emirates
+971 4304 3974
nick.e.robinson@pwc.com

Malcolm Shackell
Partner
PwC Australia
+61 (2) 8266 2993
malcolm.shackell@pwc.com

About the survey

PwC's 2018 Global Economic Crime and Fraud Survey was completed by 7,228 respondents from 123 territories. Of the total number of respondents, 52% were senior executives of their respective organisations, 42% represented publicly-listed companies and 55% represented organisations with more than 1,000 employees.

www.pwc.com/fraudsurvey