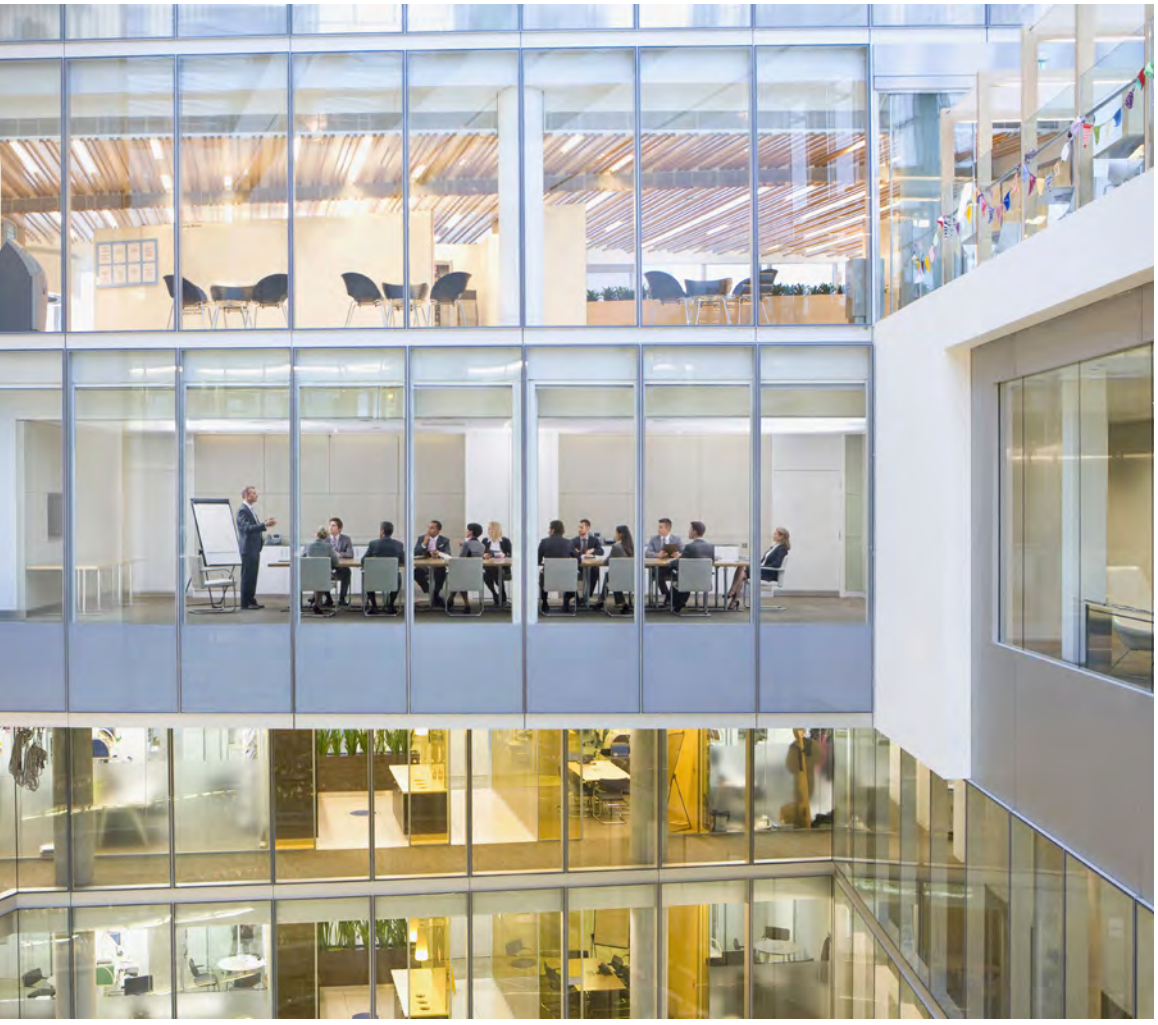
Adjusting the Lens on Economic Crime

Preparation brings opportunity back into focus



36%

More than one in three organisations report being victimised by economic crime

32%

Cybercrime climbs to 2nd most reported economic crime affecting organisations

44%

Close to half the organisations surveyed believe that local law enforcement is not adequately resourced to investigate economic crime, leaving the responsibility for fighting economic crime on organisations

pwc

Leading observations

1 *Economic crime an obstinate threat*

- More than one in three (36%) organisations experienced economic crime
- Both developed and emerging markets affected
- Company detection methods not keeping pace

What opportunities are there to counter economic crime proactively?

Economic crime is a diversified global issue

2 *Controls must be embedded in organisational culture*

- Gap between internal and external fraud actor is closing
- 1 in 5 respondents have never carried out a fraud risk assessment

What are the risks your business faces and do you actively identify vulnerable areas?

Financial damage extending to the hundreds of millions of US dollars in some cases

3 *Cyber threats climb, but business preparation is not keeping pace*

- Cybercrime climbs to 2nd most reported economic crime affecting 32% of organisations
- Most companies are still not adequately prepared for – or even understand the risks faced: Only 37% of organisations have a cyber incident response plan
- Engagement of leadership is critical, but less than half of board members request information about their organisation's state of cyber-readiness

How will your cyber-response plan stand up to reality?

Cyber preparedness should be viewed as an organisational stress test

4 *Disconnect between tone at the top and reality on the ground*

- 1 in 5 respondents not aware of the existence of a formal ethics and compliance programme and many are confused about who owns it internally
- Almost half the incidents of serious economic crimes were perpetrated by internal parties
- Employee morale (44%) and reputational harm (32%) cited as top forms of damage

How is your business strategy aligned with and led by your organisational values?

People and culture are your first lines of defence

5 *Anti-money laundering continues to confound*

- 1 in 5 banks have experienced enforcement actions by a regulator – failure to curb illicit business practices may lead to personal liability
- More than a quarter of financial services firms have not conducted AML/CFT risk assessments across their global footprint
- Data quality cited by 33% of respondents as a significant technical challenge
- Lack of experienced AML/CFT staff is a major issue

How would your organisation fare in the face of regulatory scrutiny?

The cost of compliance (and of non-compliance) continues to rise

Contents

Foreword

In business, the promise of opportunity is often tempered with the reality of risk.

This formula holds true not only for those working to build and sustain a business, but also for those looking to victimise one.

The story told in our 2016 Global Economic Crime Survey is one with which we are all too familiar: economic crime continues to forge new paths into business, regulatory compliance adds stress and burden to responsible businesses, and an increasingly complicated threat landscape challenges the balance between resources and growth. The moral of this story is not new, but is one that may have been forgotten in our haste to succeed in today's fast-paced global marketplace.

Our report challenges you to adjust your lens on economic crime and refocus your path towards opportunity around strategic preparation.

This work needs to be embedded in your day-to-day decision-making, and supported by strong corporate ethics. Preparing your company for sustained success in today's world is no longer an exercise in mapping out plans that live out their days in dusty binders on a director's shelf. Preparation today is a living, breathing exercise; one that must be constantly tweaked, practiced and tended to, so that it is ready when threats become realities.

Understanding the vision of your company and strategically mapping out a plan for both growth as well as a plan for defence – one that is based on your unique threat landscape and profile – will be the difference between realizing your opportunity or allowing those who want to victimise you to capitalise on theirs.

Trevor White

Trevor White
Partner, Global Economic Crime Survey Leader
South Africa

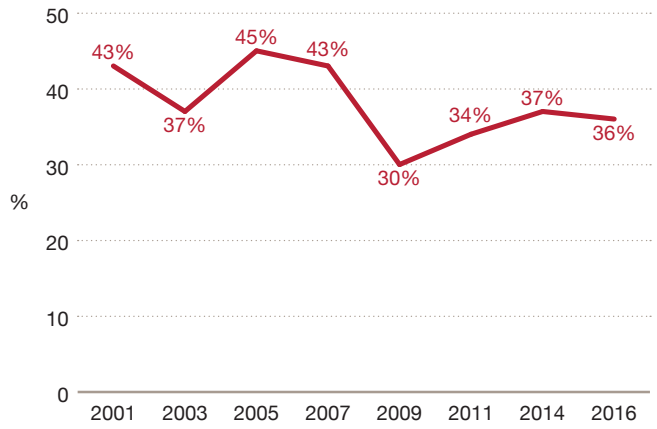
Economic crime evolution

2016: Economic crime evolving, preventative measures lagging

More than a third of organisations have experienced economic crime in the past 24 months, as reported by over 6,000 respondents to PwC's Global Economic Crime Survey 2016. This year's results show that the incidence of economic crime has come down, for the first time since the global financial crisis of 2008-9 (albeit marginally by 1%).

At first glance, this could be evidence of a return on the investments in the preventative measures which organisations have been making over the past few years. But as we look at the data more closely, it is possible that this small decrease is actually masking a worrying trend: that economic crime is changing significantly, but that detection and controls programmes are not keeping up with the pace of change. What's more, the financial cost of each fraud is on the rise.

Fig 1: Reported rate of economic crime



This year's report illustrates how economic crime has evolved over the last two years, morphing into different forms depending on industrial sector and region.

Despite this evolving threat, we have seen a decrease in the detection of criminal activity by methods within management's control, with detection through corporate controls down by 7%. What's more, one in five organisations (22%) have not carried out a single fraud risk assessment in the last 24 months. When looked at in the context of the findings in PwC's 19th Annual Global CEO Survey – where two-thirds of chief executives agreed that there are more threats to the growth of their company than ever before (a sharp increase, compared to 59% in 2015) – this points to a potentially worrying trend: that too much is being left to chance. In fact, our findings indicate that one in ten economic crimes are discovered by accident.

> ***Our findings indicate that 1 in 10 economic crimes are discovered by accident***

Today more than ever before, a passive approach to detecting and preventing economic crime is a recipe for disaster. To underscore this fact, our survey uncovered a widespread lack of confidence in local law enforcement – a phenomenon that is not limited to regions or level of economic development.

The message is clear: the burden of preventing, protecting and responding to economic crime rests firmly with organisations themselves.

Our survey this year focuses on three key areas – Cybercrime, Ethics and compliance programmes and Anti-money laundering – and explores certain common themes, including managing the risks associated with the pervasion of technology; what it means to conduct business responsibly across a widening business landscape; and integrating ethical conduct into decision-making.

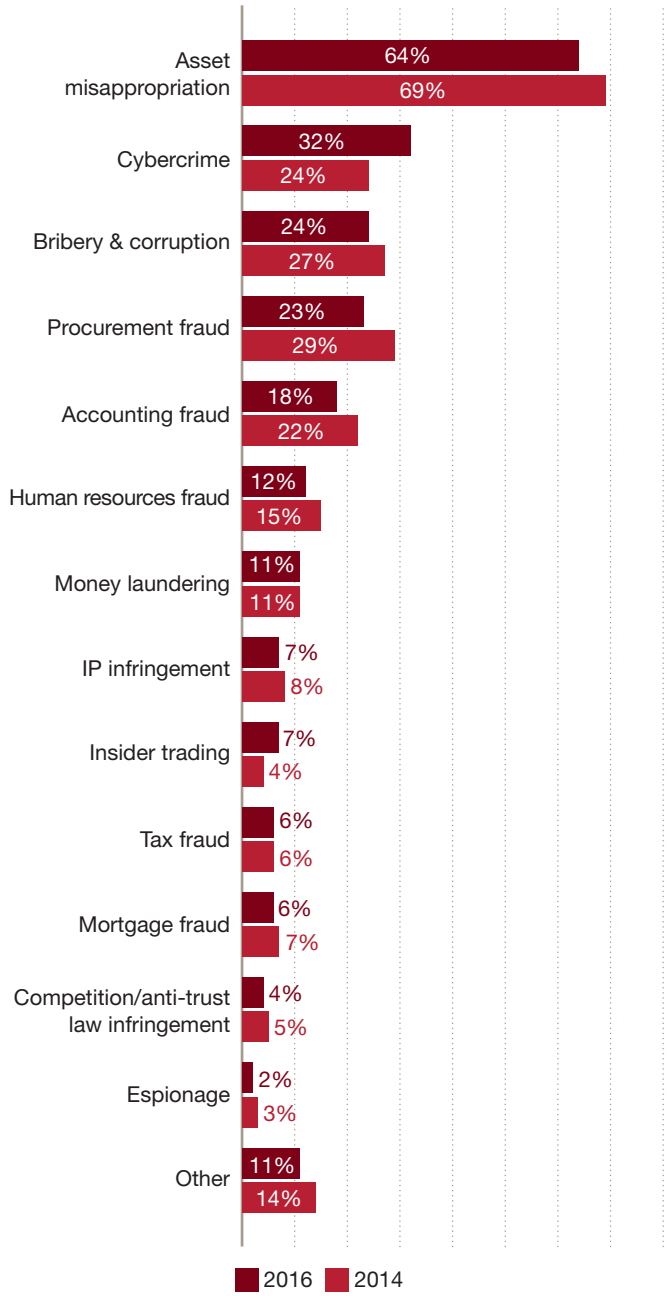
In addition to highlighting specific areas of economic crime worth focusing on, we emphasise the things you can do better to tackle them – implementing more sophisticated and effective measures that can not only reduce these risks, but also bring the benefits of a more threat-aware business, confident of its defences in a changing world.

Top 3 most commonly reported types of economic crime in 2016

Age-old crimes lead, but one pervasive enemy jumps ahead

The most pervasive economic crimes reported by our respondents for 2016 are highlighted in the figure below:

Fig 2: Types of economic crime experienced



While asset misappropriation, bribery and corruption, procurement fraud and accounting fraud – the traditional leaders in this category – all showed a slight decrease this year over 2014's statistics, one crime has been on a steady increase everywhere since it first appeared in our survey back in 2011. Cybercrime has now jumped to second place.

Asset misappropriation has historically been regarded as the easiest of frauds to detect, and the levels of this crime reported in our survey have previously been fairly easy to predict. However, since 2011, we have seen a downward trend in the reported rates of this particular crime. This could be as a result of a tightening of organisational controls – and that organisations are getting better at preventing traditional economic crime. This in turn could mean that it is evolving into different, higher-impact types of fraud, including cybercrime.

When considered in the light of the decreased rate of detection by means under management control – and of the increased prevalence of cybercrime – we must ask ourselves: are these crimes becoming harder to detect or are we simply becoming less aware of changing threats our businesses face? And the more important question: what should we do about this?

With 20% of our survey respondents on average believing that it is likely that their organisations will experience these leading economic crimes in the next 24 months, the time is right for a fresh look.

Economic crime: a global problem, but not the same everywhere

Region	Reported economic crime in 2016	Reported economic crime in 2014
Africa	57%	50%
Western Europe	40%	35%
North America	37%	41%
Eastern Europe	33%	39%
Asia Pacific	30%	32%
Latin America	28%	35%
Middle East	25%	21%
Global	**36%**	**37%**

While some regions reported lower rates of economic crime and the global trend was steady, Africa, Western Europe and the Middle East showed significant increases in our 2016 survey. The main drivers for the high and/or increased reported rates of economic crime in Africa were South Africa (69%, unchanged since 2014), followed by Kenya (61%, up 17% over 2014) and Zambia (61%, up 35% over 2014), while in the Middle East, respondents from Saudi Arabia reported that rates of economic crime more than doubled from 11% in 2014 to 24% in 2016.

Western Europe was led by France (68%) and the United Kingdom (55%), both increased by 25% relative to 2014. The significant increase for France was attributable to a jump in external frauds – predominantly cybercrime, which nearly doubled, from 28% in 2014 to 53% in 2016. In the United Kingdom, the increase was driven by an 83% increase in reported cybercrime incidents, relative to 2014.

At the regional level, while most have experienced increased incidents of cybercrime, Eastern Europe reported a fall of 2% (10% lower than the global average). Cybercrime also does not feature in the top three types of economic crimes experienced in Africa, Asia Pacific and Eastern Europe. These regions, on the other hand, have higher-than-global-average incidences of bribery and corruption and procurement fraud.

While most developed countries have seen increased regulatory attention – particularly around sensitive issues such as cybercrime, money laundering and bribery and corruption – the blurring of borders through the transnational nature of criminal activities is prompting a growing level of international cooperation in regulation and enforcement.

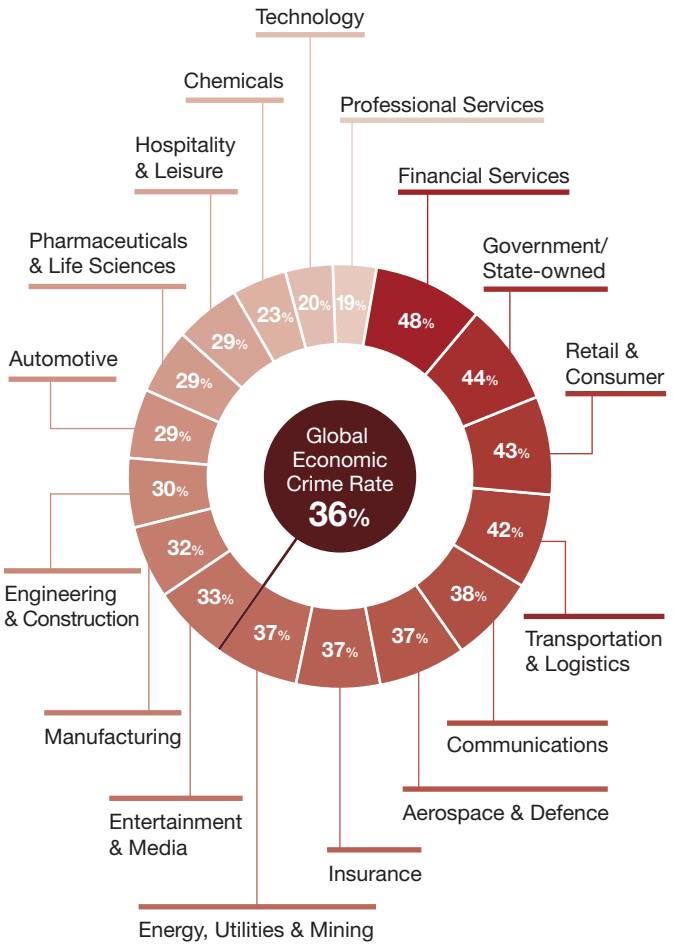
Lest an observer be tempted to fall into familiar thinking, these statistics demonstrate that economic crime is very much a diversified global issue – both in type of crime and across emerging and developed markets. Understanding these differences can help organisations focus their prevention efforts in the right areas.

The opportunity thus exists for all organisations – no matter their size or geographic diversity – to take a global view and to apply international standards to their efforts to combat economic crime.

How is economic crime affecting your industry?

Financial services has traditionally proven to be the industry most threatened by economic crime, as it serves the financial needs of all other industries.

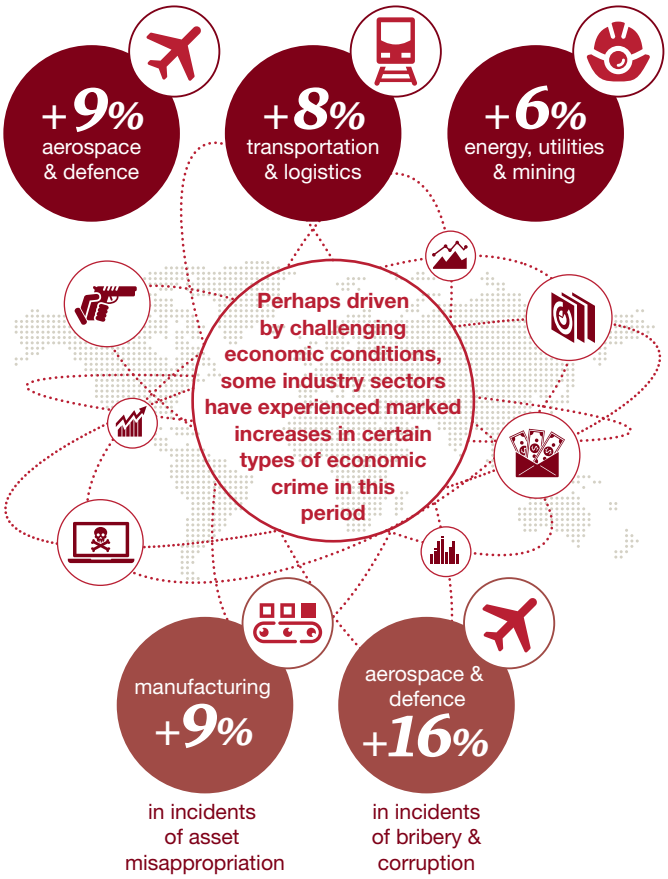
Fig 3: Which industries are at risk?



However, with the market evolving toward integrated business solutions, many organisations outside financial services are taking on activities traditionally undertaken by banks. Numerous non-financial services businesses in the automotive, retail and consumer and communications sectors, to name just a few, are either in joint arrangements with financial services companies or are in possession of banking licences of their own. Fraudsters seeking to "follow the cash" now have many more avenues to fulfil their objectives.

While the financial services industry, by virtue of its highly regulated environment, has over the decades built up sophisticated control mechanisms, detection methodologies and risk management tools, the hybrids have generally yet to come into their own in managing either the risks or the fast-evolving compliance landscape they now find themselves in.

The biggest industry sector rises in the incidence of economic crime in the past 24 months



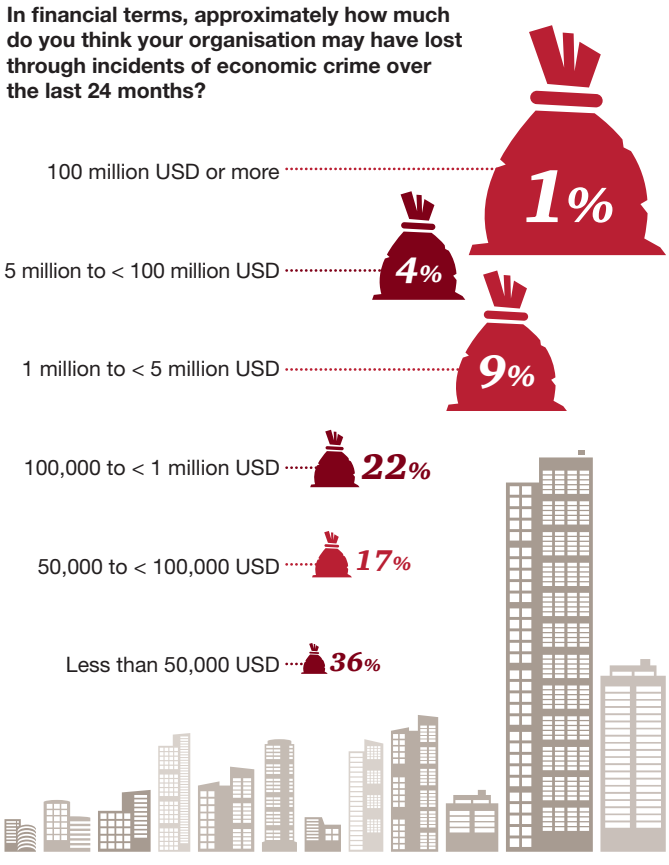
As market conditions change, so does the threat landscape. Regular re-assessment is key in preventing economic crime.

Rising financial & collateral damage

Losses can be stiff. Nearly a quarter (22%) of respondents experienced losses of between $100,000 and $1 million, 14% of respondents suffered losses of more than $1 million, and 1% of respondents (primarily from North America and Asia-Pacific) reported losses in excess of $100 million. These are substantial sums of money and are representative of a trend of rising costs of individual frauds.

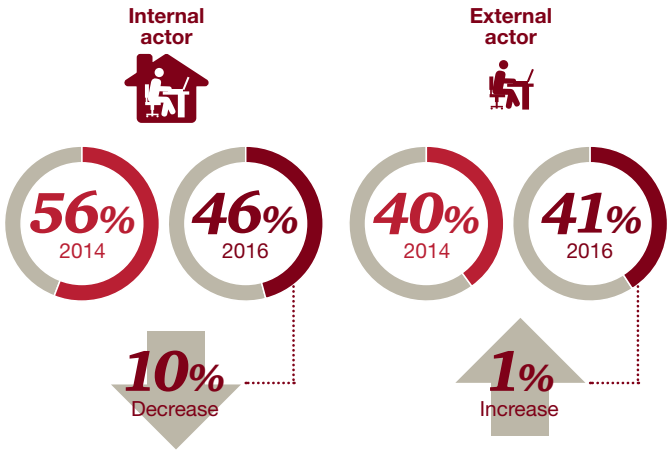
The true cost of economic crime to the global economy is difficult to estimate, especially considering that actual financial loss is often only a small component of the fallout from a serious incident. Our survey respondents consistently note wider collateral damage including business disruptions, remedial measures, investigative and preventative interventions, regulatory fines, legal fees – and, critically – damage to morale and reputation as having a significant impact on long-term business performance. These kinds of losses, of course, while not always quantifiable, can over time dwarf the relatively shorter-term impact of financial losses.

Fig 4: Financial impact of economic crime



Profile of the fraudster

Since our last survey, we've seen the gap between internal and external fraud actor is closing.



More than half of internal perpetrators still originate from middle and senior management, but junior management also contributed a great deal to the perpetration of internal fraud in some regions. This points to a potential weakness in internal controls, whereby these measures serve as check-box exercises rather than effective processes embedded into an organisation's culture. This is further suggested by the fact that 22% of respondents have never carried out a fraud risk assessment and a further 31% only carry out such an assessment annually.

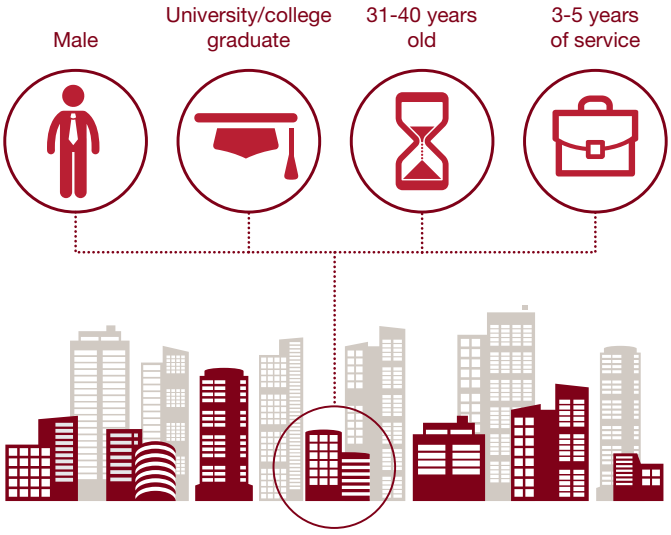
In some regions (for example Asia Pacific), senior management fraud, which is the hardest to detect and tends to have a much greater impact, has jumped significantly.

At the regional level, internal actors remain the main perpetrators of fraud in Africa (7% higher than the global average), Asia Pacific (9% higher) and Latin America (9% higher), despite significant falls in respondents stating internal actors were responsible for perpetrating fraud (6% – 15% decline across these regions since 2014).

Conversely, external actors were responsible for more fraud incidents in Eastern Europe (44%), Western Europe (49%) and North America (56%) compared to the global average of 41%.

The most fundamental change in perpetrator type was in North America where there was a very significant swing from internal to external perpetrators.

Most likely characteristics of the internal fraudster

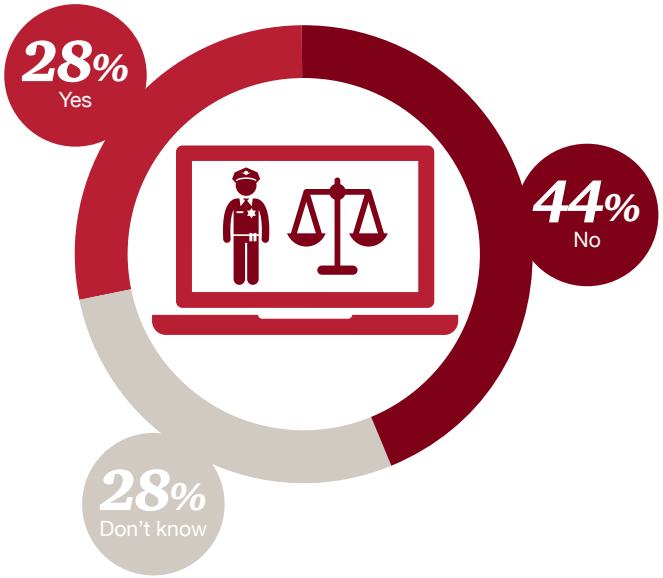


Perception of law enforcement

We asked respondents to give us their views on whether they believe local law enforcement to be adequately resourced and trained to investigate and prosecute economic crime. A resounding majority – 44% to 28% – expressed doubts on this point, while a further 28% could not answer.

This metric could result from several divergent factors. These could include the countrywide rate of economic crime, the extent to which law enforcement in the respective country publicises or downplays its expertise in certain areas like cybercrime, and the extent to which law enforcement is perceived to be above political interference.

Fig 5: Do respondents believe local law enforcement agencies are adequately resourced and trained to investigate and prosecute economic crime?



Top 15 countries that believe their local law enforcement agencies are not adequately resourced to combat economic crime

1	Kenya	79%
2	South Africa	70%
3	Turkey	60%
4	Philippines	58%
5	Bulgaria	58%
6	Poland	58%
7	Ukraine	57%
8	Mexico	56%
9	Zambia	55%
10	Nigeria	54%
11	Australia	52%
12	United States	52%
13	France	51%
14	Venezuela	50%
15	India	49%

Forewarned, forearmed, forward

Economic crime is ever-evolving, and becoming a more complex issue for organisations and economies. The regulatory landscape, is also changing, bringing with it numerous challenges to doing business. With local law enforcement not necessarily perceived as able to make a material difference, the onus is squarely on the shoulders of the business community to protect itself, and its stakeholders, from economic crime.

As we discuss in the three upcoming sections – dedicated to the strategically crucial areas of cybercrime, ethics and compliance programmes and anti-money laundering – our survey numbers can help uncover not only potentially troublesome red flags and trends. They can also serve as vitally important indicators of areas of opportunity for forward-thinking organisations to meet the challenges of a whole new world. To be forewarned is to be forearmed for success.

Cybercrime

Although military assets are assumed to be highly secure, hackers have found that "low-risk" suppliers have gaps in their security, which can be easily exploited and used to track the destination of these supplies.

A boundless threat

Digital technology continues to transform and disrupt the world of business, exposing organisations to both opportunities and threats. So it's hardly surprising that cybercrime continues to escalate – ranking as this year's second most reported economic crime.

The reality in 2016 is that like every other aspect of commerce, economic crime has, to some extent, gone digital. In a hyper-connected business ecosystem that frequently straddles jurisdictions, a breach in any node of that system – including third parties such as service providers, business partners or government authorities – can compromise the organisation's digital landscape in a variety of ways. What's more, cyber risk now encompasses more than our traditional view of computers: we've observed a sharp increase in attack activity involving the so-called Internet of Things, including cars and household devices.

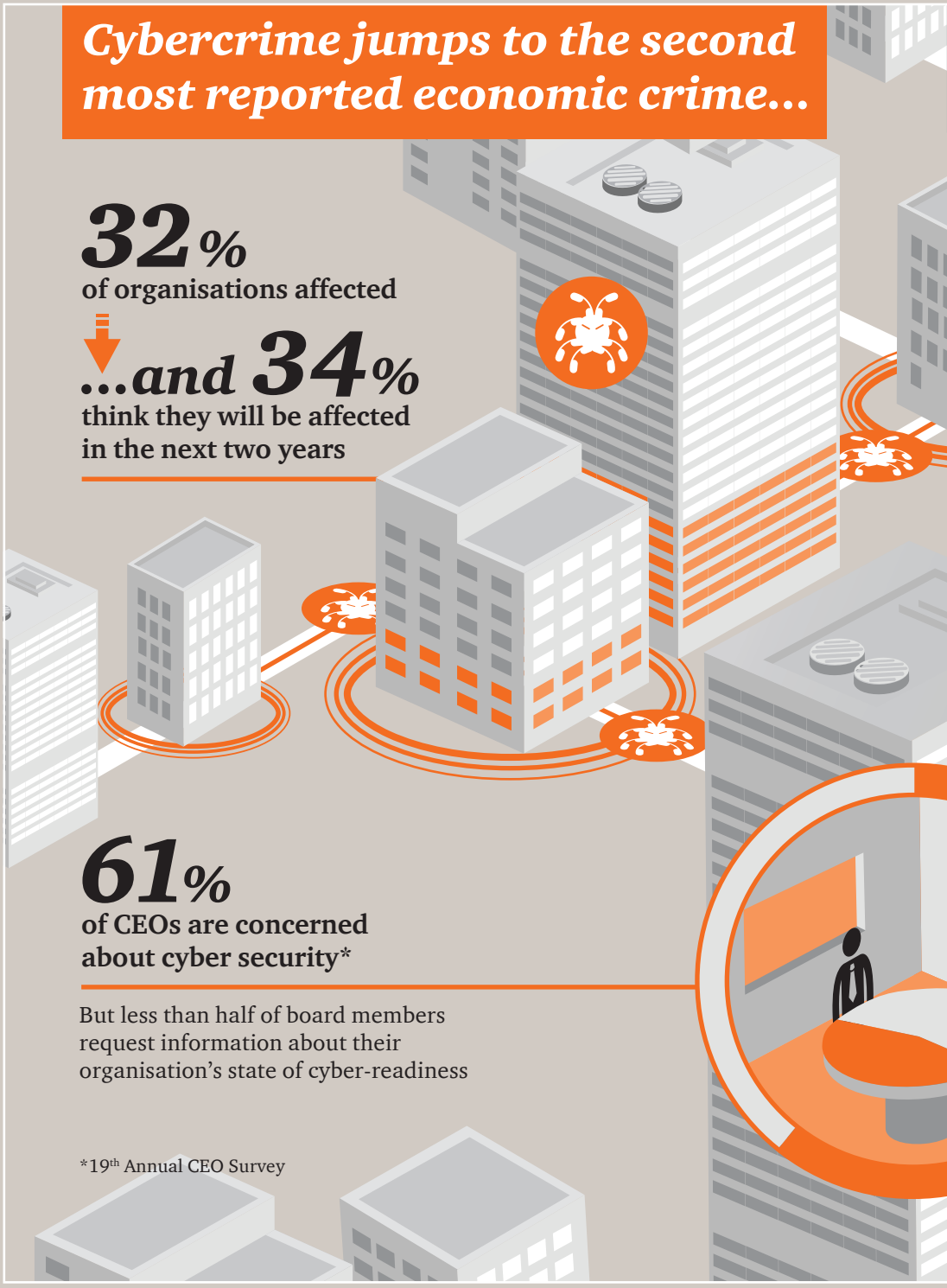
Here's the digital paradox: organisations today are able to cover more ground, more quickly, than ever before – thanks to new digital connections, tools and platforms which can connect them in real time with customers, suppliers and partners. Yet at the same time cybercrime has become a powerful countervailing force that's limiting that potential.

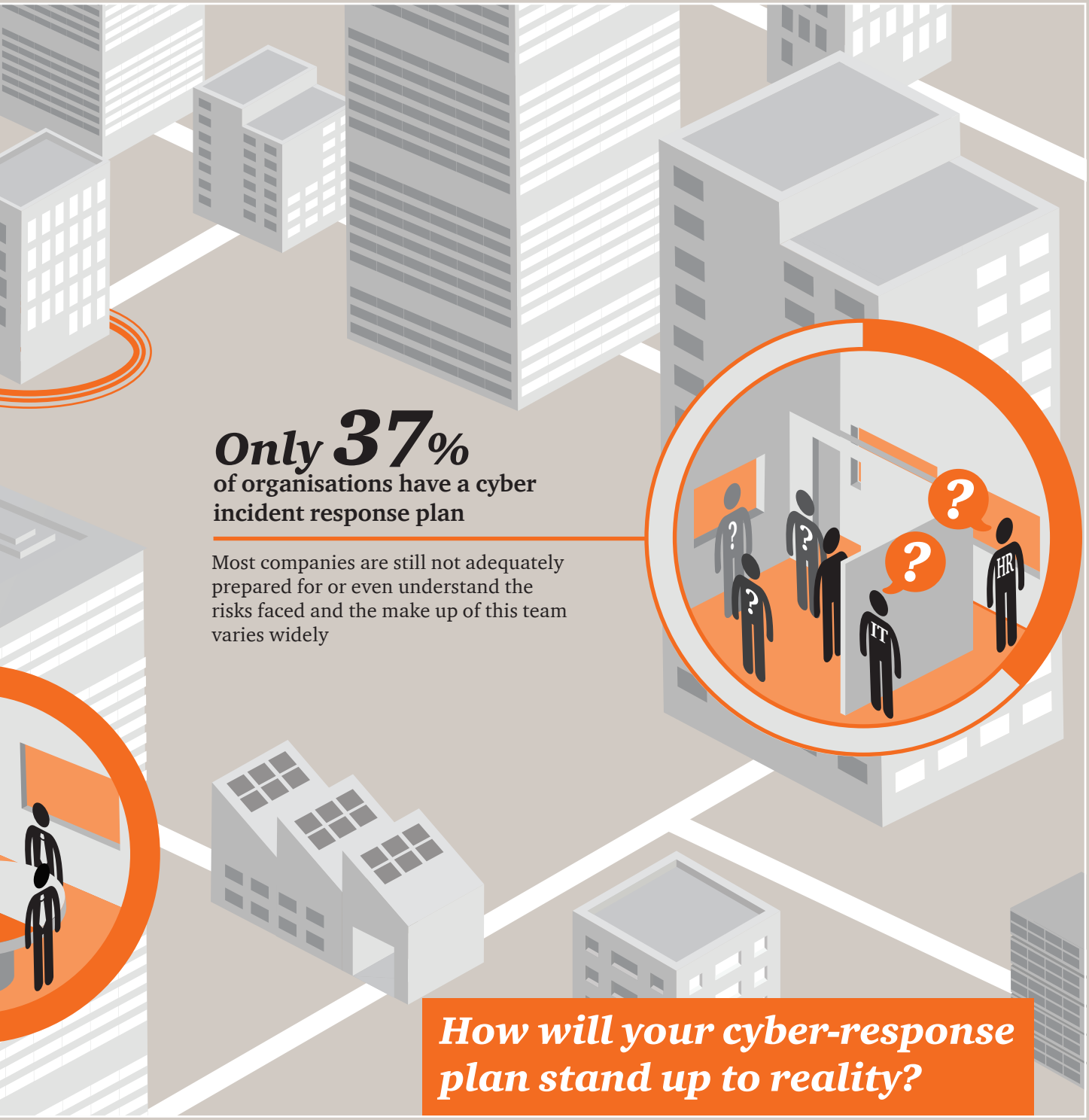
And business leaders worry it's holding them back. In PwC's 19th Annual Global CEO Survey, six in ten chief executives ranked cyber threats and the speed of technological change as top threats to growth.

This year's global economic crime survey points to the disquieting fact that too many organisations are leaving first response to their IT teams without adequate intervention or support from senior management and other key players. What's more, the composition of these response teams is often fundamentally flawed, which ultimately affects the handling of breaches.

From our firm-wide work on digital strategy and execution with thousands of companies globally, we've identified practices that distinguish leaders in the digital age. Chief among these is a proactive stance when it comes to cybersecurity and privacy. This necessitates that everyone in the organisation – from the board and C-suite to middle management and hourly workers – sees it as their responsibility.

Cybercrime continues to escalate in a hyperconnected business ecosystem – jumping to 2nd most reported economic crime

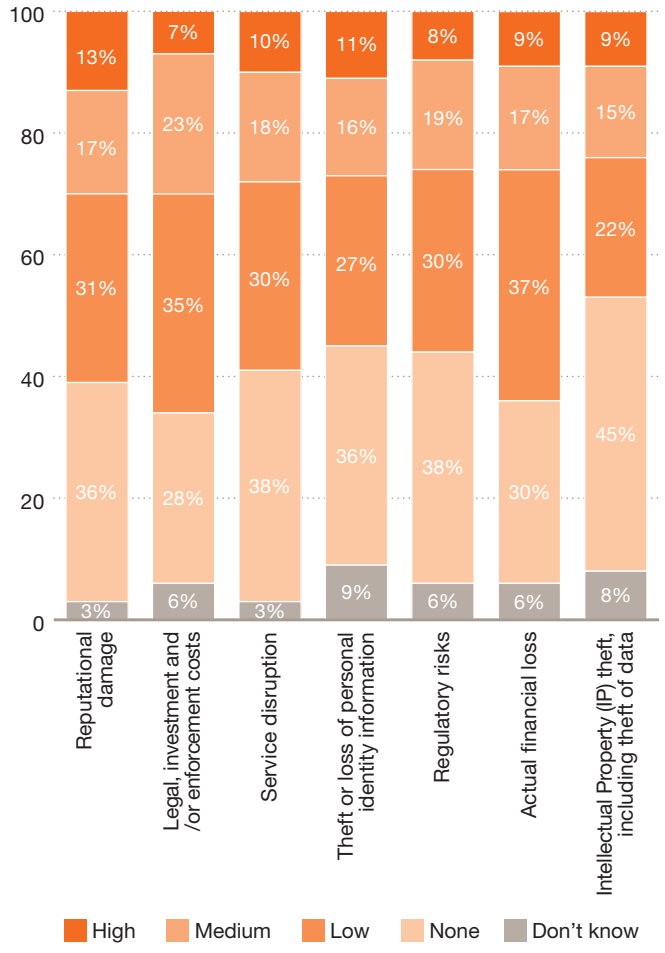



Only 37%
of organisations have a cyber incident response plan
Most companies are still not adequately prepared for or even understand the risks faced and the make up of this team varies widely
HR
IT
How will your cyber-response plan stand up to reality?

Key findings: Cybercrime keeps climbing

The incidence of reported cybercrime among our respondents is sharply higher this year, jumping from 4th to 2nd place among the most-reported types of economic crime. Notably, it was the only economic crime to have registered an increase in that category. Over a quarter of respondents told us they'd been affected by cybercrime. Ominously, another 18% said they didn't know whether they had or not.

Fig 6: Level of impact of cybercrime



Losses can be heavy. A handful of respondents (approximately 50 organisations) said they had suffered losses over $5 million; of these, nearly a third reported cybercrime-related losses in excess of $100 million.

Among survey respondents, reputational damage was considered the most damaging impact of a cyber breach – followed closely by legal, investment and/or enforcement costs.

The insidious nature of this threat is such that of the 56% who say they are not victims, many have likely been compromised without knowing it. A concerning trend we have observed is that of hackers managing to remain on organisations' networks for extended periods of time without being detected.

Attackers are also known to stage diversionary attacks to conceal more damaging activity. Diversionary techniques include the use of distributed denial of service attacks as a means of distracting and creating a lot of noise while the real focus of the attack unfolds in a slow and undetected manner. Typically in such a scenario attackers would launch attacks against systems which provide no value to them – this is done simply to misdirect incident response teams whilst in the background attackers are exfiltrating the actual information they were seeking.

Which industries are at risk for cybercrime?

Today, all industries are at risk – including some which may have considered themselves unlikely targets in the past. According to PwC's Global State of Information Security Survey 2016, the sector registering the most significant increase in cybercrime activity in 2015 was retail, while financial services – still one of the most attacked sectors – had levelled out, with very little growth in terms of number of attacks over the last three years.

Why do companies (and nation-states) steal intellectual property?

- Many developed nations are seeing a pattern in large-scale IP-focused breaches. These are not random individual company attacks, but rather parts of a larger-scale, strategically organised campaign.
- While nation-states may be behind some of these large-scale attacks, this is not a terrorism issue attempting to cripple vital infrastructure, it is an economic crime issue.
- There is an economic rationale in stealing another company's intellectual property (IP). It is less expensive in time and resources than conducting one's own R&D.
- The advice is: if you see someone else in your sector getting attacked, it is wise to assume you may be next in the bullseye.

The two kinds of cybercrime – and what they mean for you

We've come a long way from the days of teenaged hackers stealing bank cards. There's been a significant and laudable increase in awareness and sophistication in detecting the identity (or provenance) of an attacker. Still, the fact remains that the conflict between criminals and companies is as feverish as ever. For companies, it's a battle that can never really be won.

Over the last few years, cyber economic crime has evolved to a point where one could segment it into two distinct categories – the kind that steal money and bruise reputations; and the kind that steal IP and lays waste to an entire business.

- **Cyber fraud.** Monetisable cybercrime, such as identity and payment card theft, are the events that tend to grab the headlines, with millions of dollars of losses and as many victims. Despite their high profile, they rarely pose an existential threat to companies.
- **Transfer-of-wealth/IP attacks**. The more critical economic crime facing organisations is that of international cyber espionage: the theft of critical IP – trade secrets, product information, negotiating strategies and the like. Cyber professionals call such breaches "extinction-level events", and for good reason: the damage could extend to the billions of dollars, and include destruction of a line of business, a company or even a larger economic ecosystem. Not only are these kinds of attacks difficult to detect, they may not even be on a company's threat radar.

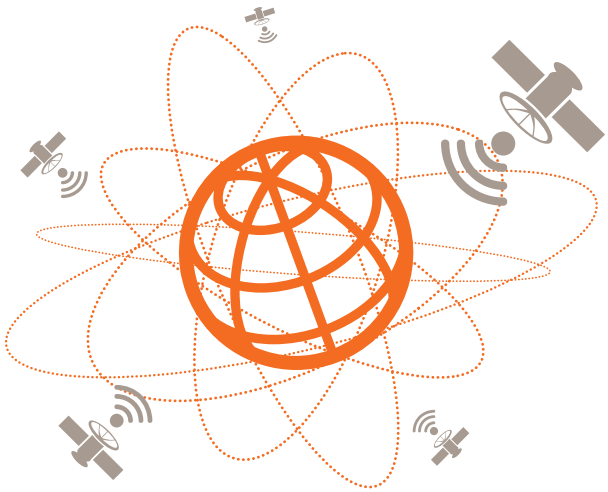
While the long-term damage, both to the entity and the economy, is potentially far higher for transfer-of-wealth attacks, the regulatory pain and media scrutiny arising from the theft of credit cards or personally identifiable information can be vast.

Threat vectors: the five categories

Nation-states
threats include espionage and cyber warfare - victims include government agencies, infrastructure, energy and IP-rich organisations

Insiders
not only your employees but also trusted third parties with access to sensitive data who are not directly under your control

Terrorists
still a relatively nascent threat - threats include disruption and cyber warfare; victims include government agencies, infrastructure and energy



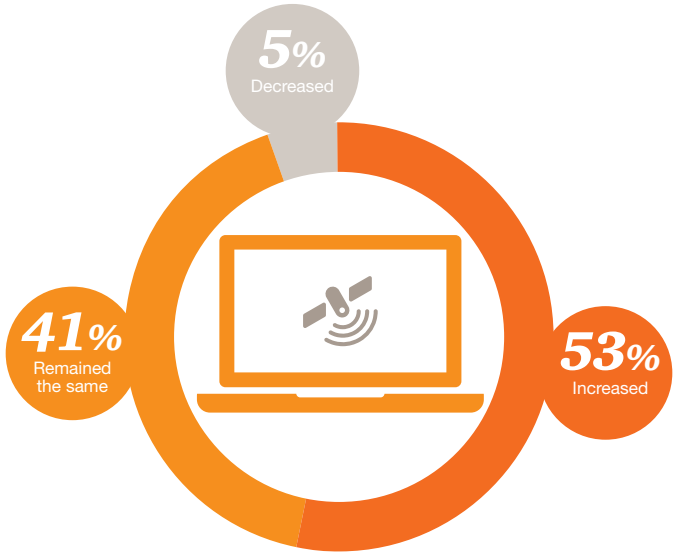
Organised crime syndicates
threats include theft of financial or personally identifiable information (sometimes with the collusion of insiders) - victims include financial institutions, retailers, medical and hospitality companies

Hacktivists
threats include service disruptions or reputational damage; victims include high-profile organisations and governments - victims can include any kind of organisation

Ready or not

Over half of our survey respondents (53%, up 10% over 2014) see an increased risk of cyber threats, perhaps due to intensifying media coverage. But our survey suggests that companies are nonetheless inadequately prepared to face current cyber threats.

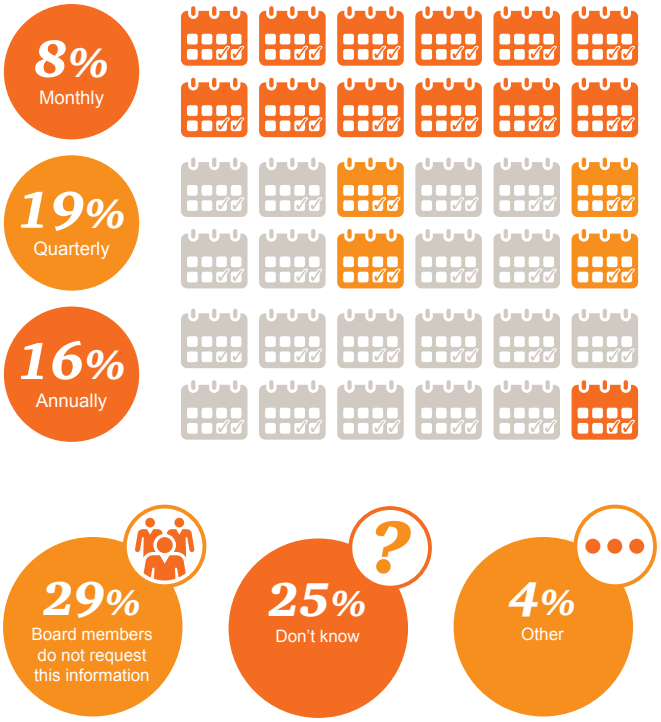
Fig 7: Perception of the risk of cybercrime



Responsibility for redressing cyber vulnerabilities starts at the top. Yet our survey suggests that many boards are not sufficiently proactive regarding cyber threats, and generally do not understand their organisation's digital footprint well enough to properly assess the risks, despite the fact that in several countries boards have a fiduciary responsibility to shareholders when it comes to cyber risk (for example, the U.S. Securities and Exchange Commission has issued a warning that future examinations will consider a company's cyber response capabilities[1]). Astoundingly, less than half of board members actually request information about their organisation's state of cyber-readiness.

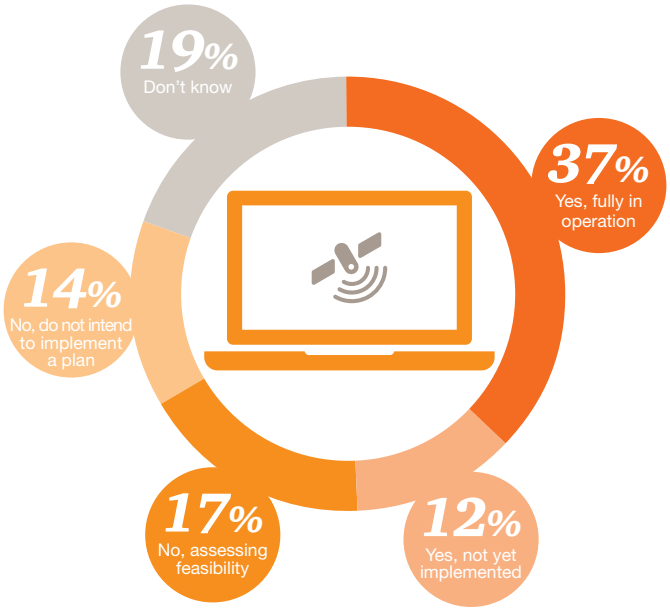
1) https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

Fig 8: Frequency of requests for information by boards regarding organisations' ability to deal with cyber incidents



Only 37% of respondents – most of them in the heavily regulated financial services industry – have a fully operational incident response plan. Three in ten have no plan at all, and of these, nearly half don't think they need one.

Fig 9: Do organisations have Incident Response Plans to deal with cyber-attacks?



Should a cyber crisis arrive, only four in ten companies have personnel that are "fully trained" to act as first responders, of which the overwhelming majority (73%) are IT security staff.

"If you are the leader of a business, you should know how strong your company's defenses are, you should know if there are response plans in place in case a significant security breach occurs, and you should be getting regular reports on cyber security threats and what your company is doing to respond to those threats."

Jacob Lew, U.S. Secretary of the Treasury, July 2014

While IT has a critical role to play in detecting and attempting to deflect an attack, it is noteworthy that fewer than half of first responder teams included members focused on the higher-level management of the crisis – senior management (46%), legal (25%), HR (14%), and the like. Only one in ten incident response teams included digital forensic investigators.

These results suggest that many organisations, in their understandable haste to contain the breach and get their systems up and working again, are at risk of overlooking potentially crucial evidence, which could later hamper their ability to prosecute and, more importantly, to understand how the breach occurred.

An insufficiently coordinated response might also limit the organisation's ability to investigate all the areas that have actually been breached, especially critical considering hackers' frequent use of diversion techniques.

Finally, excessive haste in responding to an attack can hamper the company's ability to fully understand the holistic impact of the breach, and communicate appropriately to both internal and external stakeholders, including the media. This could lead to reputational harm (ranked in this year's survey as the most damaging impact of a cyber breach).

Fig 10: Cybercrime First Responder Teams

Detecting a breach: Crisis management

What happens when you learn of a breach? It's critical to shrink the interval between effective detection and response – and interrupt damaging business impacts as quickly as possible. After calling up your crisis and cyber first responders, here are some steps you can take:

- Get the essential facts about the breach, and find out if it is still ongoing. With the increasing complexity of networks, it can be difficult to identify how a hostile actor might have entered the network. Sophisticated forensic and data analysis tools – some of which are available from outside experts, and others from law enforcement – are critical to this phase.
- Consider that a detected attack can sometimes mask deeper incursions into your organisation, and that in some situations it may take weeks, not hours, to detect a breach and begin to stem the damage.
- Decide whether and to what extent to seek the involvement of law enforcement, and whether the appropriate agency is local or federal. There are many factors to consider, and they will vary according to the type and scale of the attack. This is a significant issue, considering that nearly half of responders doubt the government's ability to investigate cybercrime.
- Consider secondary risks. For example, a simple email breach can reveal secrets to adversaries. If networks are breached, and the company uses VOIP/networked phone services, the telephones are also likely to be compromised.
- Finally, when a breach occurs,remember that a cyber investigation is still fundamentally an investigation, and the principles of a criminal investigation still apply. In focusing on stopping an ongoing attack and getting back on line, it's crucial not to inadvertently destroy evidence that could help with that investigation – and with preventing the next attack.

The importance of a multi-layered defence

Cyber threats and mitigations are the responsibility of the entire enterprise; all have a crucial part to play. Yet while we have seen major strides in the sophistication of cyber-preparedness since our last survey, most companies are still not adequately prepared either to understand the risks they face, nor to anticipate and manage incidents effectively.

Too many organisations are suffering cyber losses because they didn't get the basics right. From insufficient board involvement (or readiness-awareness), to poor system configurations and inadequate controls on third parties with access to the network, companies are suffering from unforced errors, often leaving the cyber door ajar for intruders.

It is vital that boards incorporate cybercrime into their routine risk assessments, communicate the plan up, down and across organisational lines, and discuss specifically with the IT department at what point they want to be alerted of a breach.

Cyber threats must be understood and planned for in the same way as any other potential business threat or disruption (such as acts of terrorism or a natural disaster): with a response plan, roles and responsibilities, monitoring and scenario planning. That's why leading companies are integrating crisis management exercises as a central element of their cybersecurity and incident response strategy. They convene regular table-top exercises examining specific scenarios and pressure-test their response plans, identifying any gaps or shortfalls.

IT threats & mitigations are the responsibility of the entire organisation

Executive level:

- Institute sound cybersecurity strategy
- Ensure quality information is received and assimilated
- Implement user security awareness programmes
- Support strategy-based spending on security

Audit & Risk:

- Ensure a thorough understanding and coverage of technology risks
- Conduct up-front due diligence to mitigate risks associated with third parties
- Address risks associated with operational (non-financial) systems
- Address basic IT audit issues

Legal:

- Track the evolving cyber-regulatory environment
- Monitor decisions made by regulators in response to cyber incidents
- Be aware of factors that can void cyber insurance

IT:

- Conduct forensic readiness assessments
- Be aware of the changing threat landscape and attack vectors
- Test incident response plans
- Implement effective monitoring processes
- Employ new strategies: cyber attack simulations, gamification of security training and awareness sessions and security data analytics

A corporate cyber crisis is one of the most complex and challenging issues an organisation can face. Cyber breaches require sophisticated communications and investigative strategies – including significant forensic and analytical capabilities – executed with precision, agility and a cool head.

Although potentially daunting, ramping up preparedness has its silver lining: you can view it as an organisational stress test – one that can and should lead to improvements in your processes. In today's risk landscape, a company's degree of readiness to handle a cyber crisis can also be a marker of competitive advantage and, ultimately, survival.

"A lack of cyber-readiness basics can leave the cybersecurity door ajar for intruders."

David Burg, PwC's Global and Co-US Cybersecurity Leader

Plans are good – but practice is everything

Many companies go to great lengths and conduct various exercises to ensure that they are prepared for cyber incidents.

Unfortunately, plans rarely survive first contact with reality, which tends to present incident responders and crisis managers with unforeseen circumstances.

An effective crisis response requires the skills, knowledge, and experience of a range of corporate functions working in concert: legal, human resources, media and public relations, communications, privacy counsel, audit and risk, finance, corporate security, regulatory and law enforcement relations, shareholder relations, as well as the front-line business units and regional management.

The process – the "plan for a plan" – that comes of a regular exercise programme is far more valuable than the plans it produces. It generates "muscle memory" for incident response, making the process, the environment, and the decision-making construct second-nature to the stakeholders who will be under pressure in a crisis, so they can focus on solving the issue at hand.

Key contacts

David B. Burg
Global and Co-US Advisory
Cybersecurity and Privacy Leader

t: +1 (703) 918 1067
e: david.b.burg@us.pwc.com

Kris McConkey
Partner
United Kingdom

t: +44(0) 77 2570 7360
e: kris.mcconkey@uk.pwc.com

Junaid Amra
Associate Director
South Africa

t: +27 (31) 271 2302
e: junaid.amra@za.pwc.com

Ethics & compliance

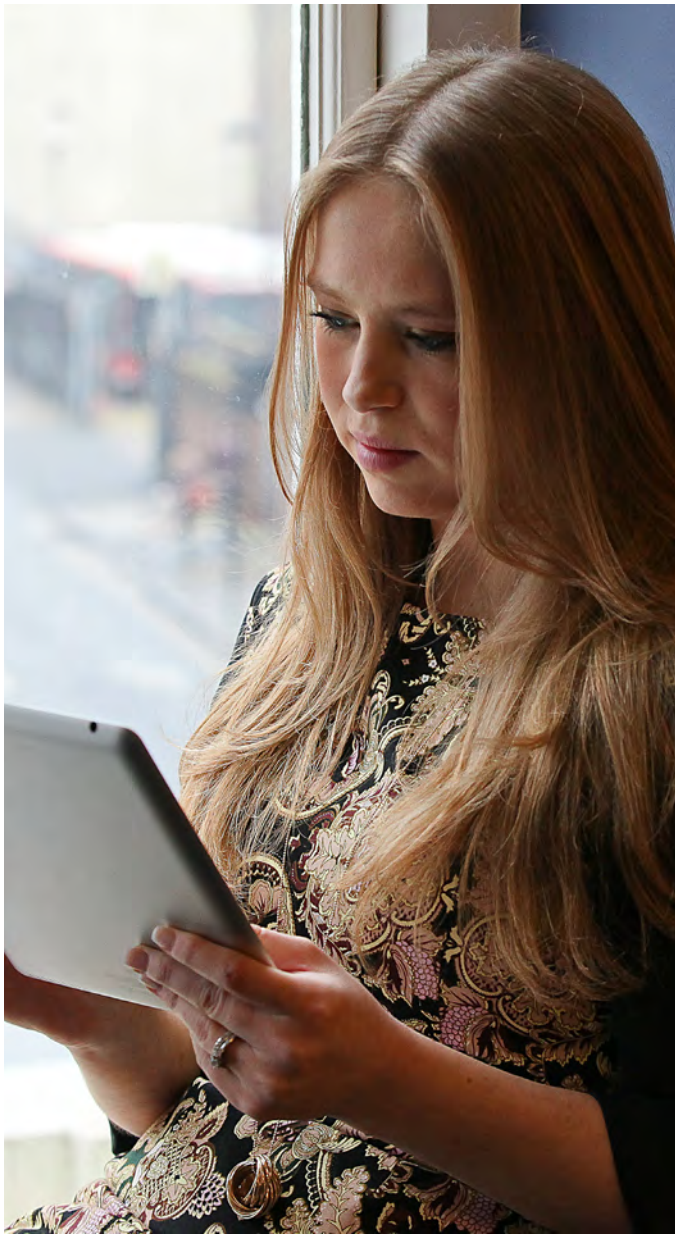
Managing the balance between trust and compliance can be the difference between retaining or losing top talent. In today's continuously evolving marketplace, it's vital to have a strategy to align ethics and compliance with business risks

Aligning decision-making with values

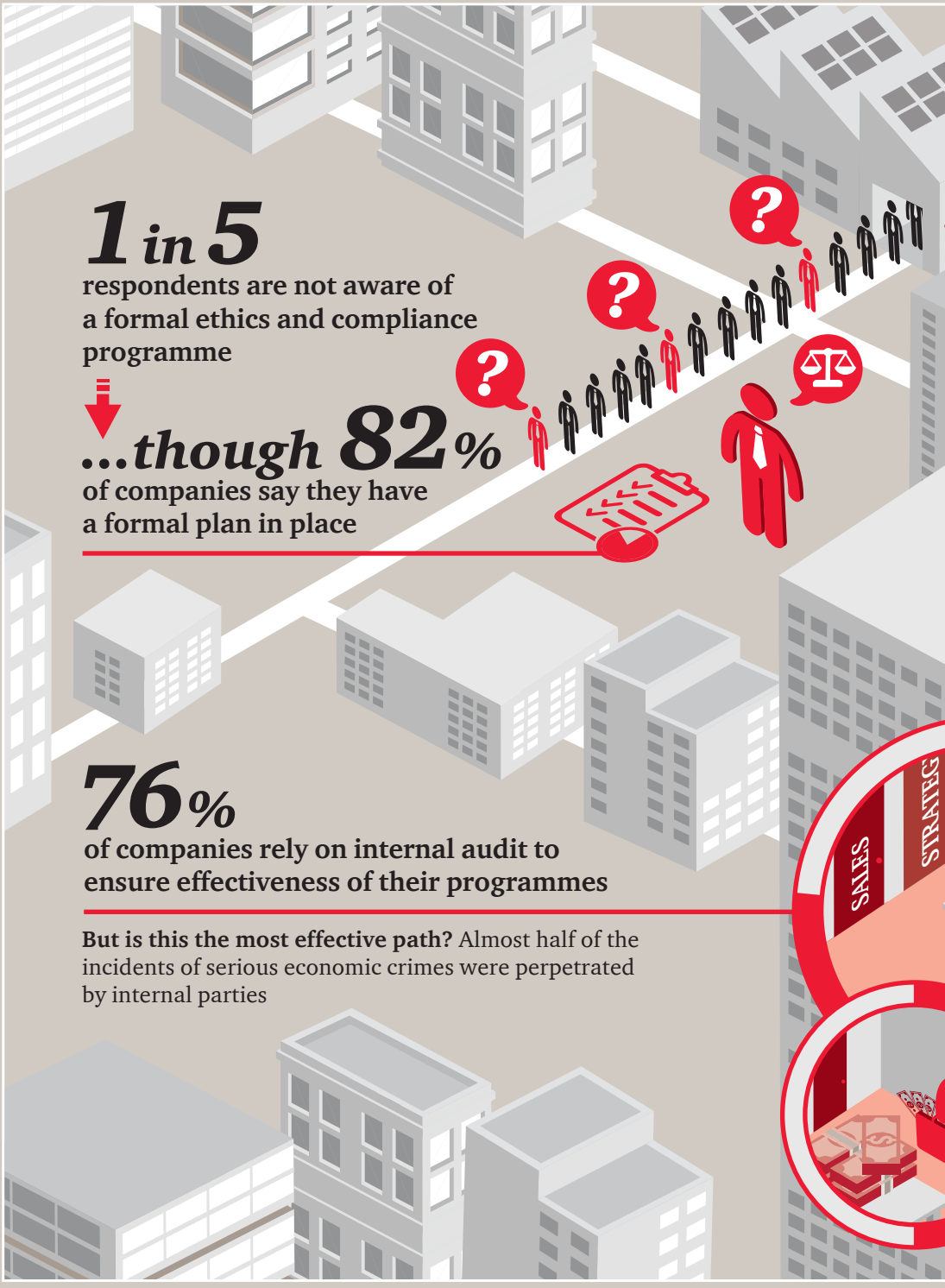
Our survey results show that not only are the number of economic crime risks increasing, so too are the complexity of those risks and the role that technology plays. This is hardly a surprise in a business environment characterised by growing globalisation, increasingly vigilant enforcement and greater demand for public accountability.

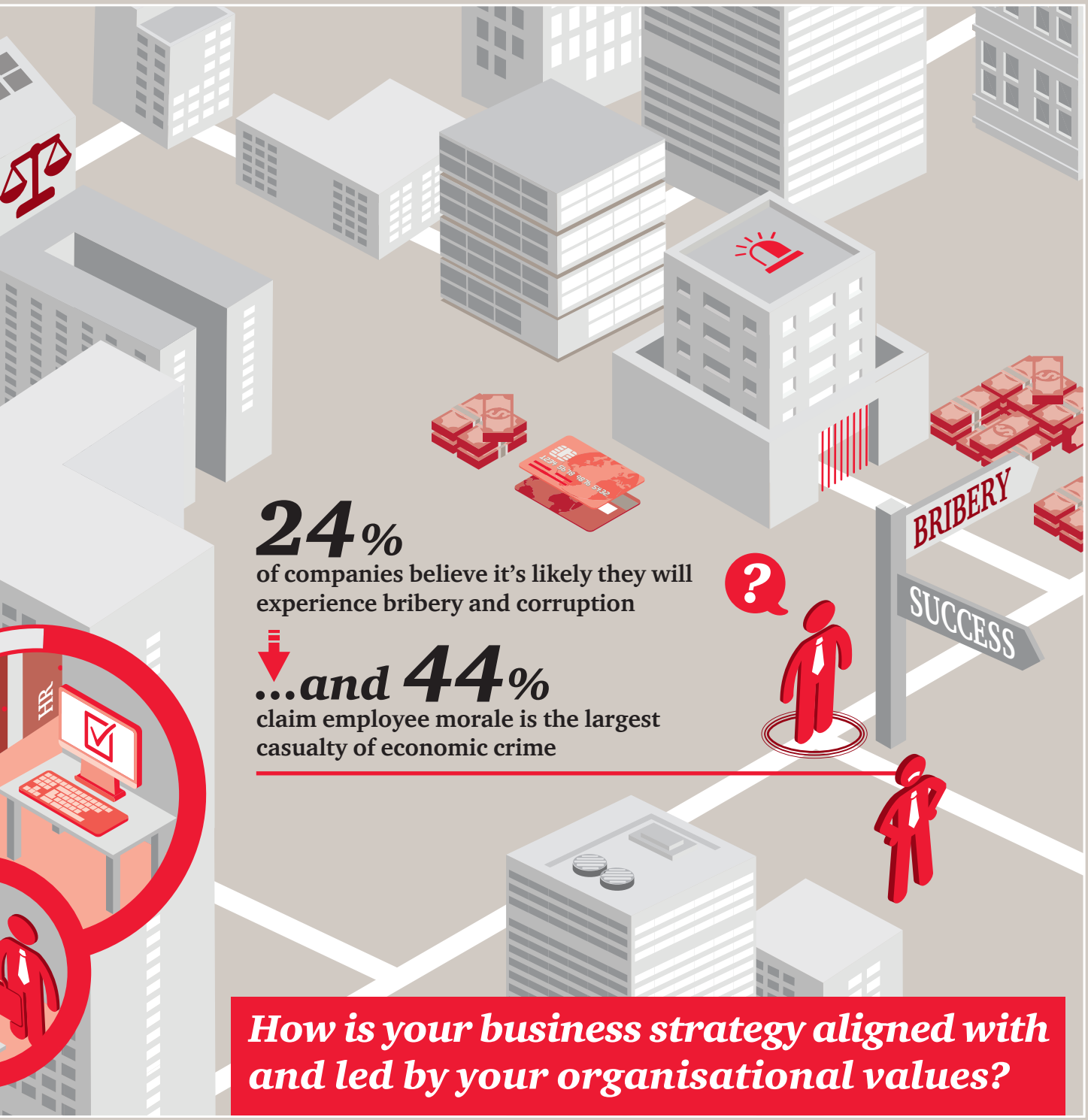
That's why your ability to identify and mitigate compliance risks needs to evolve at a rapid pace. A risk-based approach to ethics and compliance – one that begins with a holistic understanding of your economic crime risk, and an understanding of where your compliance weaknesses are – is a must-have. From that position of clarity, you can create an effective programme that mitigates those risks, and positions you for reaching your business goals. Yet a worrying 22% of organisations have not carried out a fraud risk assessment in the past 24 months.

While the number of organisations reporting fraud overall has, at 36%, remained fairly consistent in recent years, a closer reading of the data reveals important nuances. Most "traditional" frauds (such as asset misappropriation, accounting fraud, and bribery and corruption) have fallen somewhat from their 2014 levels. Other crimes – notably cybercrime, money laundering and insider trading – have either stayed at the same level or increased, with cybercrime jumping by a third (32% vs 24%) in just two years.



Responsible people want to work for responsible companies – ones that bring life to their ethical beliefs and "walk the talk"





24%
of companies believe it's likely they will experience bribery and corruption

...and 44%
claim employee morale is the largest casualty of economic crime

How is your business strategy aligned with and led by your organisational values?

The modest drops in incidents of 'traditional' frauds, relative to our last survey, may be feeding a false sense of security. There is a risk that companies may not see the value in investing more resources into ethics and compliance programmes if they have not noticed an increase in their experience of economic crime.

Indeed, many organisations have been cutting costs in both headcount and training, or stretching their existing compliance team's responsibilities to include additional duties. This may be a strategic miscalculation: in many industries and geographies, economic crime risks are not diminishing and a short corporate memory can be dangerous. The deeper point is that while risks and threats are always changing, the essence of a successful compliance programme is one that can foresee and address an evolving risk landscape.

A disconnect

One needs only consider publicised incidents involving multinational organisations – all of whom have well-established ethics and compliance programmes. Do these incidents indicate that such programmes are not keeping up with changing business risks? That they are sending mixed messages? Or is there a deeper reason for the disconnect?

The numbers point to a perception gap between what CEOs and boards think is occurring and what's actually happening in the business, particularly among senior and middle managers. According to our survey, middle managers remain the most likely to commit fraud (though there is variation by region), and also the most likely to feel that values are not being clearly stated, or that incentive programmes are not fair.

PwC's 19th Annual Global CEO Survey corroborates this theme of a gap between intention and execution. Of the top threats facing organisations, the percentage of chief executives naming bribery and corruption saw the greatest increase, from 51% to 56%. A lack of trust in business was another reported key threat, underscoring the importance to leadership teams of having a sophisticated, credible corporate ethics programme.

Ensuring your compliance programme is fit for purpose

So how do the C-Suite ensure that what they espouse is actually being put into practice by management? How is compliance being incentivised? How is it being measured?

Below are four key areas of focus for enhancing the effectiveness of ethics and compliance programmes, which we examine in the remainder of this section:

- **People and culture.** Maintaining a values-based programme, measuring and rewarding desired behaviour.
- **Roles and responsibilities.** Ensuring they are correctly aligned with current risks.
- **High-risk areas.** Better implementation and testing of the programme in high-risk markets and divisions.
- **Technology.** Better use of detection and prevention tools, including big data analytics.

Five steps on the way to a more effective compliance programme

1. Ensure your programme is in line with corporate strategy; and communicate this alignment.
2. Evaluate and potentially reimagine the identity of your compliance function so it may adapt to an environment where risk and threats are ever-changing.
3. Ensure all owners of compliance obligations fully understand the compliance "big picture" across the organisation, and the scope of their own responsibilities within it.
4. Remember that policies and training on values are not enough: credible, consistent engagement across the organisation are essential.
5. Don't downsize when risks are going up.

People & culture: Your first line of defence

At the heart of any economic crime is a poor decision driven by human behaviour. So it stands to reason that the answer should start with people. That means not only instilling clear processes and principles for your employees, but also creating a culture where compliance is hard-wired to values – and to the overarching strategy of the organisation.

Our respondents told us that the greatest organisational damage they experienced as a result of economic crime was not to their share price or even in relations with regulators. It was reflected in damaged employee morale – with 44% of respondents experiencing medium or high impact. Reputational damage was also cited by 32% of respondents as having significant impact. In both cases, the nature of how a business is perceived – from the inside as well as the outside – was the area of greatest concern. This underscores the key role played by values in a successful business strategy.

"Recent research from PwC and the London School of Business on promoting ethical behaviour in the financial services sector shows that a "get-tough" approach to the management of performance has created a climate of fear which, in turn, leads to unethical behaviours.

The study found that anxiety caused by this blame culture disrupts people's capacity to make good decisions – and often leads them to behave less well than those who are motivated by the potential positive outcomes of success."

Publication: 'Stand out for the right reasons' – PwC and London Business School research, June 2015.

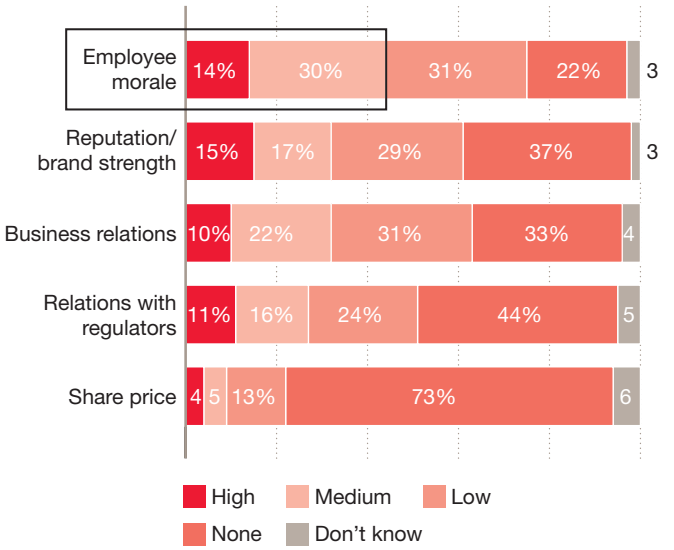
Put the Spotlight on your risk

Many organisations are struggling to collect meaningful data that would allow them to actively monitor and address their behaviour risks. Adding to these internal pressures are external ones: increased public scrutiny and ease of availability of information means that investors, consumers, suppliers, and all types of third parties require more evidence of an organisation's commitment to doing the right thing.

As recent, highly publicised events have demonstrated, a static approach to ethics and compliance is not sufficient to embed ethical behaviour throughout an organisation.

Spotlight, PwC's web-enabled tool, allows you to quantify your behavioural risk, while providing you with an assessment of the effectiveness of your ethics and compliance programme. It measures the alignment between the behaviour you want to see and what is happening in practice, using an online survey and other subjective and objective measures including interviews, focus groups and document review.

Fig 11: Impact of economic crime



A values-based compliance programme will help attract the best and the brightest to your organisation. Responsible people want to work for responsible companies – ones that bring life to their ethical beliefs and "walk the talk".

A well-designed compliance programme – supported by a focus on supporting ethical behaviours – can offer a clear strategic benefit to the business.

But to be effective, your compliance programme must also be more than an updated code of conduct, a policy, and a few hours of training. Fundamentally, it must address the deep connection between values, behaviour and decision-making.

Rather than attempt to address or anticipate each individual risk as it arrives, the sophisticated approach is to empower your people with an underlying appreciation of how and why to make the right decisions in certain circumstances. The need for this approach is supported by our survey findings that in regions where more senior management was involved in the perpetration of economic fraud (such as Asia Pacific, Eastern Europe, North America and Western Europe), one of their biggest drivers was incentive or pressure to perform (i.e., making the wrong decision when it mattered most).

Mind & measure the (perception) gaps

Nearly all survey respondents agreed that their organisation had clearly stated and well-understood organisational values (86%), with CEOs and CFOs expressing this particularly strongly. But our survey identified areas where senior management and boards were not perceiving the same realities as those in the middle. While 90% of CEOs felt values were clear and understood, this had reduced to 84% at the level of managers.

In our experience this is a statistically significant gap – between what senior leaders think and say and what middle management perceive – which can potentially create a vacuum within which, despite the best of intentions, unethical activities can spring.

Perception gaps

A persistent theme in our survey results is that of gaps of perception, which can lead to unwanted outcomes. These can be broken down into 3 basic categories:

- The gap between what the board believe and promote, and what people inside the organisation actually see, believe and do day to day.
- The gap between intentions and funding to fulfil them.
- The gap between senior management and middle managers in overseeing compliance.

Fig 12: Perceptions of business ethics and compliance

Aligning roles & responsibilities: Who's in charge here?

Our survey revealed that approximately one in five (18%) of all respondents told us they knew of no formal ethics and compliance programme in place in their companies. Interestingly, the percentage of CEOs, board members and COOs that stated not knowing of a formal ethics and compliance programme was higher, at 23%.

82% of organisations have established a formal business ethics and compliance programme, but responsibility for that programme is widely dispersed among roles.

Organisations with fewer than 1,000 employees are generally less likely to have a formal ethics and compliance programme. Although they may be focusing on the actual needs of the business rather than taking a "bells and whistles" approach, this can pose a challenge as many of them face a similar risk landscape to their larger peers.

Fig 13: How many organisations have a formal business ethics & compliance programme?

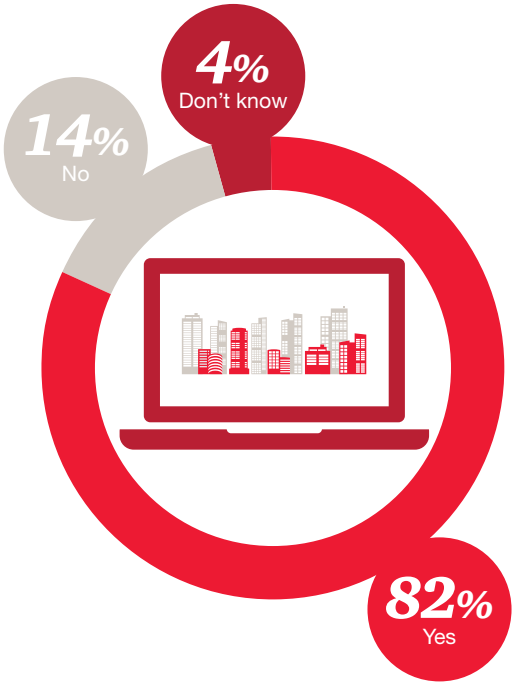
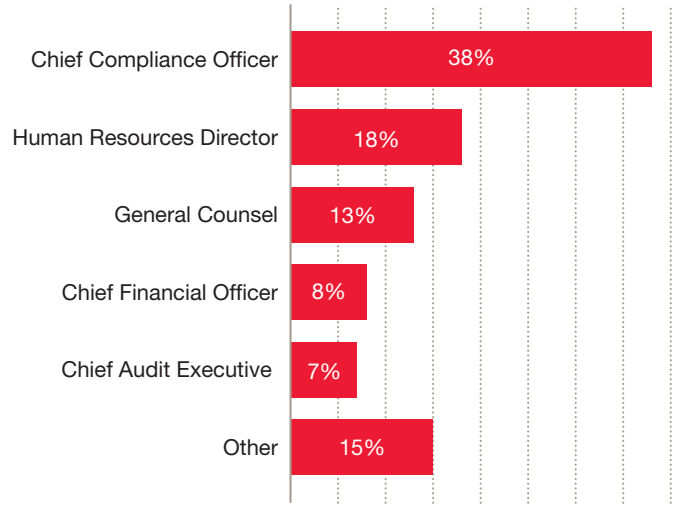


Fig 14: Who is responsible for business ethics & compliance programmes?



Who has ownership? Adopting a risk-based approach

It is important that all people across the business – not just compliance professionals – understand their roles and responsibilities in ensuring the business is aligned and delivering its ethics and compliance programme and priorities. Still, many companies exhibit a degree of confusion about who has ownership for what.

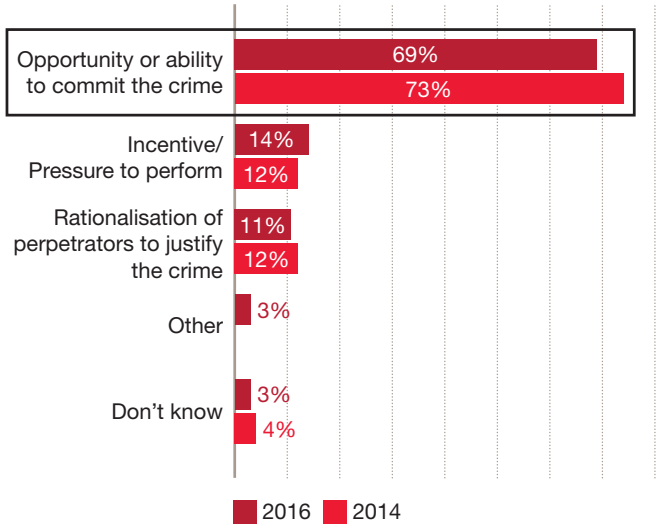
"Ownership" of the programme should belong to the first line – business-unit management – whose responsibility it is to understand the risks and determine the unit's appetite for that risk. The role of the compliance function, on the other hand, is oversight and guidance. In some organisations, however, there is a tendency to view compliance as a kind of insurance policy upon which a passive responsibility can rest.

Ultimately, all members of the business need to be working towards the same compliance goals. Forward-thinking organisations create a broader "compliance community," where the roles and responsibilities of ethics and compliance become part of day-to-day business for everyone.

Opportunity (for crime) knocks. But who's listening?

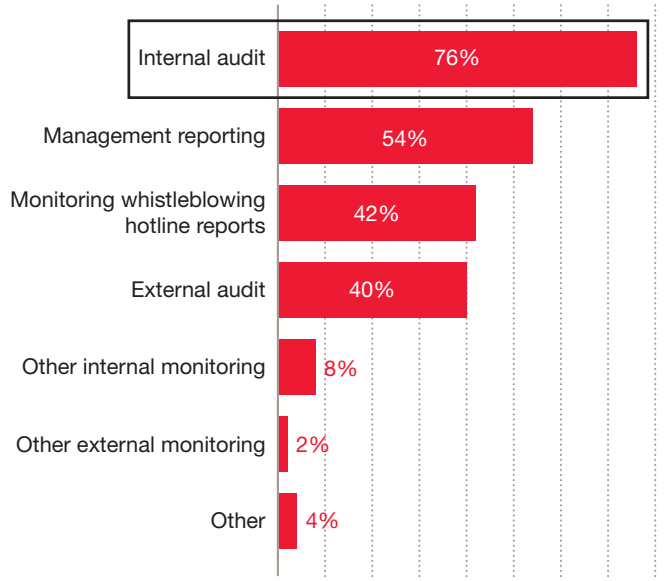
Seven in ten organisations believe that opportunity is the main driver of internal economic crime. This far outweighs the other two elements of the fraud triangle, which are incentive/ pressure to perform and rationalisation of the crime.

Fig 15: Factors contributing to economic crime committed by internal actors



A large majority seem to favour stronger control environments as a means of reducing this opportunity, but our top-line results show corporate control environments are 7% less effective in detecting and preventing economic crime than two years ago. Over three quarters (76%) of respondents told us they are relying on their internal audit function to assess the effectiveness of their compliance programmes.

Fig 16: How does your organisation ensure that your business ethics & compliance programme is effective?



Large organisations remain more susceptible to procurement fraud and bribery and corruption

While internal audit is an important piece of the framework for assessing a compliance programme's effectiveness, it is not by itself a sufficient means of assuring compliance, due to the fact that its interventions are both periodic and historical. Moreover, the fraud risk profile has changed (for example an increase in new frauds such as cybercrime), and incidence of some fraud types is rising or persistent in certain types of organisation.

For example, large organisations with more than 1,000 employees remain more susceptible to procurement fraud and bribery and corruption (5% higher and 2% higher, respectively, than the global average) as fraud schemes find a way around established control frameworks. In effect, hackers and fraudsters have worked out how to circumvent some of the more common control frameworks.

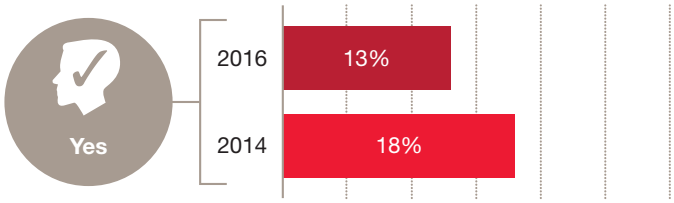
Since prevention must ideally occur at the point of decision making, internal audit mechanisms should be integrated with management reporting and real-time monitoring in the business so that issues are detected and prevented in time. Our financial sector respondents in particular point to management reporting as key to ensuring the effectiveness of compliance programmes, with 60% using this tool. Currently only 8% of of all respondents say they are using other, more promising internal monitoring approaches – such as data or predictive analytics – which are more difficult to circumvent.

Implementing in high-risk areas: The devil is in the details

Ingraining ethical behaviour within a global organisation requires better training, consistent communication, and management reporting. But it should also include an understanding that country and division risks are not created equal, even across high-risk areas. Thus, a sophisticated global compliance programme must be finely tuned to the specific realities on the ground.

Take the familiar transnational risk of bribery and corruption. Regulators are increasingly willing to hold companies liable for unethical behaviour that takes place far away from the head office, and management therefore has to find ways to ensure that all their people are doing the right thing all the time.

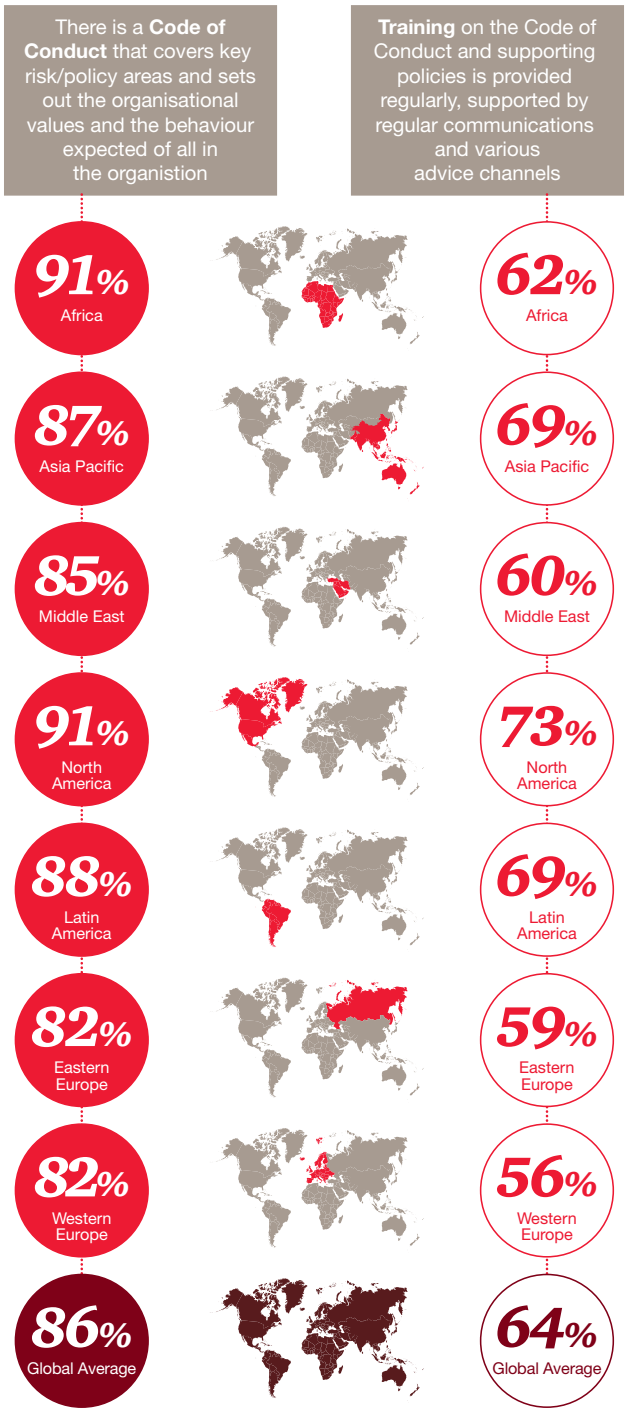
Fig 17: Percentage of organisations asked to pay a bribe

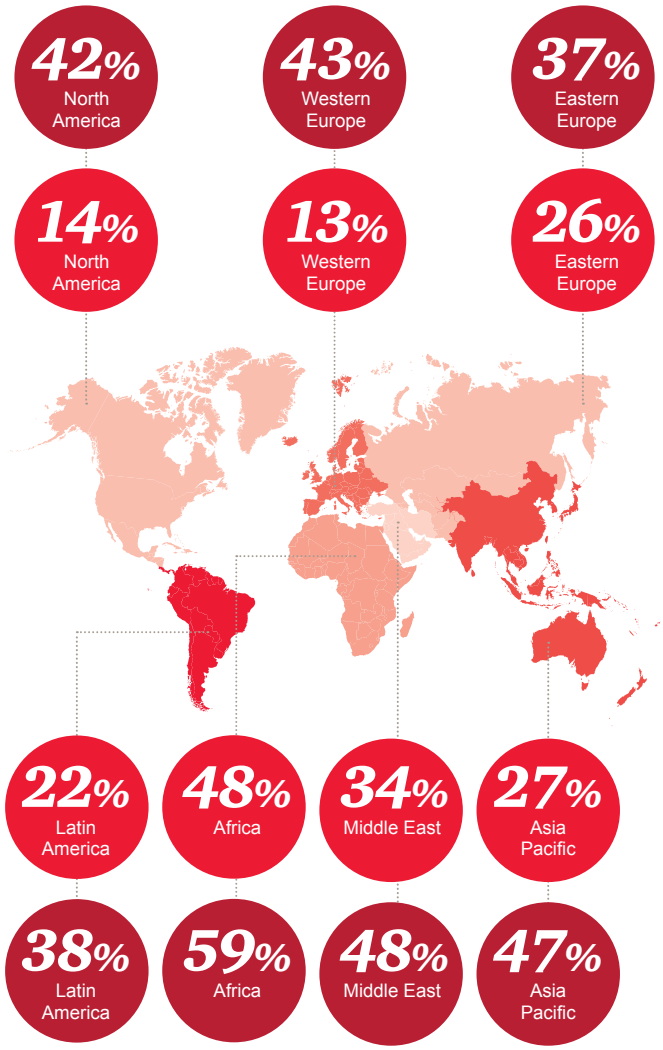


How do organisations respond to this risk? Having a recognised code of conduct is a starting point, but if employees do not know how to use it in their day-to-day decision-making this does little to mitigate compliance risks. The code and other polices need to be embedded through training, regular communications, reward and recognition of where good decisions are made, and disciplinary procedures where bad decisions are made.

Although 86% of organisations globally said they had a code of conduct in place, only 64% said that training was provided regularly and supported by regular communication and advice. The discrepancy was particularly sharp for respondents from Africa, Western Europe, the Middle East and Eastern Europe.

Fig 18: Training and Codes of Conduct





Overall, 91% of respondents believe their top management makes it clear that bribery is not a legitimate practice. This was consistent across all regions and all industries. However, we're still seeing a large number of reported incidents – and, in many regions, an ever larger number of organisations who expect to experience bribery and corruption in the next 24 months.

Technology: Not a cure, but strong medicine

Today there are several sophisticated tools – including big-data analytics capable of much more effective monitoring – that can help bring compliance closer to operations by handling a variety of structured and unstructured data.

Yet apart from transaction-monitoring systems (which are used primarily by financial sector clients), very few organisations are using these kinds of technologies to help detect and prevent economic crime. Currently only 8% of respondents use other internal monitoring approaches such as data analytics.

But beware: organisations can fall prey to technology-related missteps. Driven by a disconnected risk assessment process, some engage in too much monitoring in some places (with limited effect), and none in others. Others unknowingly duplicate their expenditures on different tools. Still others follow a "tick-the-box" approach to compliance – and don't always gather or use the right data, often prompting the abandonment of data analytics exercises before they prove their worth.

We have observed that the best place to start is not in the "big data" space of transaction monitoring, but rather in the "small data" of risk assessments. What matters most is collecting consistent comparable data – an act that sounds straightforward, but isn't.

The optimal model encompasses the spread of risks an organisation faces and allows reporting by business unit, geography or third party. To achieve this three things are needed:

- A consistent approach to defining risk
- Transparency of risk measurement
- A common data platform

These conditions, combined with a centralised governance and operating model, can help you begin to assess how effective your current transaction monitoring is – and focus them on the real threats to your company. Ultimately, the focus should be not on technology *per se*, but rather on what it enables. Data alone will never be a panacea. But used effectively, it can offer companies additional power to stay ahead of their compliance risks.

Key contacts

Mark Anderson
Partner
United Kingdom

t: +44(0) 20 7804 2564
e: mark.r.anderson@uk.pwc.com

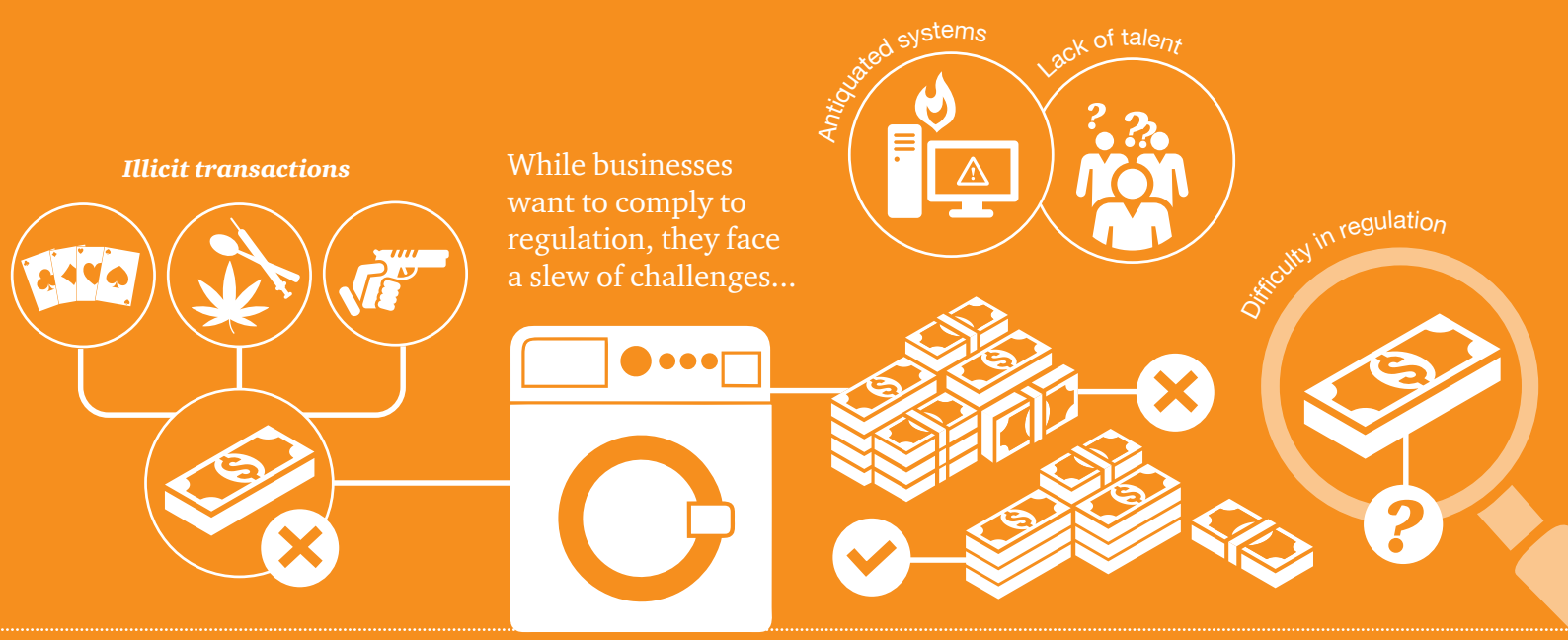
Manny Alas
Partner
United States

t: +1 (646) 471 3242
e: manny.a.alas@us.pwc.com

Martin Whitehead
Partner
Brazil

t: +55 11 3674 2141
e: martin.j.whitehead@br.pwc.com

Anti-money laundering



Money laundering destroys value

Money laundering destroys value. It facilitates economic crime and nefarious activities such as corruption, terrorism, tax evasion, and drug and human trafficking, by holding or transferring the funds necessary to commit these crimes. It can be detrimental to an organisation's reputation – and its bottom line.

Global money laundering transactions are estimated at 2 to 5% of global GDP, or roughly U.S.$1-2 trillion annually. Yet according to the United Nations Office on Drugs and Crime (UNODC), less than 1% of global illicit financial flows are currently seized by authorities[2].

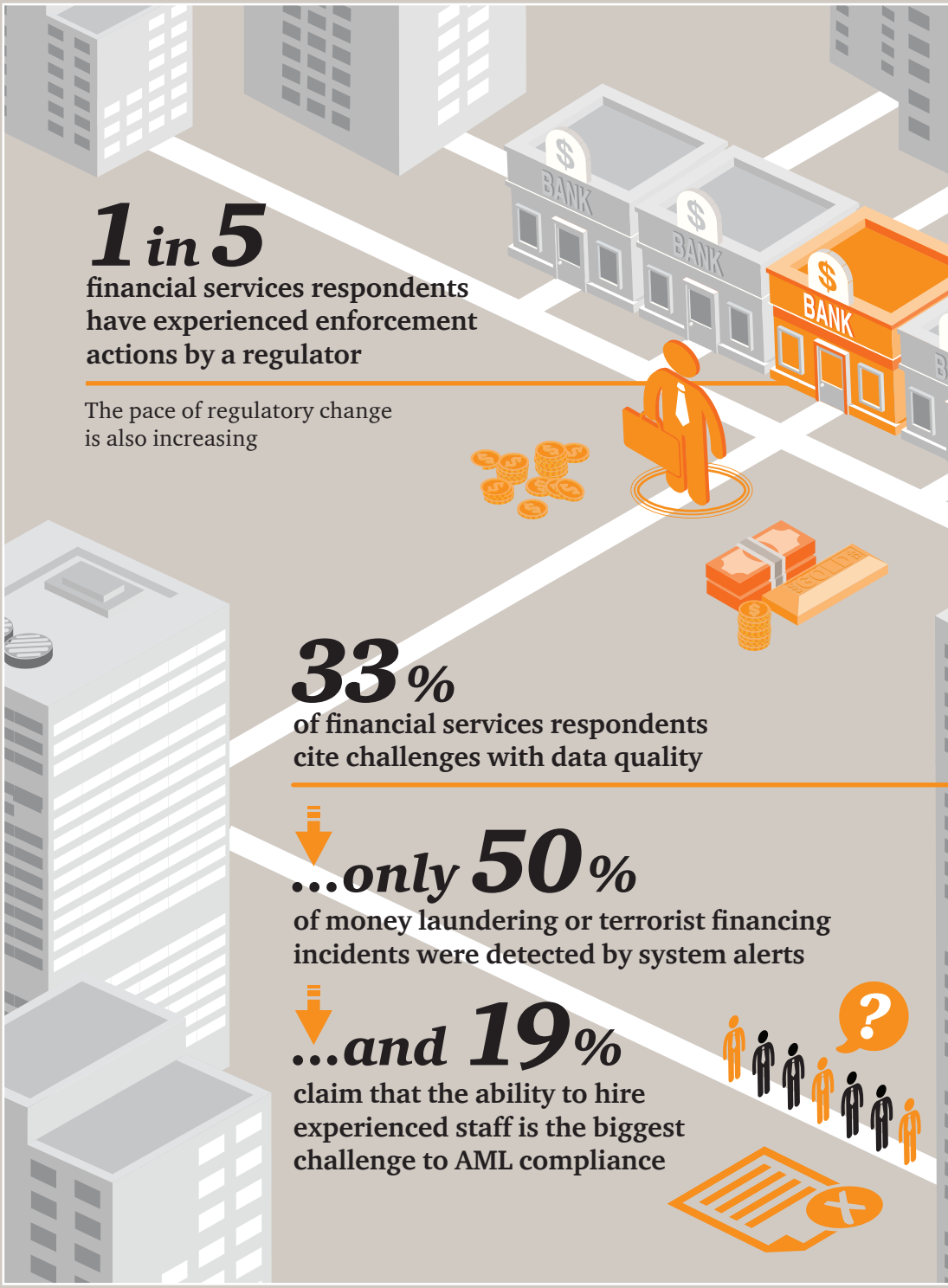
With the rising visibility of terrorist attacks, money laundering and terrorist financing are escalating in priority for governments across the globe. Over the last few years, in the U.S. alone, nearly a dozen global financial institutions have been assessed fines in the hundreds of millions to billions of dollars for money laundering and/or sanctions violations. There are strong indications that other countries will follow in substantive regulation and enforcement.

But it's not just financial services institutions. Any organisation that facilitates financial transactions – including non-bank money service businesses such as digital/mobile payment services, life insurers and retailers, to name a few – is also coming within the scope of anti-money laundering (AML) legislation worldwide. Alarmingly, but not surprisingly, many of these new participants are not yet up to speed on the requirements they must meet or on the compliance programmes they will need.

As regulation deepens in complexity and scope, the cost of compliance continues to rise. According to new figures from WealthInsight, global spending on AML compliance is set to grow to more than $8 billion by 2017[3] (a compounded annual growth rate of almost 9%). But many balk at increasing compliance spend – notwithstanding the cost of enforcement actions and large-scale penalties resulting from compliance failures.

2) From 'Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes' by the United Nations Office on Drugs and Crime © 2011 United Nations. Reprinted with the permission of the United Nations.
3) Statistics provided courtesy of WealthInsight

Heightened regulatory standards are driving sharp increases in enforcement action

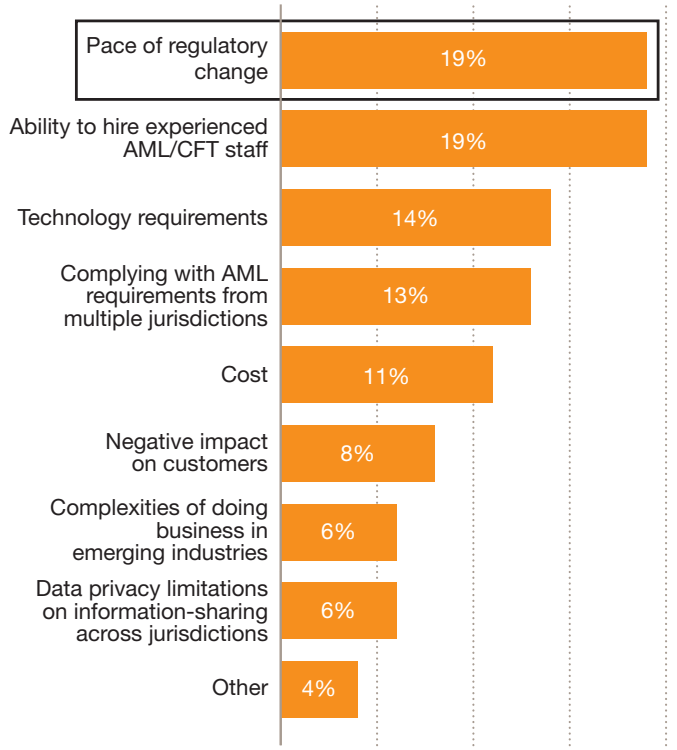



More than 25%
of financial services firms have not conducted AML/CFT risk assessments across their global footprint
BANK
How would your organisation fare in the face of regulatory scrutiny?

Regulation by examination

Heightened regulatory standards are driving sharp increases in enforcement action. Our survey shows that the level of enforcement of anti-money laundering and combating the financing of terrorism (CFT) measures has created challenges for even sophisticated financial institutions.

Fig 19: Most significant challenges to compliance with AML/CFT requirements



Certain governments have imposed fines – and in some cases, pursued criminal actions – against financial institutions that have not implemented sufficient controls to monitor their global transactions. Some financial institutions have come into the crosshairs of regulators in one country for illicit business practices in another. Often there is confusion about where an institution can legitimately operate, if it is under sanctions elsewhere.

AML Watchdogs & Regulators

- **The Financial Action Task Force on Money Laundering (FATF).** An inter-governmental policy-making and standard-setting body, whose current mission is to promote policies to combat money laundering and terrorism financing by monitoring global AML and Counter Financing of Terrorism (CFT) trends, and setting international standards. FATF established "Forty Recommendations" – a global minimum standard for an effective anti-money laundering system, currently adopted by 34 member countries as part of their anti-money laundering regulation and legislation.
- **The United Nations Security Council** issues resolutions containing lists of people and groups against which sanctions have been imposed, such as known terrorist organisations. These lists are often used by participating governments to support measures against terrorist activity.
- **The Office of Foreign Assets Control (OFAC),** an entity under the U.S. Treasury Department, maintains and administers a number of U.S. economic sanction programmes and embargoes.

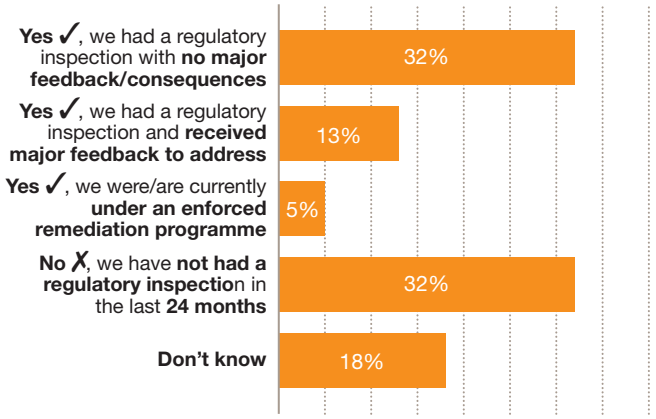
Inspections and remediation are on the rise. As financial services organisations grow by acquisition (as many have done of late), their legal vehicles, businesses and markets are not always immediately consolidated into group processes or standards. Many still struggle in the aftermath of regulatory actions or sanctions. All of these factors increase the risk profile for AML enforcements. Our survey indicates that 18% of banks – a very significant number in our opinion – have recently experienced enforcement actions by a regulator.

Unequal enforcement?

While most nation-states have some mechanism for AML inspections, the degree of thoroughness of those inspections varies substantially.

The United States and a few other developed countries have examination staff dedicated to AML and sanctions. But many other countries employ compliance or risk generalists rather than AML specialists, and conduct more infrequent inspections.

Fig 20: Regulatory enforcements experienced



Another challenge for organisations wrestling with global AML/CFT compliance is that regulatory expectations are increasingly replacing clear legal requirements. This is most prominent in the areas of customer due diligence and transaction monitoring, where examiners may apply a standard on one institution based on the practices of another. This so-called "regulation by examination" challenges the well-known risk-based approach concept that organisations and their stakeholders are expected to apply.

FATF: A new focus on effectiveness

FATF has shifted its evaluation standard of countrywide AML/CFT standards from technical compliance to effectiveness, where all organisations are measured by a similar yardstick.

This new focus on effectiveness should drive some developing countries to make changes in their enforcement practices, which we expect to trickle down to institutions – and, in turn, given the global nature of AML initiatives, to other jurisdictions. It could also temporarily create a gap in perception of the meaning of "effectiveness" between more mature markets and developing ones.

Global compliance is not just a matter of following the laws of a single jurisdiction. Regardless of home jurisdiction, organisations should consider AML/CFT matters as being globally regulated, for three reasons:

- FATF sets international standards for AML/CFT risk management and enforcement. Thus, it forms the basis for national regulations outside the U.S., and therefore the obligations of banks and other regulated institutions.
- OFAC, along with other national treasuries such as Her Majesty's Treasury, administer economic sanctions programmes covering the movement of goods, services and funds overseas and across borders.
- It is almost impossible for financial institutions to avoid the laws of the jurisdictions administering major global currencies such as the U.S. dollar, British pound and Euro. The mere act of clearing a single transaction in the U.S., or with U.S. dollars – or of contacting a person in the U.S. by telephone or email – is enough to establish nexus and clear the way for prosecutions in the U.S.

Increasingly, the regulatory frameworks of the major financial centres – for example Hong Kong, Singapore, London and New York – are converging, requiring institutions to incorporate the highest standards, both internationally and in their home jurisdictions.

Taken together, these fast-changing, unpredictable developments can lead to a kind of strategic inertia, as institutions try to predict the future regulatory landscape they will face. One thing is abundantly clear: a great deal of judgment will be required in crafting their financial crime compliance programmes.

What does this mean for your organisation?

With the globalisation of AML/CFT standards, it's important to remember that you may be judged by the highest international compliance standards. Here are three action points to consider:

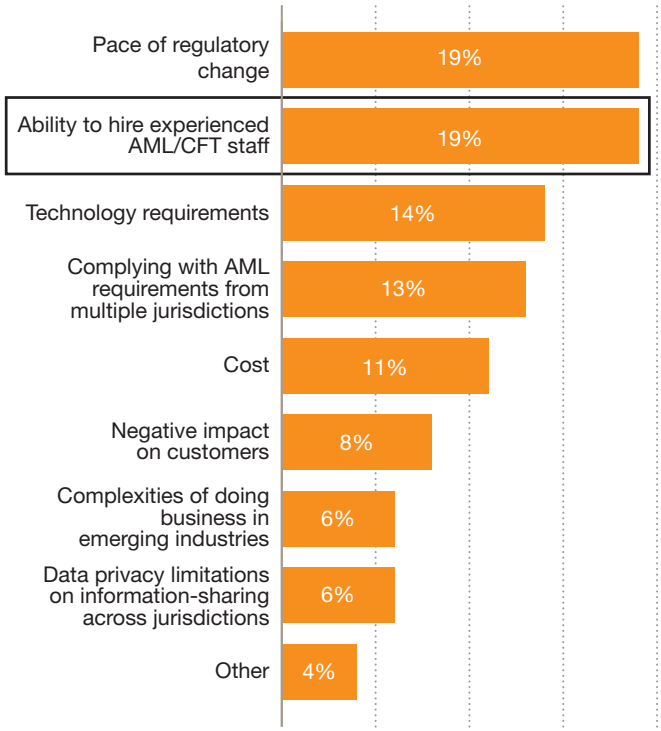
- **Keep your finger on the regulatory pulse.** Look beyond mechanical compliance with today's laws. Instead, look ahead and examine how to properly structure to comply with upcoming legislative trends. Focus on having a viable function within the organisation that keeps track of pending regulations in this area.
- **Lead the pack; don't follow.** Being in the middle of the pack exposes you to the risk of falling behind the regulatory curve. Focus on being strategically nimble and innovative to help you stay on top of the regulatory changes.
- **Learn from others' mistakes.** Few organisations are known to actively investigate the root cause of significant issues as identified by regulators. Remediation often serves as a quick solution to address regulatory findings – yet the cost of remediating breaches often outweighs penalties imposed by regulators. Since most transactions have a multinational financial component, it is good practice to default to the highest global standard of compliance whenever possible, and to carry out more rigorous AML/CFT self-assessments. Establish "enterprise-wide" requirements to ensure consistency across geographies.

Your people, your processes

Our survey respondents said that hiring experienced staff is the most significant challenge they face in the AML arena, tied at 19% with concerns on the pace of regulatory change.

Unfortunately, the supply of talent continues to fall behind demand. Churn among AML and compliance staff is high, and competition for top-shelf people is significant for both financial services and non-financial services companies.

Fig 21: Most significant challenges to compliance with AML/CFT requirements



Some organisations are addressing the talent challenge through training of in-house resources, with a significant focus on both AML/CFT and anti-bribery resources.

Fig 22: People measures implemented to address increased regulatory expectations

Risk assessments are critical. Over the last decade, improved money laundering control measures in the formal financial systems have forced criminals to seek new ways to "move" the proceeds of their crimes. That's why regular risk assessments are crucial, enabling your organisation to identify and address the money laundering and terrorist financing risks you face – wherever and with whomever you do business.

Despite the clear advantages, more than a quarter of the financial services firms that participated in our survey either do not currently conduct an AML/CFT risk assessment across their global business footprint, or don't know if they are.

And as the sophistication of money launderers continues to increase over time, this is a measure that cannot be put off. Trade-based money laundering (TBML), for example is complex system of false documentation that enables criminals to earn and move value around the world under the guise of legitimate trade. This is becoming harder to detect through traditional transaction monitoring systems.

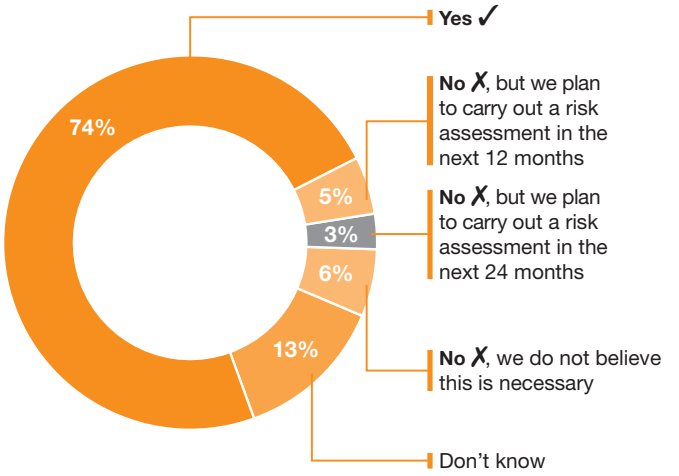
Risk assessments should be conducted on a periodic basis. They should be closely attuned to changed circumstances such as the operating environment, global standards and regulation in countries of operation. Notably, assessments should also include the profiling of customers into different money laundering and terrorist financing risk categories. It is also the global standard recommended by FATF and regulators to curb threats.

Right people, right skills, right places. What skills do you need?

When your best line of AML defence is having the right people in the right roles with the right skills, you need to know what you are looking for. There's significant demand for specialised expertise and skills around:

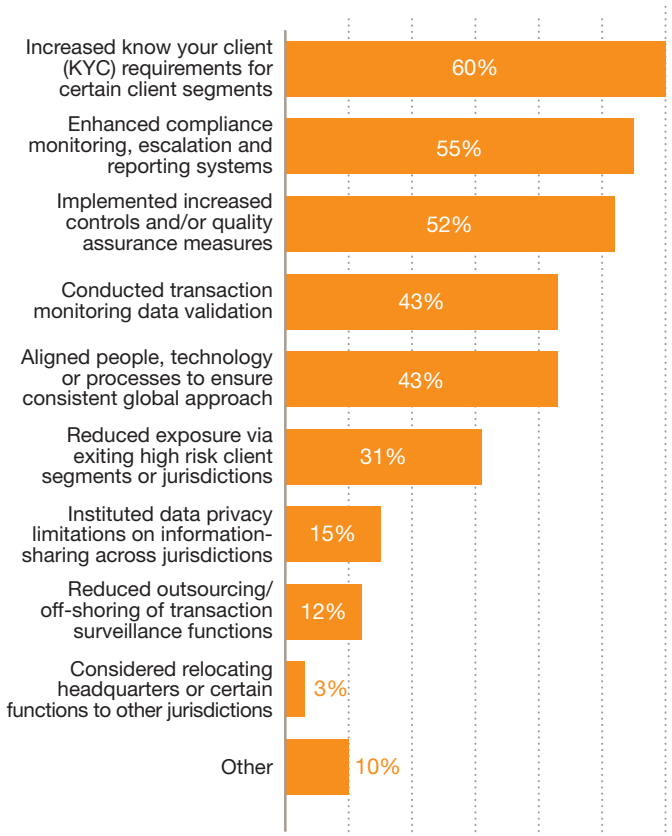
- Global standards and requirements
- Jurisdictional regulations and obligations
- The global regulatory ecosystem
- Customer due diligence
- Technical expertise in transaction monitoring
- Data analytics

Fig 23: Percentage of organisations that carry out AML/CFT Risk assessments



Know your customer, today and tomorrow. Transparency into your customer base goes beyond merely identifying and verifying the information they provide. It must be a dynamic act, not a static one. It is essential to keep monitoring for red flags and suspicious activity on a regular basis. Special attention should be paid to clients' business relationships and transactions – especially when they conduct business with persons residing in countries with weak or insufficient AML regulations.

Fig 24: Measures to reduce AML/CFT risks



Technology

Companies across the industry spectrum seem stuck in a bind. Most – particularly financial services organisations – are facing the hurdle of "rightsizing" their AML programmes for their changing business in an evolving global regulatory landscape. Yet many are hampered by legacy monitoring systems that are proving to be burdensome and extremely expensive to tune, validate and maintain.

Unfortunately, the cost and complexity of implementing some of the new, more sophisticated data-analytical platforms – leading-edge algorithms which could help them move from a cumbersome transactional basis to a more strategic and efficient approach – is likely prohibitive to many. Our financial services respondents seem to be well aware of these systems challenges, with one in three citing data quality as the most significant technical challenge they face.

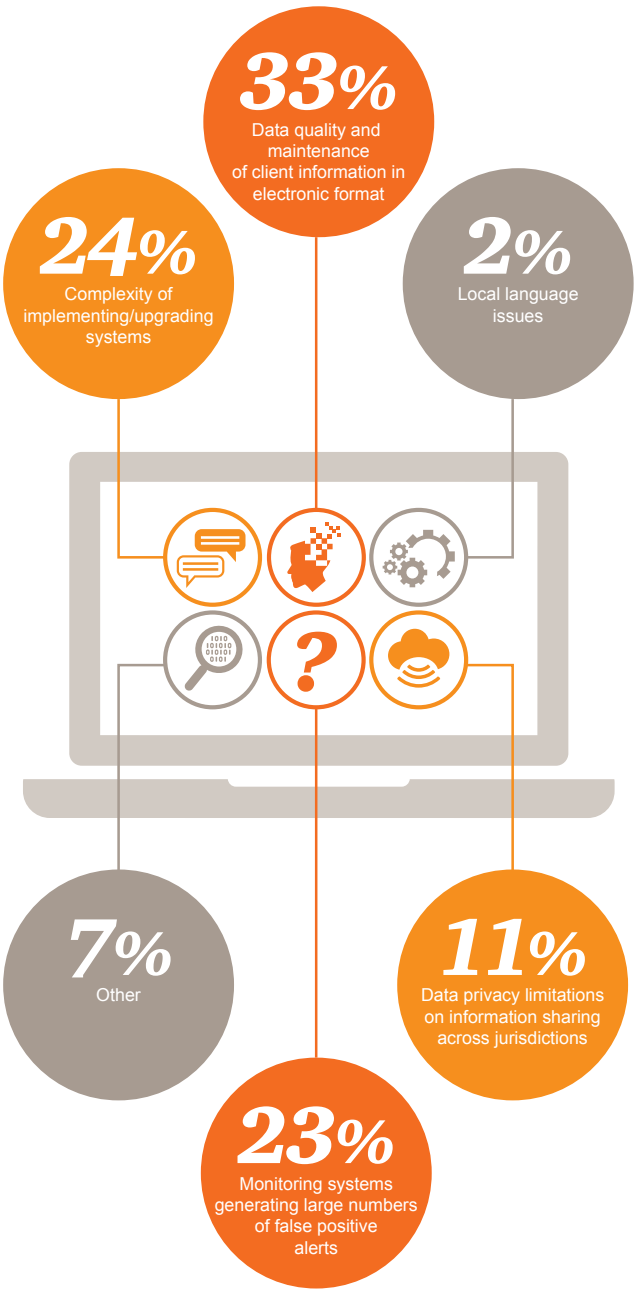
What makes a company take the leap to new technology?

Often such a shift is catalysed by an event – a remediation due to regulatory sanctions, or a merger, acquisition or other transaction that reveals legacy systems are no longer fit for purpose. Or a new disruptive competitor enters the market, and changes the stakes for everyone.

But sometimes it is simply a matter of an organisation reaching a tipping point, where it realizes that the expected return on investment of jumping to a new technology platform is greater than the cost of abandoning the systems that have cost millions in investment and maintenance.

And there may be other benefits to new technology as well. Beyond AML compliance, it can enhance other key compliance functions – including anti-bribery, export sanctions, fraud monitoring and response, financial controls and investigations – potentially strengthening your overall governance.

Fig 25: AML/CFT systems: Most significant challenges faced



Further compounding the issue: AML alert monitoring is performing poorly. According to our survey, only half of identified suspicious money laundering or terrorism financing is getting flagged by transaction-monitoring systems. Current AML typologies might not be catching the nuances and complex structures necessary to identify high-risk transactions.

Fig 26: Methods by which suspicious activity identified

Converting to new analytic models and platforms is not, as of yet, a widespread phenomenon. This could be an indication that institutions have "priced in" a certain degree of ineffectiveness in their legacy detection systems – perhaps to their disadvantage.

Key contacts

Didier Lavion
Principal
United States

t: +1 (646) 471 8440
e: didier.lavion@us.pwc.com

Andrew Clark
Partner
United Kingdom

t: +44(0) 20 7804 5761
e: andrew.p.clark@uk.pwc.com

Malcolm Shackell
Partner
Australia

t: +61 (2) 8266 2993
e: malcolm.shackell@au.pwc.com

Participation statistics

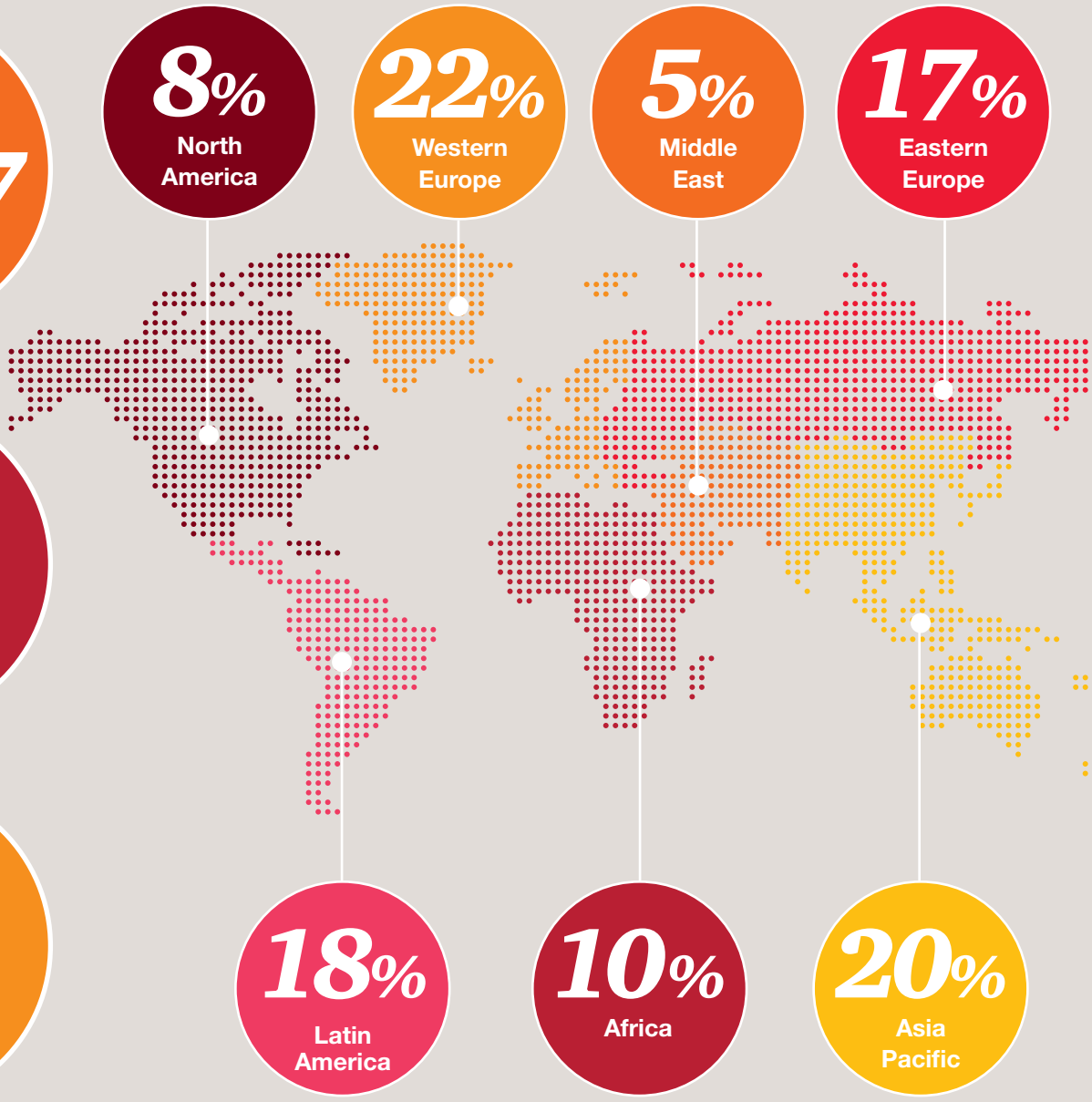
Participation statistics

6,337 completed surveys

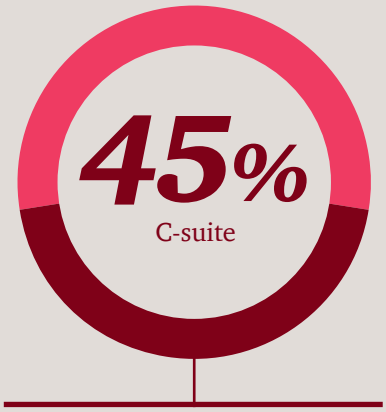
Across 115 countries

Surveyed in 17 different languages

Participation by region



Respondents



70%
of respondents were managing the Finance, Executive Management, Audit, Compliance and Risk Management Functions

54%
of respondents employed by organisations with more than 1,000 employees, with

48%
of these participants having more than 10,000 employees

37%
of the survey population represented Publicly Traded Companies, and

59%
of respondents were from multinational organisations

Industry sectors

35% Industrial

24% Financial Services

14% Consumer

7% Technology

6% Professional Services

13% Other

Data resources

Looking for more data?

The crime survey website ***www.pwc.com/crimesurvey*** has been designed to be an extension of the survey with many exciting and useful resources for readers wishing to delve deeper into the data, including:

- Survey methodology
- Terminology
- Comparative country counts
- Additional information regarding the nature of participants

In addition, this year's survey data has been loaded onto an innovative tool referred to as the Global Data Explorer which will allow visitors to the site the ability to customise their analysis of the data for their specific needs.

Contributors

Survey Leadership Team

Trevor White
Partner, South Africa
t: +27 (31) 271 2020
e: trevor.white@za.pwc.com

Mark Anderson
Partner, United Kingdom
t: +44 (0) 20 7804 2564
e: mark.r.anderson@uk.pwc.com

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

Editorial Board Members

Alex Tan
Partner, Malaysia
t: +60 (3) 2173 1338
e: alex.tan@my.pwc.com

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

Martin Whitehead
Partner, Brazil
t: +55 (11) 3674 2141
e: martin.j.whitehead@br.pwc.com

Antoinette Lau
Partner, China
t: +86 (21) 2323 5533
e: antoinette.yy.lau@cn.pwc.com

Dinesh Anand
Partner, India
t: +91 9818267114
e: dinesh.anand@in.pwc.com

Survey Management Team

Moazam Fakey
Senior Manager, South Africa
t: +27 (11) 797 4750
e: moazam.fakey@za.pwc.com

Anjali Fehon
Forensics Strategy Leader,
United States
t: +1 (973) 236 4310
e: anjali.t.fehon@us.pwc.com

Survey Marketing Team

Gemma Peart
Global Marketing Manager, United Kingdom
t: +44 (0) 771 1589 331
e: gemma.peart@uk.pwc.com

Kate Glenn
Forensics Marketing Leader,
United States
t: +1 (202) 312 7542
e: kate.n.glenn@us.pwc.com

Survey Research & Data Team

Colin McIlheney
Research Director, Northern Ireland
t: +44 (0) 289 0415719
e: colin.mcilheney@uk.pwc.com

Sabrina McCotter
Manager, Northern Ireland
t: +44 (0) 289 0415598
e: sabrina.c.mccotter@uk.pwc.com

Forensic Services Leaders

Andrew Gordon
Global Leader, United Kingdom
t: +44 (0) 20 7804 4187
e: andrew.gordon@uk.pwc.com

Andrew Palmer
EMEA Leader, United Kingdom
t: +44 (0) 20 7212 8656
e: andrew.palmer@uk.pwc.com

Erik Skramstad
US & APA Leader, United States
t: +1 (617) 530 6156
e: erik.skramstad@us.pwc.com

www.pwc.com/crimesurvey

The Design Group 22394 (02/16)