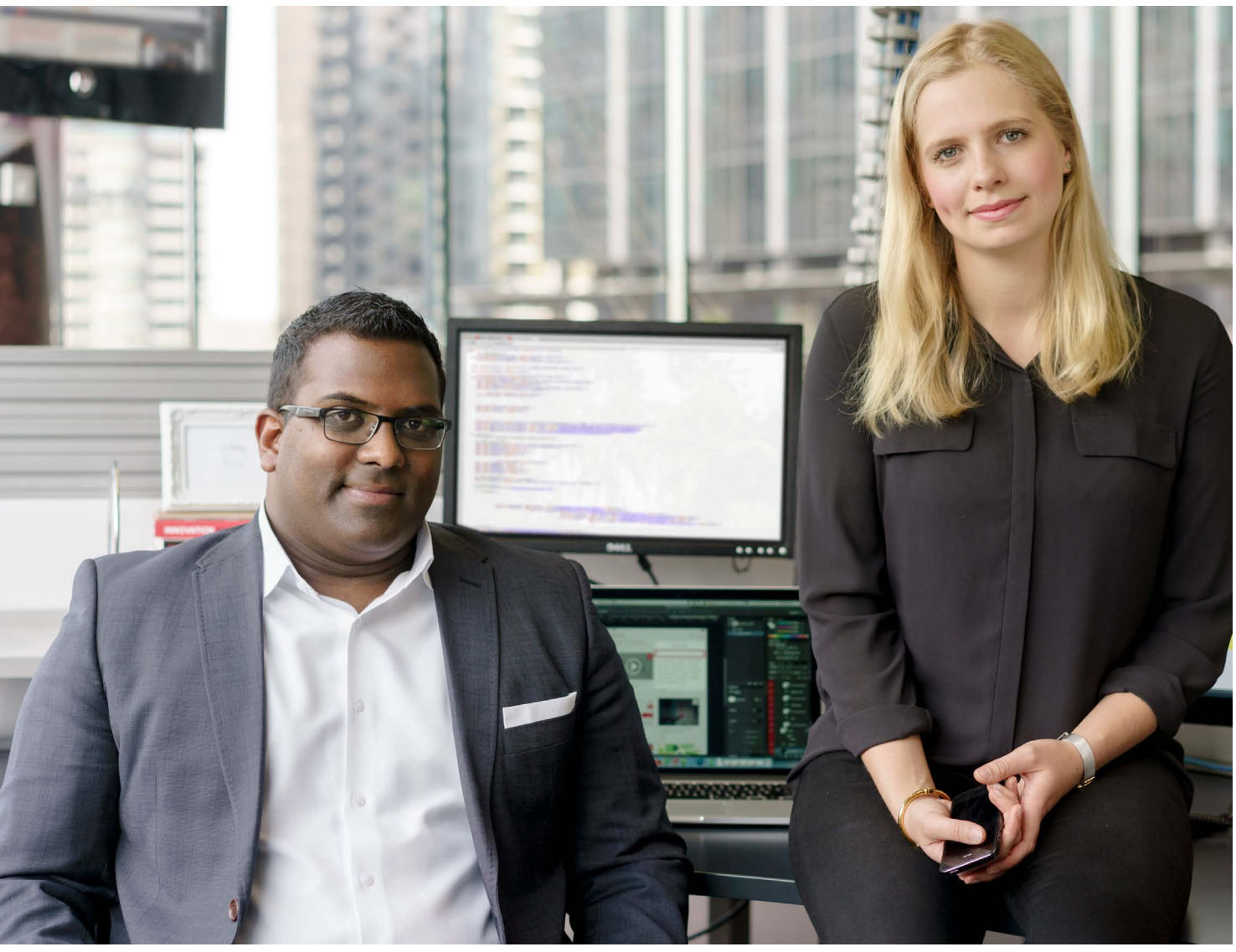
Adjusting the Lens on Economic Crime

Preparation brings opportunity back into focus



38%

More than one in three US organizations report being victimized by economic crime.

54%

Cybercrime is one of the fastest-growing economic crimes since our last update, now affecting more than half of organizations reporting economic crime.

52%

More than half of respondents don't believe local and federal agencies have the skills or resources to investigate and prosecute economic crime, leaving the responsibility to organizations.

pwc

www.pwc.com/crimesurvey

Leading observations

1. Economic crime outpaces company preparedness

Page 3

- More than one in three (38%) US organizations experienced economic crime in the last 24 months
- 57% report external actors as the main perpetrator, surpassing internal fraudsters (29%)
- Company detection efforts are not keeping pace: 1 in 10 have never carried out a fraud risk assessment

What are your opportunities to prevent economic crime?

2. Cyber threats climb

Page 9

- Almost 50% of US organizations in our survey expect to have a cyber breach in the next 24 months
- Most are still not adequately prepared: Just over half of US companies have an active cyber incident response plan
- Engagement of leadership is critical, but only 40% of boards request cyber readiness information more than once a year

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

3. Tone at the top and menace in the middle

Page 16

- 1 in 10 US organizations still do not have a formal ethics and compliance program in place
- Only half "strongly agree" that organizational values are clearly stated and well understood
- Turmoil is coming both from the middle and the top: Of internal crimes, 53% are committed by middle management; 18% by senior management (up from 4%)

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

4. Anti-money laundering continues to confound

Page 23

- 1 in 4 banks have experienced enforcement actions by a regulator: Failure to curb illicit business practices may lead to personal accountability
- 12% of financial services firms have not conducted AML/CFT risk assessments across their global footprint
- Top challenges include complexity of upgrading systems (28%), data quality (26%), and pace of regulatory change (22%)

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

Economic crime evolution

The story that emerges from our 2016 Global Economic Crime Survey is a familiar one: crime continues to forge new paths into business. Regulatory compliance adds stress and burden to responsible organizations. The increasingly complicated landscape challenges the balance between resources and growth.

As we analyze the experiences and feedback from more than 6,000 respondents across the globe — among them over 300 US executives, including C-Suite (26%), senior executives and VPs (37%) and heads of departments (23%) — we challenge you to adjust your lens on economic crime and refocus your path towards opportunity around strategic preparation. Ask:

- What is your experience with economic crime and how has it evolved?
- How can you strategically prepare for and focus on your opportunity to pre-empt economic crime?
- What kind of fraud landscape do you expect in the coming years?
- Do you have the right team, resources, systems and processes in place to appropriately combat threats?

Our study found that 1 in 10 economic crimes are discovered by accident. How many crimes are not discovered at all?

The evolution of economic crime

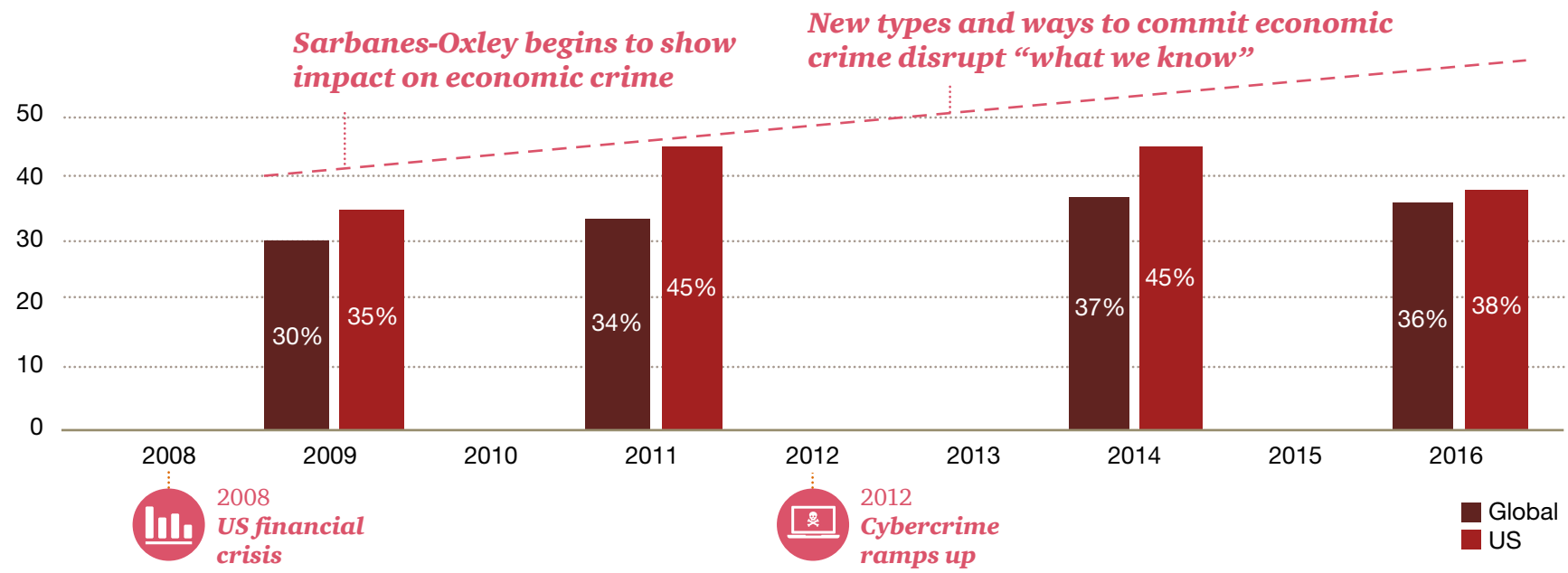
Our 2016 results show that just over one-third of all organizations reported experiencing economic crime in the last 24 months — 36% of global organizations; 38% in the US. However, US experiences of economic crime show a marked decline from the 45% reported rate of 2014 — while the global rate of economic crime remained basically flat.

At first glance, this decline could be evidence of a return on the investments from preventative measures made over the past few years. But a closer look at the data reveals that although there are year-to-year fluctuations, the general trend line in economic crime since the financial crisis of 2008-09 has been on an upswing.

What could be behind the overall ups and downs in reported economic crime over the past 15 years? In 2002, the US Sarbanes-Oxley Act was enacted, flooding the global market with expanded compliance requirements for all SEC registrants, their boards and management, as well as public accounting firms. Looking at trend lines, it appears that it took around seven years for the establishment of these rules to have a significant impact on economic crime — albeit with some fluctuations.

But as our survey illustrates, new types of economic crimes — and the means to commit them—have complicated the threat landscape over the past several years, contributing to an upturn in economic crime. As we begin 2016, the need for a watchful eye on these trends is echoed in the corner office: 72% of US chief executives think there are more threats to the growth of their company than ever before[1].

Fig 1: Rates of economic crime experienced



Source PwC's Global Economic Crime Survey, 2009-2016

1 PwC's 19th Annual Global CEO Survey - US Results. PwC, 2016.

Types of economic crime

When comparing US experiences with economic crime to those of the overall global respondents, a divergence appears.

- **Cybercrime** was added as a type of economic crime in our 2011 survey, but it is already on the verge of surpassing the "age-old" asset misappropriation as the leading economic crime committed against organizations. Cybercrime climbed to 54% this year, very close to the level of asset misappropriation (55%).

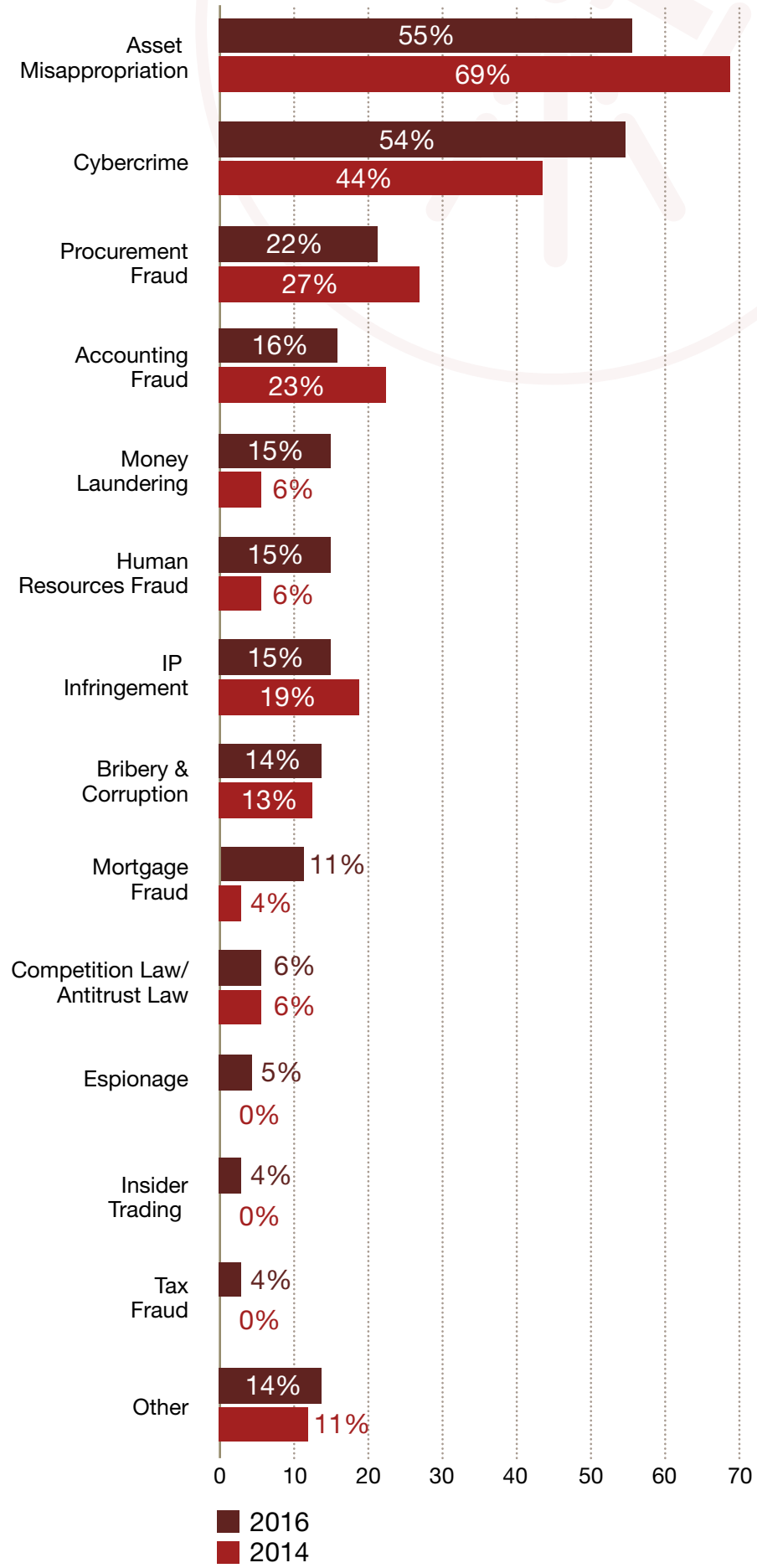
  It is worth noting that significantly fewer global respondents predict having to grapple with cyber criminals in the next two years: 34% globally, vs. 49% in the US. This may be due to the disproportionately large impact of cyber breaches — including media coverage and reputational crises — that US-based companies have experienced. It may also be a result of the increased focus on cybercrime from US law enforcement, national security, regulators and shareholders.

- **Asset misappropriation**, historically regarded as the easiest of frauds to detect, continues its prevalence as a top threat, year to year. However, we have seen a drop in the reported rates of this particular crime from US respondents: 55% in this year's survey, down from 69% in 2014. This could be a result of tightening organizational controls and investments in prevention that are starting to show a return on investment. This could be a result of tightening organizational controls and preventative measures that are starting to show a return on investment.

- **Bribery and corruption** saw a slight uptick among US respondents, from 13% in 2014 to 14% in 2016. US executives still report fewer instances of alleged bribery and corruption than their global counterparts (where 24% have experienced it over the past two years). This may be due to the vanguard anti-corruption regulations enforced in the US, such as the Foreign Corrupt Practices Act (FCPA). As a result of this attention, US-based organizations tend to be "first movers" in the anti-corruption compliance space. Other countries are following the US by creating similar regulations or enhancing previously dormant anti-corruption laws — and following through with more robust enforcement.

- **Insider trading**. A notable trend is that US organizations report fewer insider trading crimes than their global counterparts (4% in US; 7% globally). They are also relatively less concerned about future threats of insider trading (7% domestically; 13% globally). While this may appear counterintuitive given the prevalence of the financial services sector in the US economy, in fact this low percentage could simply be reflection of more robust inspection and monitoring and more stringent enforcement. While this may appear counterintuitive given the prevalence of the financial services sector in the US economy, in fact this low percentage could simply reflect a more robust inspection and monitoring regime as well as more stringent enforcement.

Fig 2: Types of economic crime experienced



Organizational damages

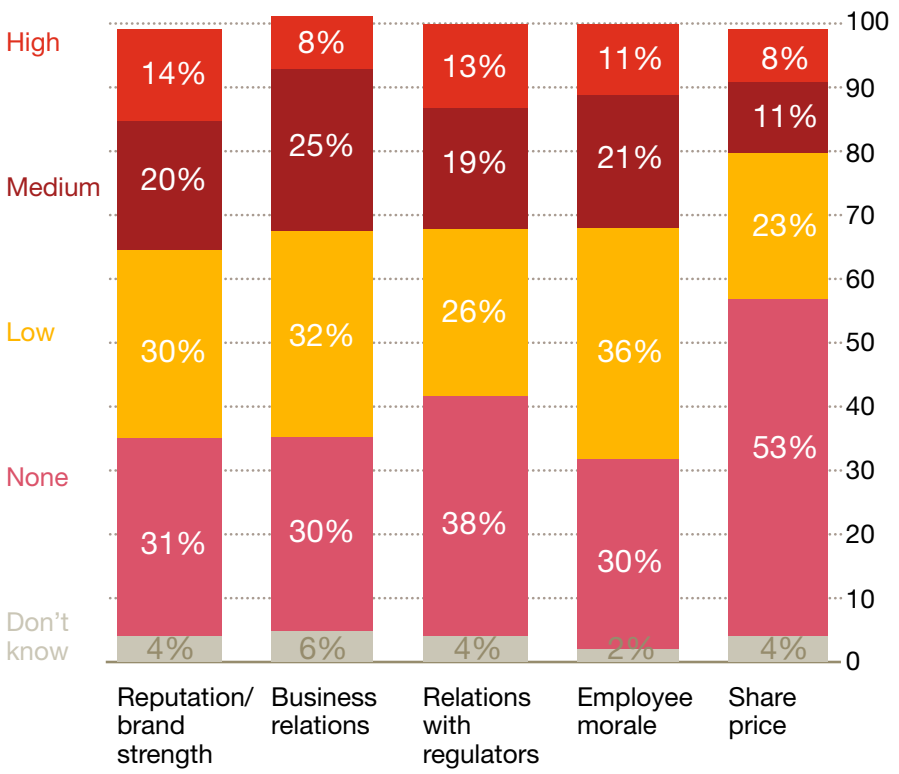
Economic crime can send shock waves of damage throughout an organization. Financial losses can be extensive:

- Over one-quarter of US respondents experienced losses of between $100,000 and $1 million
- 13% of respondents suffered losses between $1 million and $5 million
- 8% of respondents reported losses between $5 million and $100 million
- 3% of respondents reported losses in excess of $100 million

Financial losses can come in many forms, ranging from actual fraud losses to remediation costs and civil and/or criminal penalties. These are substantial sums of money and are representative of a continuing trend of the rising cost of individual frauds.

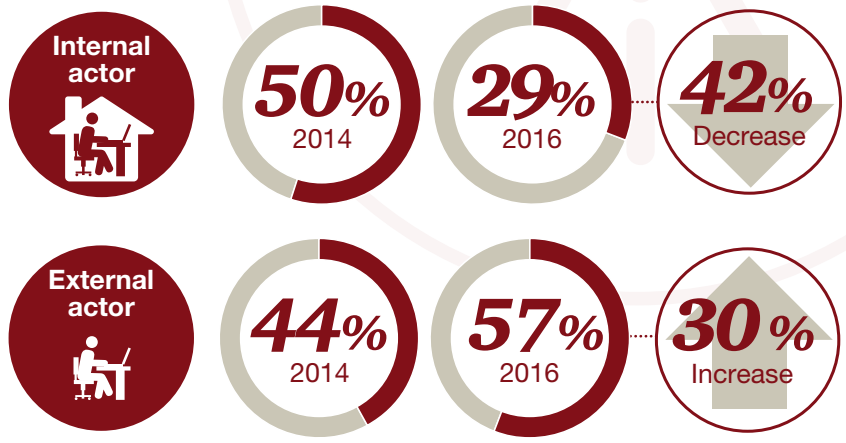
The true cost of economic crime is near impossible to estimate, because the financial loss is often only a small component of the fallout from a serious incident. Our survey respondents consistently note wider collateral damage from business disruptions, remedial measures, investigative and preventative interventions, regulatory fines and legal fees. These can have a significant impact on long-term business performance and, perhaps more critically, cause lasting damage to morale and reputation.

Fig 3: Impact of economic crime on business operations



Profile of the fraudster

Among all territories, US respondents reported the most significant swing from internal to external perpetrators, which likely correlates with both the decrease in asset misappropriation and the rise of cybercrime.



It is interesting that while the share of crimes committed by senior management in the US has jumped from 4 to 18%, globally, that share has declined (down to 16% from 20% in 2014). Although it is difficult to determine if this represents a true shift in the profile of the fraudster, it is clear that accountability for the fraud is rising up the company ranks. Management is no longer shielded by the corporate entity and plausible deniability is no longer a viable defense from substantive fraudulent acts.

Increased personal accountability for economic crime has also been demanded by the American public, particularly since the global financial crisis. Recently, the Department of Justice (DOJ) articulated a major alignment of its formal prosecution strategy with this theme. With the issuance of the so-called "Yates Memo"[2], the DOJ stressed to its prosecutors and civil attorneys the importance of thoroughly investigating and holding individuals, not just companies, accountable for corporate misconduct.

Executives should, at a minimum, understand that the Yates Memo sets expectations not only for its prosecutors, but also for companies, who are required to fully investigate and report individual misconduct in order to receive cooperation credit. It will be interesting to follow the developments over the next few years and see what, if any, effects may be reported by our 2018 survey respondents.

2 US Department of Justice, http://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school

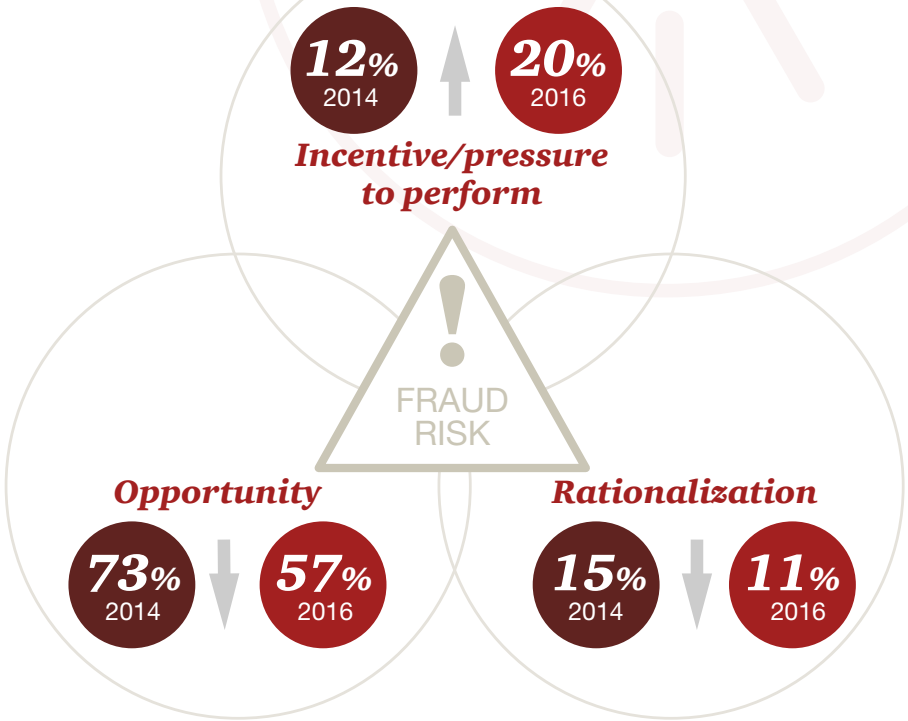
The fraud triangle

We believe that the decreased rate of crime committed by individuals inside of the organization may be a result of escalating attention and increased controls in the US (while, globally, controls of such strength and sophistication are typically not in place or not as active).

Differences further emerge when examining the factors that contribute to economic crime committed by internal players, which can be viewed in the context of the fraud triangle:

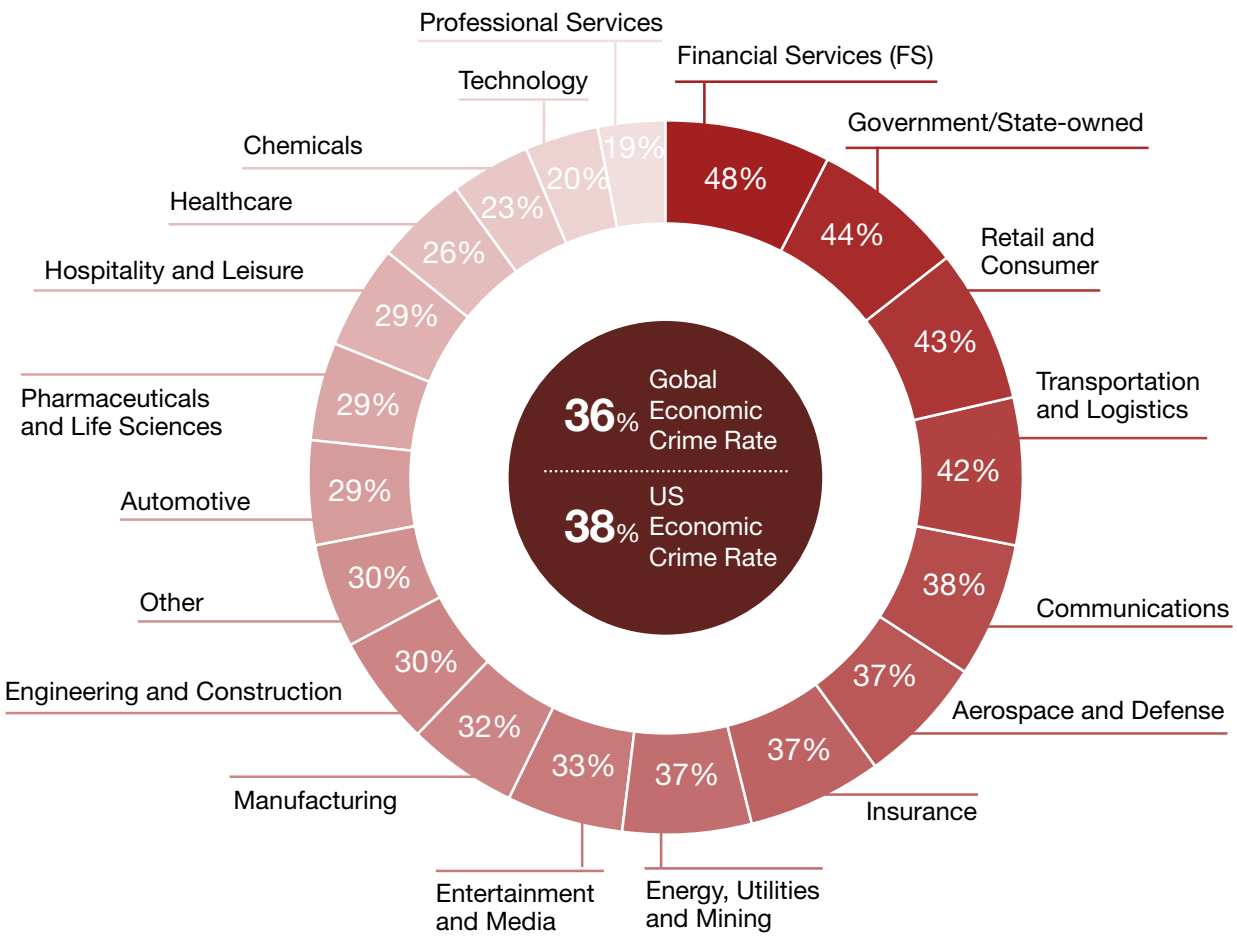
- ***Opportunity or ability to commit the crime***. Growing public awareness and expectations for companies to manage risks, coupled with increasing regulatory attention and action, have led to tightened internal controls in the US — and in turn to decreased opportunity for internal perpetrators to pounce.
- ***Incentive/pressure to perform***. Increased global competition and thinning margins have turned up the pressure on management to gain market share. This may explain why "pressure to perform" has spiked as a main contributor to internal fraud — up to 20% this year from 12% in 2014. This is significantly higher than the overall global results, where 14% referenced pressure to perform.
- ***Rationalization*** of perpetrators to justify the crime is slightly down. This may be due to the dramatically higher visibility of economic crime in today's saturated, 24/7 media landscape — which could make rationalization of such an act more difficult.

Fig 4: Factors that contributed most to internal economic crime, through the fraud triangle lens



Source PwC Analysis
Figures do not add up to 100% due to "Other" and "Don't Know" survey responses.

Fig 5: Reported economic crime rates: Globally, by industry



Traditionally the Financial Services industry has been most threatened by economic crime, as it serves the financial needs of all industries. Due to the highly regulated environment, FS companies have built up sophisticated control mechanisms, detection methodologies and risk management tools to address key crimes such as money laundering. However, large legacy monitoring systems may also prove challenging to modify and conform to new standards and regulations; a troublesome fact as more sophisticated threats are attacking these systems.

As industries converge and the US moves toward integrated business solutions, non-FS organizations are providing for the financial requirements of their clientele in-house, in joint arrangements with financial institutions or with banking licenses of their own. Fraudsters seeking to "follow the cash" now have many more industry avenues to fulfill their objectives.

When confronted with externally committed economic crime, US organizations are more likely than their global counterparts to report it to external authorities. This could also be a reflection of a greater degree of confidence in the impartiality, skills and professionalism of domestic law enforcement compared to the global aggregate.

Thinking about the most serious economic crimes your organization experienced in the last 24 months what actions did your organization take against the main **external perpetrator**?

	US 2016	Global 2016
Civil action was taken	17%	28%
Law enforcement informed	61%	53%
Notified relevant regulatory authorities	43%	38%
Cessation of the business relationship	17%	25%
Other	4%	10%
Don't know	19%	7%
No action taken	3%	9%

Detection methods to deter economic crime

Surprisingly, almost 1 in 5 organizations (18%) have not carried out a single fraud risk assessments in the last 24 months — or have done so only one time. The good news is that US companies overall are trending towards performing an increased number of fraud risk assessments on a more frequent basis. Fewer organizations report that they have not performed a fraud risk assessment at all (9% of those surveyed, down from 15% in 2014 and 19% in 2011). However, properly scaled fraud risk assessments are a baseline expectation of an effective compliance program for all companies, regardless of size.

As they increasingly adopt risk assessments and tighten controls, a higher majority of US organizations also report having a formal ethics & compliance program in place (89% vs. 82% globally). This is an improvement — but one in ten still without a formal program in place means there is a lot of ground left to cover.

For those with formal programs in place, it is too often treated as a check-the-box compliance exercise instead of a fundamental component woven into the values and beliefs of the entire organization. Regardless of programs initiated by leadership, economic crime continues to infiltrate all levels — from junior management (24%) and middle management (29%) to senior management (18%). This may be due to a "one and done" mentality on training — only 46% agree strongly that training is provided regularly and supported by regular communication and advice.

When calling for help

In the event that an organization identifies an incident of potential fraud, US companies are more likely than their global counterparts to seek help from the outside:

- 40% of US respondents stated they consult with their auditor; vs. 29% globally
- 36% contact external legal advisors; vs. 27% globally
- 29% hire a special forensic investigator; vs. 20% globally

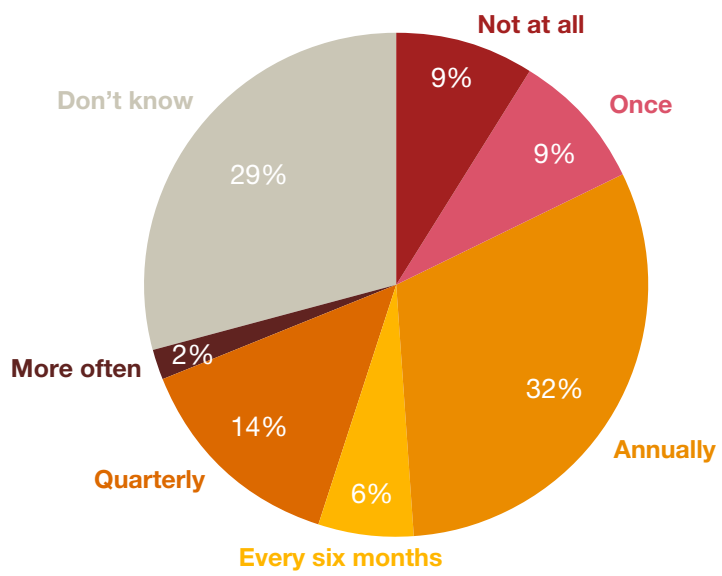
Those that rely on internal investigation resources plummeted 22 points to 67% this year, down from 89% in 2014. Does this indicate that US company leadership is increasingly seeing the value of bringing in an independent outside perspective? Or does it reflect the simple reality that today's more diversified and sophisticated crimes require specialized expertise that lies beyond current internal capabilities?

And what about when law enforcement is called in? We asked respondents to give us their views on whether they believe law enforcement to be adequately resourced and trained to investigate and prosecute economic crime. A majority — 52% — expressed doubts on this point.

Although this lack of confidence is echoed in global responses, this may be a surprising result for those who believe the US to be at the forefront of global economic crime enforcement. In the six years since the financial crisis, law enforcement has focused on high-profile investigations of large organizations. The public awareness and experience are there; where is the confidence?

Perhaps public opinion over the lack of individual prosecutions is impacting US responses. Respondents may view large prosecution settlements as merely punitive in nature, not driven by regulatory oversight, and some may view "deferred prosecutions" as not induced by law enforcement.

Fig 6: In the last 24 months, how often has your organization performed a fraud risk assessment?



From their opportunity to commit economic crime to your opportunity to prevent it

Our point on economic crime is that you should refocus your path to opportunity around strategic preparation — "strategic" in that it's related to and interwoven with the daily activities of a business unit as part of the overall ethical fabric of the company.

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 you are ready when threats become realities.

In the following three sections — dedicated to the strategically critical areas of cybercrime, ethics & compliance and anti-money laundering programs — we lay out insights, grounded in US and global responses, that can help you realize your opportunity to prevent economic crime.

We encourage you to take a step back and assess how these survey results impact your approach to the future, using the following lenses:

- ***What does this mean for your company, strategically, geographically, competitively?***
- ***What if you could….?***
- ***What would happen if you harnessed the power of data and analytics to better understand how economic crime could be mitigated or even controlled?***
- ***Back at the office: What can you do now to better address areas where you are exposed?***

You need to understand the vision of your company and strategically map out both a plan for growth and a plan for defense, based on your unique threat landscape and profile. This approach can represent the difference between the fraudsters' opportunity to commit economic crime and your opportunity to prevent it.

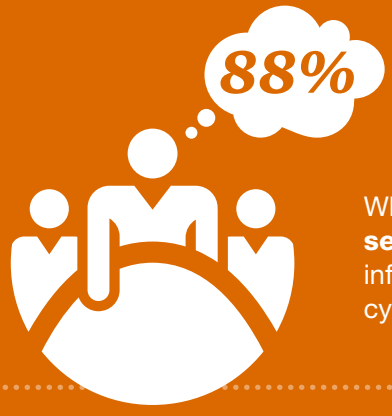
Your time is now: How will you prepare and bring your opportunity back into focus?

Cybercrime

Focus on the threats, transparency and teaming

54%

Cybercrime catches up to the top reported economic crime, affecting 54% of organizations – and **half of organizations expect to experience cybercrime** in next two years.



While **88% of CEOs are concerned about cyber security**[3], less than half of board members request information about their organization's state of cyber-readiness more than once a year.

Only 54% of organizations have an operational cyber incident response plan; the make up of those teams is not strategic and varies widely.

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

3 PwC's 19th Annual Global CEO Survey, 2016

Cybercrime races to the top

The prevalence of reported cybercrime among US survey respondents is sharply higher this year (54%), jumping to a virtual tie for first place among the most-reported types of economic crime in our 2016 Survey (within 1% of asset misappropriation).

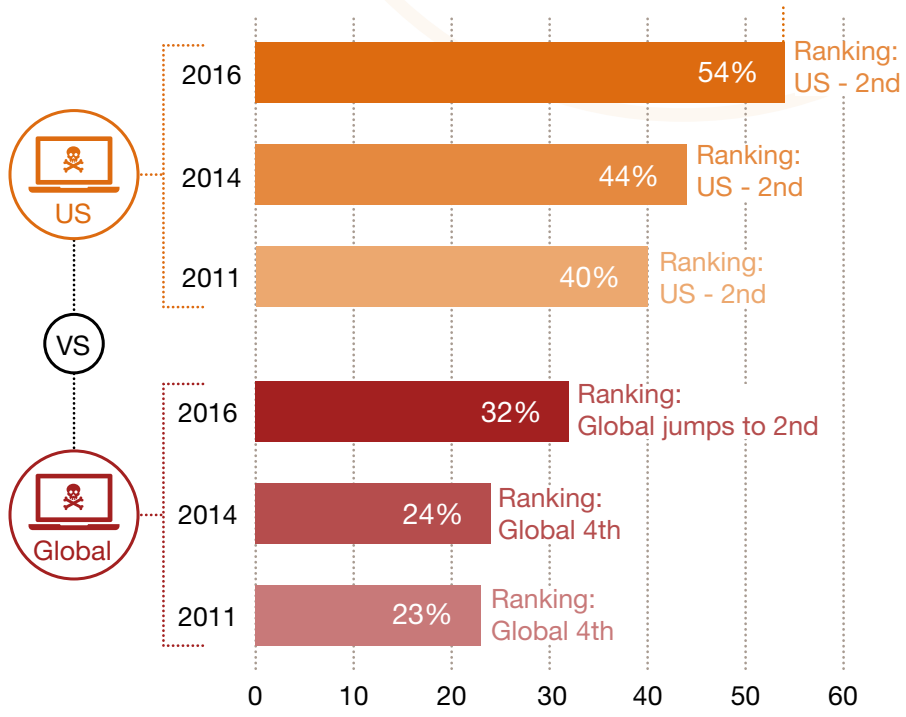
The insidious nature of this threat is such that of the 42% who believe they have not fallen victim to cybercrime (the remaining 19% stated they did not know), many may have been compromised without knowing it.

Like every other aspect of commerce, economic crime has, to some extent, gone digital. In a hyperconnected business ecosystem that frequently straddles jurisdictions, a breach to any node — including third parties such as service providers, business partners or government authorities — can compromise the organization's digital landscape in a variety of ways. 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: Companies today are able to cover more ground, more quickly, than ever before — thanks to new digital connections, tools and platforms which can link 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, 88% of US chief executives ranked cyber threats as a top threat to growth in the coming year[4].

Fig 7: Incidence of cybercrime among organizations who reported economic crime



The US Director of National Intelligence has ranked cybercrime as the top national security threat — higher than that of terrorism, espionage and weapons of mass destruction.

Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Committee, January, 2014

Threat vectors

Who are today's cyber attackers? They fall into 5 categories, each with its own agenda and means:

Nation-states
Threats include espionage and cyber warfare; victims include government agencies, infrastructure, energy and IP-rich organizations.

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

Hacktivists
Threats include politically focused service disruptions or reputational damage; victims include high-profile organizations, governments or even individuals.

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

Organized 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.

4 PwC's 19th Annual Global CEO Survey - US Results. PwC, 2016.

What does this mean for your company?

From our firmwide 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 adopting a proactive stance when it comes to cybersecurity and privacy. This necessitates that everyone in the organization — from the board and C-suite to middle management and hourly workers — see it as their personal responsibility.

Two kinds of cybercrime

We've come a long way from the days of teenage 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. In fact, 68% of all US respondents report having an "increased perception of the risks" of cybercrime.

Cyber threats may generally be segmented into two categories — (a) the kind that steal money and bruise reputations, and (b) the kind that can lay waste to an entire business:

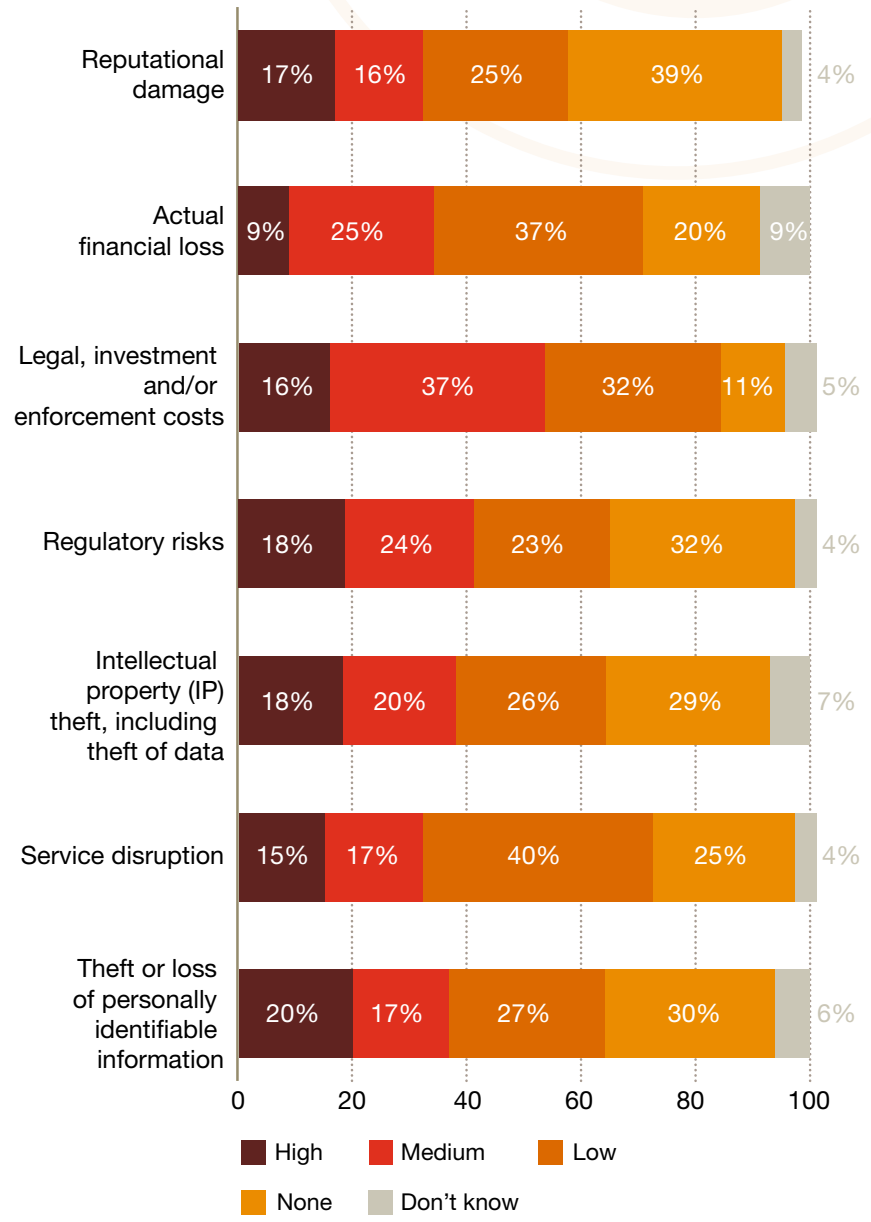
- ***Cyber fraud***
  Monetizable cybercrime, such as ID and payment card theft, are the events that tend to grab the headlines, with millions of dollars of losses and as many victims. Despite their high profile, they rarely pose an existential threat to companies.
- ***Transfer-of-wealth/intellectual property (IP) attacks***
  The more critical economic crime facing organizations 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" for good reason: damages could extend to the billions of dollars, and include the destruction of an entire 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 your 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 cyber-fraud, especially that involving the theft of personally identifiable information can be significantly greater.

Losses can be heavy

Seven percent of respondents reported losses over $5 million — with 2% reporting losses through cybercrime in excess of $100 million. Overall, the percentage of companies suffering a loss greater than $1 million has doubled since our 2014 survey (7% in 2014 to 15% in 2016) — a pattern that also held for all global respondents (from 3% to 7%). This speaks to the growing potency of cyber attacks.

Fig 8: Organizational impacts from cybercrime



What if you could...?

Take it to the top

Leadership attention is mission critical when it comes to addressing cybercrime — yet our survey suggests that many boards are not proactive enough regarding cyber threats. Globally, just 27% of boards request information about the company's state of cyber readiness more than once a year. Although the US outlook appears a bit better — with 40% reporting that boards request this information more than annually — both US and global results demonstrate that board attention on these issues is not where it needs to be. Perhaps US organizations are buttoning up at a time when federal agencies and regulators are taking a firmer stand in the area of cybersecurity. To wit, the US Securities and Exchange Commission has issued a warning that future examinations will consider a company's cyber response capabilities.

Pull together the "A" team

Just 54% of US respondents — most of them in the heavily regulated financial services industry — have a fully operational cyber incident response plan. Seventeen percent have no plan at all, and of these, one out of three don't even think they need one.

Should a cyber crisis arise, do you have fully trained responders? Fewer than half (48%) of those surveyed reported that they do — of which the overwhelming majority (90%) are IT staff.

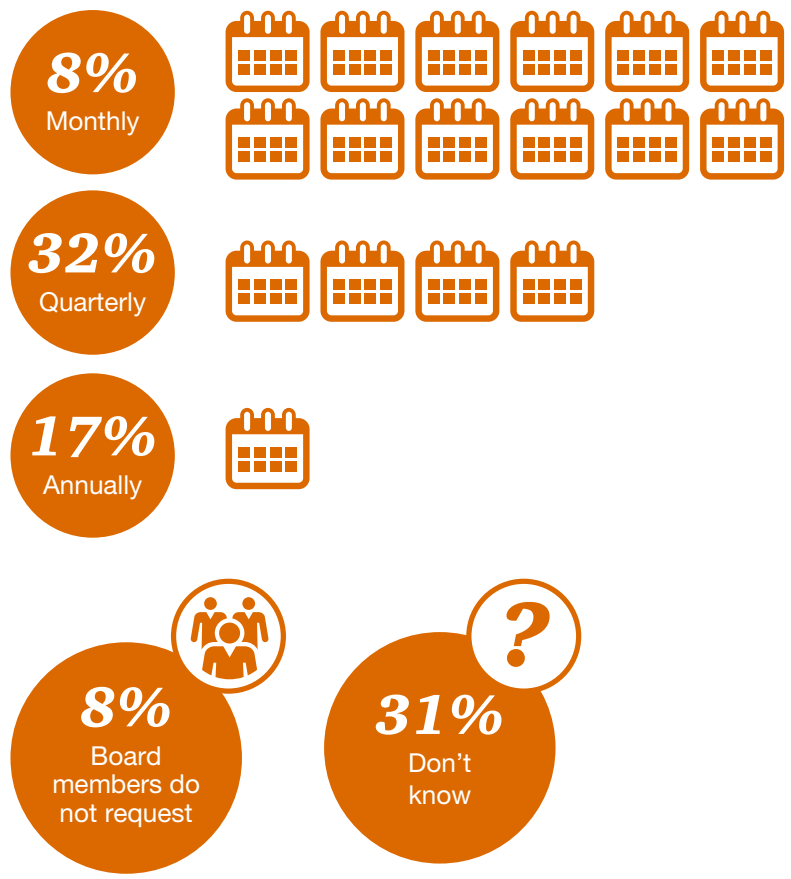
While IT has a critical role to play in detecting and mitigating an attack, it is noteworthy that half or fewer reported that their first-responder teams include key crisis management players such as: legal (50%), HR (35%) and digital forensic investigators (34%).

Perhaps even more confounding is that 60% have identified first responders internally (and another 6% have outsourced that role) — which exceeds the 54% that have operational plans. There's no doubt that having responders without a set plan is inefficient. Leadership needs to ensure they have both an operational cyber response plan and a trained team, and that the two work in lock step.

"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."

US Secretary of the Treasury Jacob Lew

Fig 9: How often do board members request information regarding the organization's state of readiness to deal with cyber incidents?



The lack of awareness and alignment on cyber threats is further underscored by our 2016 Global State of information Security Survey, which reported that only 45% of boards participate in the overall security strategy.

PwC's 2016 Global State of Information Security Survey. PwC, 2016

These results suggest that many organizations, in their understandable haste to contain the breach and get their systems up and working again, are at risk of overlooking potentially crucial evidence. This could later hamper their ability to prosecute and, more importantly, to understand how the breach occurred. It could also represent a lost opportunity to improve future prevention and detection efforts.

When it comes to seeking help from local law enforcement, the results showed surprising caution. Only 23% of US respondents said they had confidence in local law enforcement's ability to effectively investigate cybercrime (identical to the global rate of confidence). This may suggest that the overall business community does not feel that law enforcement has caught up to, or thoroughly understands, the true cyber threats that companies face. As organizations are forced to take on the burden of preventing and remediating cyber threats, regulators need to continue their push to be as close to the front lines as possible.

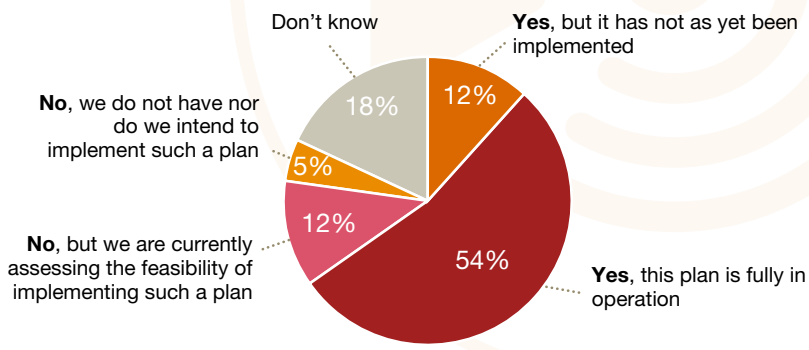
Give cyber a wider scope

Preparedness for cyber crime must be embedded within the wider scope of crisis planning, not separate from it. 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. Organizations need a strategic, organization-wide response plan that details roles and responsibilities, monitoring and scenario planning.

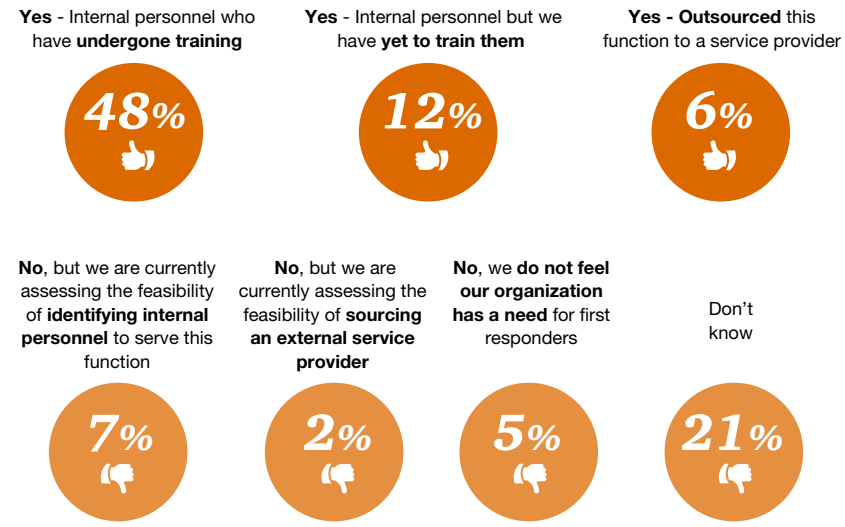
Cyber threats and mitigations are the responsibility of the entire enterprise; all have a crucial part to play. Yet while we have seen major strides in sophistication and cyber-preparedness since our last survey, most companies are still not adequately prepared either to understand the risks they face, or to anticipate and manage incidents effectively.

Fig 10: Cyber incident response plans and team composition

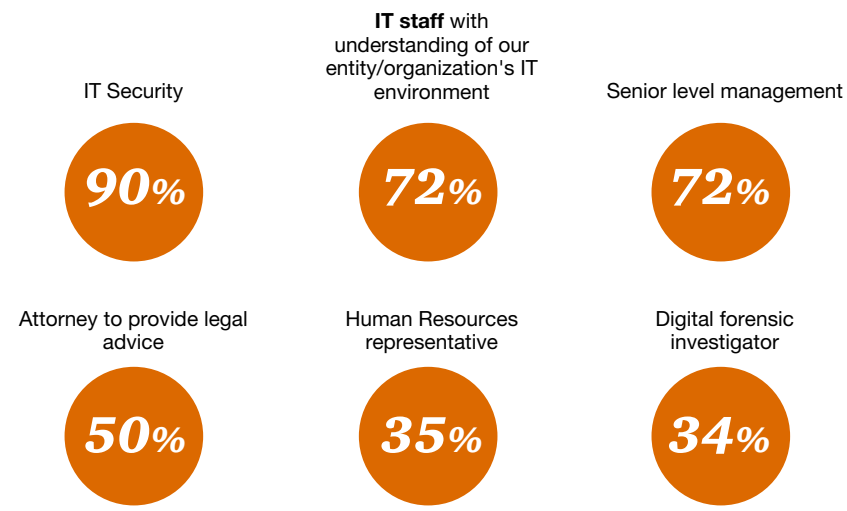
Do you have a plan?



Have organizations identified first responder teams?



Composition of first responder teams



Other: 5%

Back at the office: What can you do now?

Accelerate board involvement

Boards of directors have a fiduciary responsibility to shareholders when it comes to cyber risks. Guidelines from the National Association for Corporate Directors (NACD) advise that boards should view cyber-risks from an enterprise-wide standpoint and understand the potential legal impacts. But we know from our survey results that this is not happening as often as it should. Enhanced communication between company leadership and the board — perhaps even including company-wide training on common cyber threats and techniques — can help build and strengthen company clarity and preparedness. Critically, cyber-preparedness need not be a fear-based activity. It should be treated with openness, as a risk that should be managed as part of the organization's overall risk tolerance.

Reassess your responder team

First responder teams should include all aspects of the business, including legal, HR and digital forensic investigators. Critically, it should also include organizational leadership, communications and public relations teams.

Convene regular tabletop exercises

Like any other emergency readiness plan, the table-top exercise — a "plan for a plan" which mimics cyber crisis scenarios — should be conducted regularly. Many companies integrate regular crisis management exercises as a central element of their cybersecurity and incident response strategy, convening table-top exercises on specific scenarios, pressure-testing incident response plans, and identifying any gaps or shortfalls that need resolution. The process 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.

Learn from others

It's clear that the threat of cybercrime is greater than any one individual company's ability to address it. Despite often competitive perspectives, companies, governments, law enforcement and competitors realize they need to collaborate to combat it effectively. According to PwC's State of Cybercrime 2015 survey[5], 82% of companies with high-performing security practices collaborate with others to deepen their knowledge of security and threat trends. Notably, President Obama signed an Executive Order to promote the creation of Information Sharing and Analysis Organizations (ISAOs). Congress also recently passed the Cybersecurity Act of 2015[6], which provides a framework for the sharing of cyber threat information between private industry and the government.

Hone in on your specific needs

The cyber threat equivalent of the question "What keeps you up at night?" is whether you're capable of and prepared to take action. If the answer is "No," and your organization cannot act organically, ensure that you have a service provider with the technical and legal expertise required to fill the action gap[7].

A cyber corporate crisis is one of the most complex and challenging issues an organization 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 at it as an organizational 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, its survival.

Game of Threats: PwC's cyber threat simulation

Game of Threats™ is a digital game that is designed to simulate the speed and complexity of an actual cyber breach by integrating elements of game theory in an interactive company experience. The game environment creates a realistic encounter where both sides — a threat actors team played by company personnel and a company team to defend the organization — are required to make quick, high impact decisions with minimal information. Game of Threats is a critical decision-making game designed to reward good decisions, penalize poor ones and provide organizations with a better understanding of the steps they need to take to better secure their organization today and for the future.

5 PwC's 2015 State of Cybercrime Survey. PwC, 2015.
6 Consolidated Appropriations Act, 2016. https://www.congress.gov/bill/114th-congress/house-bill/2029/text#toc-HFACF06D6097F4214B31BA54F817EC583
7 PwC's Cybersecurity & Privacy blog. http://usblogs.pwc.com/cybersecurity/cyberthreat-intelligence-a-call-to-evolve-beyond-the-feed/

Cybercrime: What if you could harness the power of data & advanced analytics?

Today's cybersecurity models are waging an "effectiveness" battle against cyber attacks and are often losing. But most businesses are over-saturated in the day-to-day management of relentless cyber-risks and lack the time and resources to reinvent their cybersecurity programs.

Your cybersecurity program should harness the power and efficiency of data, analytics and cloud computing to safeguard your business before, during and after detection of security incidents. This approach can bring plentiful benefits, including:

- **Continuous threat monitoring and information sharing** across the organization's digital ecosystem in real time. This enables companies to visualize, correlate and quickly analyze their unique security-event data against live intelligence.
- **Real-time security analytics and detection**. Rapid detection of cybersecurity incidents is increasingly critical to curtailing damage and losses. Analytics platforms enable businesses to quickly collect and analyze enormous volumes of enterprise security data, then compare threats to a global database of threat intelligence. The solution can immediately transmit alerts to system administrators when relevant threats are detected.
- **Prioritization of threats based on your unique business risk profile**, by performing targeted searches and analytics across your historical security data. This helps map out support to the parts of your business that would be most impacted by the attack.

Most businesses also don't have the specific expertise, technology infrastructure and global access to threat intelligence necessary to single-handedly transform cybersecurity, and will need to look to outside providers and experienced specialists to find the right program attuned to their company risks and nuances. With this kind of data-driven defense, they can better block attacks, enhance collaboration, and accelerate incident detection and remediation across globally dispersed IT environments in real time.

Ethics & Compliance

Putting a values-based program back into focus

89%

of US organizations say they have a formal ethics & compliance program, but **only half strongly agree that organizational values are clearly stated and well understood**.

53%

Share of internal perpetrators are middle management; this year also saw a 350% increase in senior management as the perpetrator of internal crime (18% up from 4%).

1 in 5

state that "pressure to perform" is contributing most to internal crime.

In the next 2 years companies expect to be hit by all types of crime:

- Cyber crime (49%)
- Asset misappropriation (36%)
- IP infringement (25%)
- Bribery and corruption (14%)

Weaving in values and ethics has never been more important. Crime damages relations with regulators, brand reputation and employee morale.

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

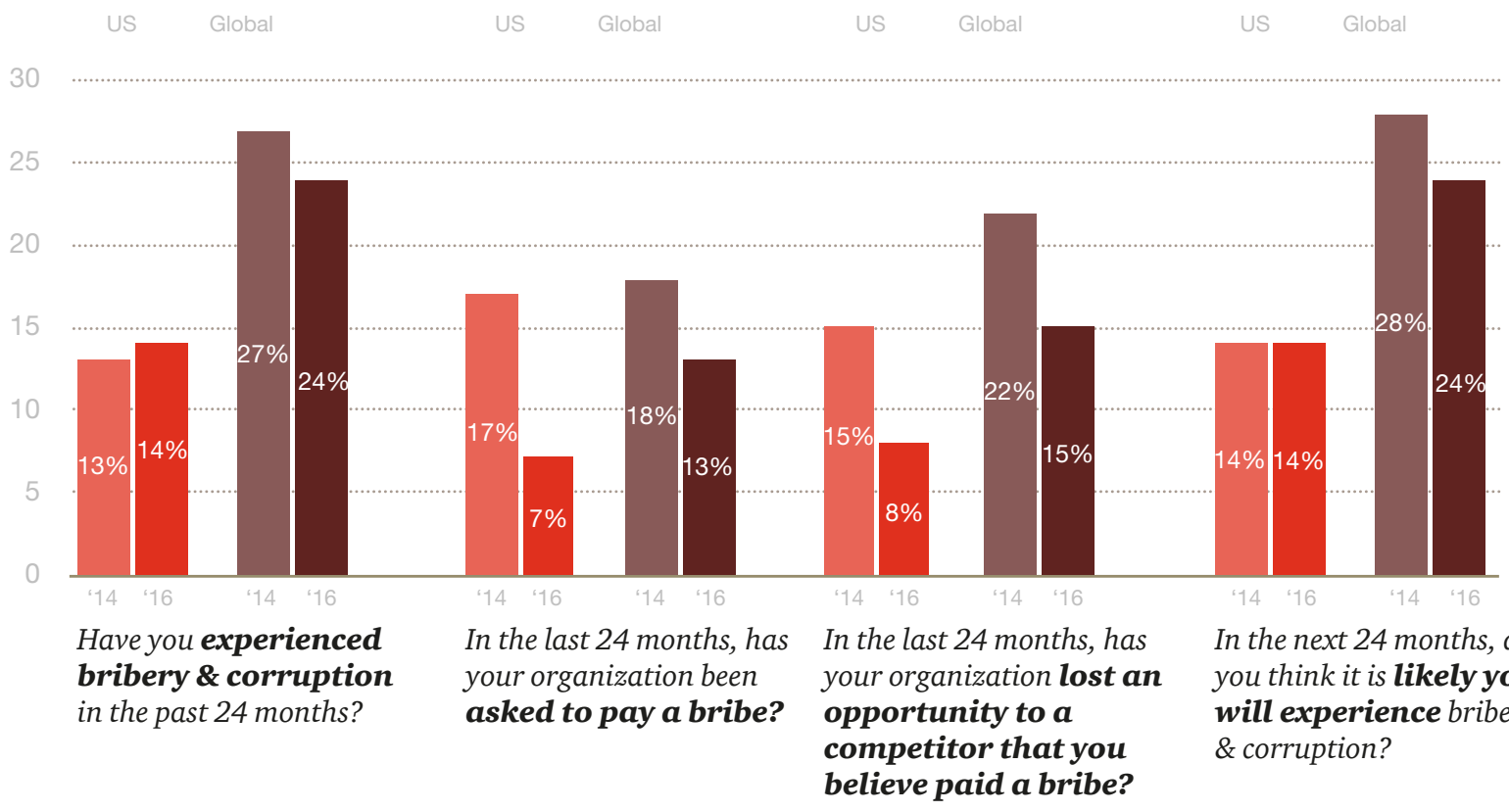
Instances of economic crime are down; defense mechanisms shouldn't be

Thirty-eight percent of US organizations reported experiencing some type of economic crime over the last two years, down from 45% in our last two surveys. But beware a false sense of security: a closer reading of the data reveals important nuances.

While experiences of bribery and corruption, at 14%, were essentially flat, and "traditional" frauds such as asset misappropriation, procurement fraud, IP infringement and accounting fraud were down from their 2014 levels, other crimes — notably cybercrime, money laundering, HR fraud and mortgage fraud — increased sharply.

Given today's mercurial business trends — including globalization, growing technological dependency, more vigilant enforcement and greater demand for public accountability — a short corporate memory is dangerous. It is imperative that organizations and their leadership see the value in investing more resources into ethics and compliance programs, even if they have not observed an increase in their own experience of economic crime.

Fig 11: Experiences of bribery and corruption



US CEOs agree:

55%

state a lack of trust in business is a key threat to growth[8]

8 PwC's 19th Annual Global CEO Survey. PwC, 2016.

What does this mean for your company?

Consider this: You have a formal code of conduct with which employees must comply. You also have organizational values. You know it's not OK to offer (or take) a bribe. But does everyone really believe that? Who is assigned to ensure compliance? How are you assessing potential risks? How are you weaving your company values into every aspect of your culture?

Realize that bribery and corruption will always be a threat

Our study results show that this year, fewer report having been asked to pay a bribe in the last 24 months (7%, down from 17%) — and half of the reported rate from all global respondents (13%). Anti-bribery and anti-corruption policies also seem to be more effective: just 8% of US respondents stated that they lost business to a competitor that they believe paid a bribe, down from 15% in 2014 (and again, about half the global rate of 15%). These trend lines, both globally and domestically are encouraging.

While the news is mostly positive, the harsh reality is that bribery and corruption will likely never be eradicated. They still account for one-quarter of reported global crime and 14% in the US; and 14% of US companies told us it is "likely" they will experience bribery and corruption in the next two years. These are significant numbers, particularly due to the potential for staggering fines and penalties, not to mention the potential damage to brand that accompanies bribery scandals.

Beware the perception gaps

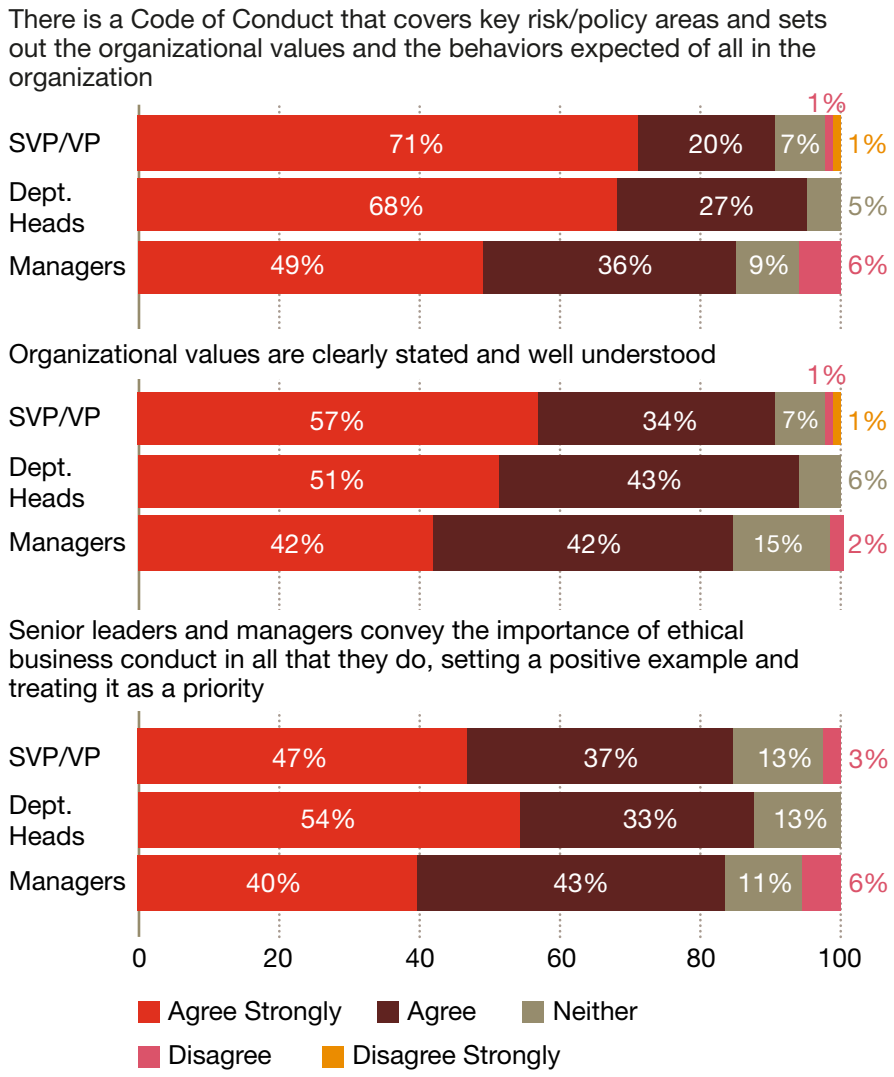
Consider recent, highly publicized incidents involving iconic automakers and global financial institutions — all of whom have well-established ethics and compliance programs. Do these lapses indicate that such programs are not keeping up with changing business risks? That they are sending mixed messages? Or is there a deeper reason for the disconnect?

Ethics and compliance programs are a deterrent that can help create a good environment, but it is important to remember that preventative controls and ongoing monitoring are also crucial elements. A program alone — no matter how thorough — will likely not stop an employee motivated to commit fraud. Simply stated, ethics and compliance programs are a piece of the puzzle — but not the puzzle alone.

The numbers also point to a perception gap between what CEOs and boards believe and communicate is happening — and what's actually taking place in the business, particularly among senior and middle managers in their day-to-day roles. Our survey identified areas where leadership is not perceiving the same realities as those in the middle:

- While the majority of organizational SVPs/VPs and heads of department "agree strongly" that the code of conduct sets out key risk areas and expected behavior (71% and 68%, respectively), that figure drops to 49% for manager respondents.
- 57% of SVP/VPs and 51% of department heads agree strongly that their company's values are clearly stated and understood, with only 42% of managers saying the same.
- When asked about senior leaders and managers conveying the importance of ethical business behavior and setting a positive example, SVPs (47%) and heads of department (54%) strongly agree, but only 40% of managers strongly agree that this takes place.
- Consider the change in the perpetrator in the US: the share of internal fraud committed by senior managers has more than quadrupled since the last survey, from 4% to 18%. This is a sharp contrast to what global businesses are experiencing, where senior management culprits decreased from 20% to 16% this year.

Fig 12: Are senior management and boards perceiving the same realities as those in the middle?



What if you could...?

Make compliance assessment a multi-layered effort

A large majority (87%) of respondents told us they are relying on their internal audit function (IA) as part of their approach to assess the effectiveness of their compliance programs. More than half (53%) also state they rely on external auditors for this task. While the audit is an important piece of the compliance framework, it is not by itself a sufficient means of confirming compliance.

Fraud schemes can often find a way around established control frameworks, usually through some sort of internal collusion. Internal Audit's interventions are generally periodical and after-the-fact, whereas the fraud risk profile companies face is constantly changing (consider the sharp increases in cybercrime and money laundering, and the drop in asset misappropriation and accounting fraud).

Since prevention must ideally occur at the point of decision making, effective controls should be integrated with management reporting, real-time monitoring, whistleblower hotlines and other measures to ensure that issues are detected and prevented in time.

Know who has ownership — it's half the battle

It's important that all people across the business — not just your compliance professionals — understand their role in ensuring that operations are aligned with ethics and compliance policies. Still, many companies exhibit a degree of confusion about who has ownership for what. Of the 89% who have a formal business ethics and compliance program, responsibility for that program is widely dispersed among roles.

In some organizations, there is a tendency to view compliance as a kind of insurance policy upon which a passive responsibility can rest. This lack of codification of roles can lead to structural problems.

Fig 13: How do you ensure that your compliance and business ethics program is effective?

Compliance professionals are the stewards of oversight and guidance, but as a matter of course are rarely in a position to commit fraud. Fraud is more likely to occur with client-facing employees, or those in the field — especially in organizations with a wide global reach. Getting these individuals to understand and buy into their roles and responsibilities as they relate to compliance is critical. Therefore, forward-thinking organizations position themselves as being a broader "compliance community," wherein the roles and responsibilities of ethics and compliance become part of day-to-day business for everyone. We believe this is a healthy, positive approach: ultimately, all hands should be on deck — and rowing in the same direction.

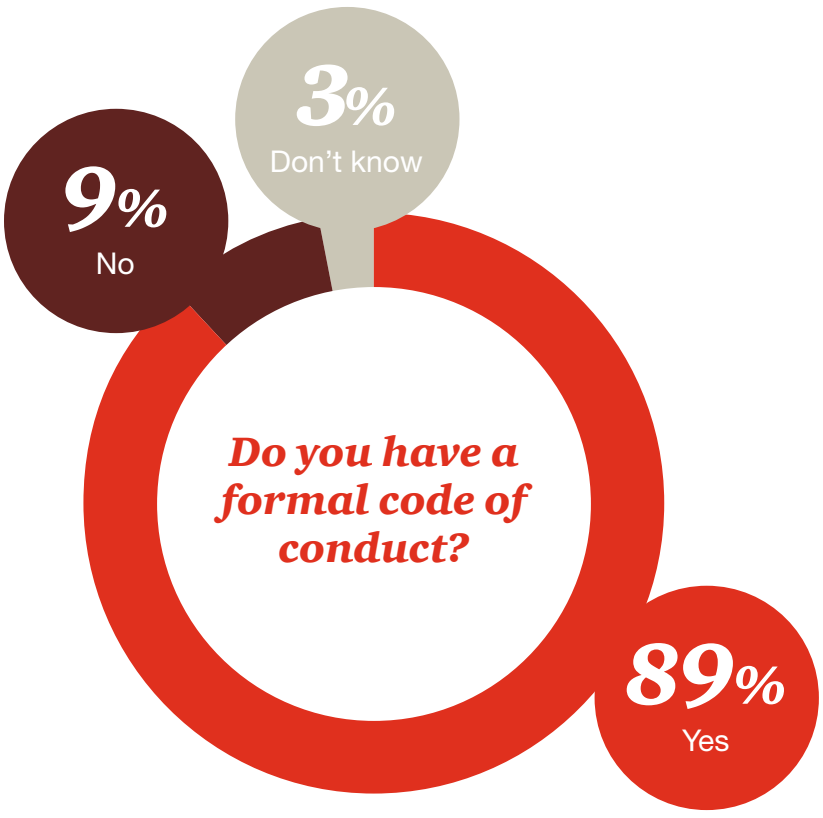
Put a detail-oriented lens on high-risk areas

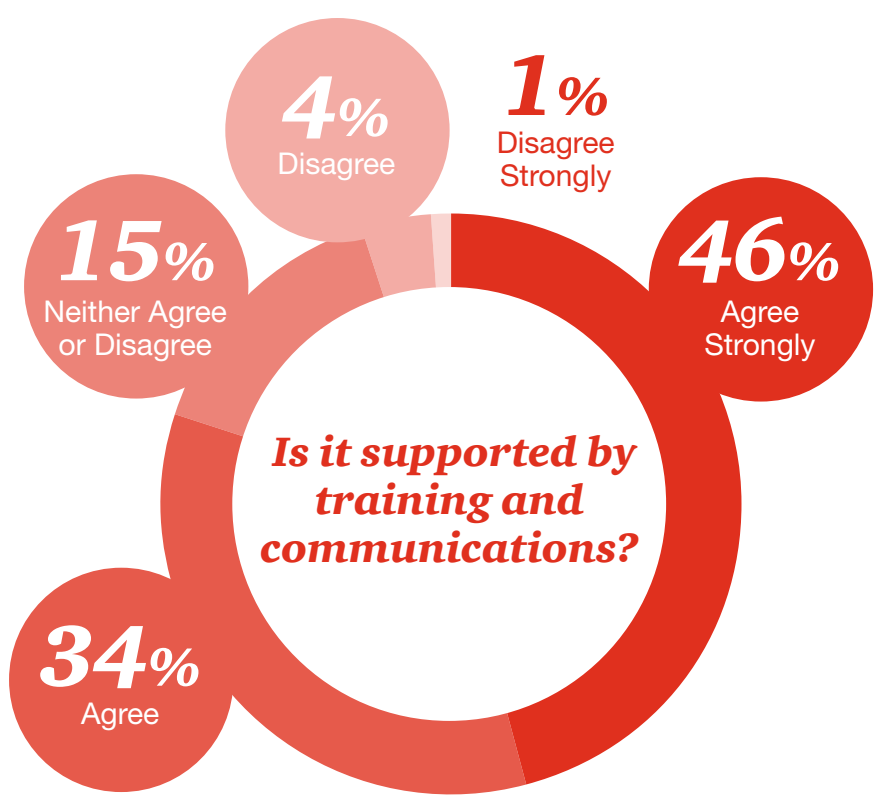
Regulators have increasingly shown a willingness to hold companies liable for unethical behavior that takes place far away from the head office. Overall, 90% of respondents agreed with the statement that top-level management made it clear that bribery is not a legitimate practice — but 1 in 10 still disagreed or were neutral on this point. Focus on communicating and training to the unique regional risks in the areas you operate. Only 80% reported that training was provided regularly and supported by regular communication and advice.

Take a fresh look at your compliance program

What is legal and what is ethical are not necessarily the same thing. Top teams focus on understanding what really drives behavior — and then set about to build a positive culture that incentivizes the behavior they want. Many organizations are increasingly combining a values-based program with heightened behind-the-scenes monitoring. This makes things more transparent to employees while also giving leadership the comfort of enhanced data-based monitoring and detection systems.

Fig 14: Is the code of conduct adequately supported by training and communications?





Back at the office: What can you do now?

Treat fraud risk assessment like a routine physical

Although more US companies are trending towards performing fraud risk assessments, on a more frequent basis, a concerning percentage (9%) report not performing a single one in the past 24 months. Every company, regardless of size and industry, should conduct these risk assessments routinely — preferably more than once a year. Consider it a baseline expectation of an effective compliance environment.

This should be a proactive measure, not a reactive one. Treat it like a routine, organizational physical to help ensure that the types of compliance breakdowns that happen to other companies don't happen to yours. This can be very effective in a regulatory context, where the company can demonstrate that it has performed the appropriate diagnostics and has the data sets to back it up. It can also be well-needed ammunition for conversations with the C-suite, board and/or audit committee, should you need to raise a red flag on structural, regulatory or budgetary issues or control deficiencies.

Reassess your compliance program

There is no need to re-do your program, just make sure you are going deep enough based on your company's footprint. Conduct a risk profile, evaluate what you are doing and what you want to achieve, and then assess what internal actions need to be taken. Figure out the "best in class" compliance program for your company; not the overall "best in class" or a carbon copy — but the best model for your business, industry and size.

Consider combining your code of ethics with your code of conduct

We've seen success where organizations combine their code of conduct with their ethics policy. Employees are provided a much clearer definition of the actions and behaviors that are permitted, versus those that are discouraged or prohibited. This offers measurable and valued assistance to employees, and can provide evidence to regulators that the company is acting transparently and ethically. Be sure to keep the message as simple and clear as possible — and don't overlook ensuring your policies, manuals and training are correctly translated as needed, with appropriate cultural nuances.

Ultimately, at the heart of any economic crime is a poor decision driven by human behavior. A sophisticated, risk-based approach to ethics and compliance should begin with a holistic understanding of your economic crime risk and an understanding of where your compliance weaknesses are, and then wholly encompass your people as the first line of defense. 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 organization.

Ethics & Compliance: What if you could harness the power of data & advanced analytics?

Increased regulatory scrutiny has elevated the need to look beyond whistle-blowers or "smoking guns" as a way of uncovering bribery and corruption. Today there are several sophisticated tools — including big-data analytics capable of more effective monitoring — that can help bring compliance closer to operations by handling a variety of structured and unstructured data.

Few organizations are using these kinds of technologies to help detect and prevent economic crime; only 6% of US respondents indicated that they use "other" internal monitoring approaches such as data or predictive analytics to ensure their ethics and compliance program is effective.

- ***If you are just starting out:*** We have observed that rather than beginning with the "big data" of transaction monitoring, it is often better to start with the "small data" of risk assessments. A strong model encompasses the spread of risks an organization 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
- ***If your program is developing/mature:*** When it comes to proactive fraud detection, rather than apply a series of "red flag" tests to transactions, companies can statistically model vendor or employee activity using cluster analysis to detect behaviors that differ significantly from the norm.

In addition to traditional screening (exception testing) and searching (keywords) of transactions, advanced and innovative techniques are being used to uncover previously undetected relationships or patterns, including:

- Faceted search over multiple-structured data
- Interactive network visualization of financial transactions
- Semantic extraction from unstructured text enabling "intelligent" queries and search
- Ultra-fast, highly advanced, fuzzy logic text search engines to interrogate millions of records across disparate information systems

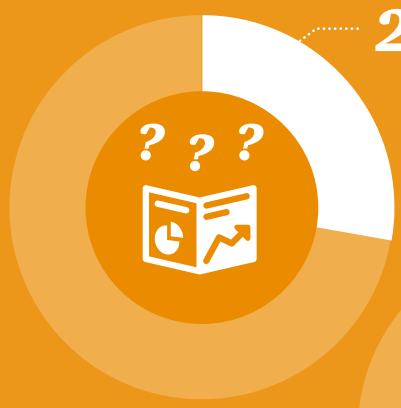
An approach using sophisticated analytics — alongside a centralized governance and operating model — can help you evaluate the broad transaction monitoring efforts currently in use and focus them on the real threats to your company. Ultimately, the focus should be not on technology, but rather on what it enables and how it can help you stay ahead of compliance risks.

Anti-money laundering

Focus on increasing regulations and enforcement

1 in 4

banks have experienced enforcement actions by a regulator and the pace of regulatory change is increasing.



28%

Financial services respondents cite challenges with **complexity of implementing/upgrading systems** (28%) and **data quality** (26%).

26%

Only 40%

of money laundering or terrorist-financing incidents were **detected by system alerts**.

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

Money laundering: A greater threat than ever

Money laundering destroys value. By enabling criminals to hold or transfer the necessary funds, it facilitates economic crime and nefarious activities such as corruption, terrorism, tax evasion, and drug and human trafficking. It can be detrimental to an organization's reputation — and its bottom line.

Over the last few years in the US 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.

And it's not just financial services institutions. As industries converge, any organization that facilitates financial transactions is coming within the scope of anti-money laundering (AML) legislation worldwide — including (to name a few) operators offering digital/mobile payments, money service businesses, retailers and insurers of all types. Alarmingly, but not surprisingly, many of these new participants are not yet up to speed on the applicable requirements or on the proper compliance programs needed to properly onboard new customers and monitor their relevant transactions.

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

9 2020 Foresight: The Impact of Anti-Money Laundering Regulations on Wealth Management. WealthInsight, 2013.

How will cryptocurrency add complexity?

Cryptocurrency, part of a larger trend of diversification of payment processes, is playing a growing role in the "flattening" of payment options. With the convenience and anonymity it affords, cryptocurrencies such as Bitcoin are adding to the growing concerns about money laundering and terrorist financing. On a global level, the inter-governmental Financial Action Task Force (FATF) is undertaking meaningful discussion of AML standards as they relate to cryptocurrency.

Seven percent of US respondents in our survey (6% globally) listed the complexities of doing business in emerging industries as the most significant challenge they faced in AML compliance. We would expect this trend to continue to increase as controls steadily evolve to the point where — as with bribery and corruption — the effectiveness of controls will temper organizations' worries about future threats.

What does this mean for your company?

Heightened regulatory standards

Our survey shows that the level of enforcement of AML and combating the financing of terrorism (CFT) measures has created challenges even for financial institutions with the most sophisticated AML compliance programs.

As financial services organizations grow by acquisition, their legal vehicles, businesses and markets are not always immediately consolidated into group processes or standards. Further, many are still struggling with the aftermath of regulatory actions or sanctions. Our survey found that almost one-quarter of banks (24%) have recently experienced enforcement actions by a regulator.

What's more, some financial institutions have come into the crosshairs of regulators in one country for illicit business practices in another.

AML watchdogs and regulators

- **The Office of Foreign Assets Control (OFAC)**, under the US Treasury Department, maintains and administers a number of US economic sanction programs and embargoes.
- **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 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 *inter alia* lists of persons against which sanctions have been imposed, such as known terrorist organizations. These lists are often used by participating governments to support measures against terrorist activity.

It's not just business — it's personal

The days of individuals being protected by corporate settlements will soon be gone. Some regulators are looking to assign personal accountability to individuals involved (or responsible for) compliance failings. Certain governments have imposed substantial fines — and in some cases, pursued criminal action — against financial institutions that have not implemented sufficient controls to monitor their global transactions. Some have further signaled an intent to pursue individual criminal prosecution — including potential jail time — where individuals are found to be complicit in illicit business practices or even substantive compliance failures.

"Regulation by examination"

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

Global compliance is more than following jurisdictional laws

Organizations 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 — and by extension the obligations of banks and other regulated institutions.
- OFAC, along with other national treasuries such as Her Majesty's Treasury, administers economic sanctions programs — and by design is focused on the movement of goods, services and funds overseas and across borders.
- Increasingly the regulatory frameworks of the major financial centers — e.g., 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.

What if you could...?

Get the right people, with the right skills, in the right place

Survey respondents told us that hiring experienced staff is one of the most significant challenges they face in the AML arena (16% of US respondents; 19% globally). The cost of hiring the right resources has recently skyrocketed and today's supply of talent continue 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.

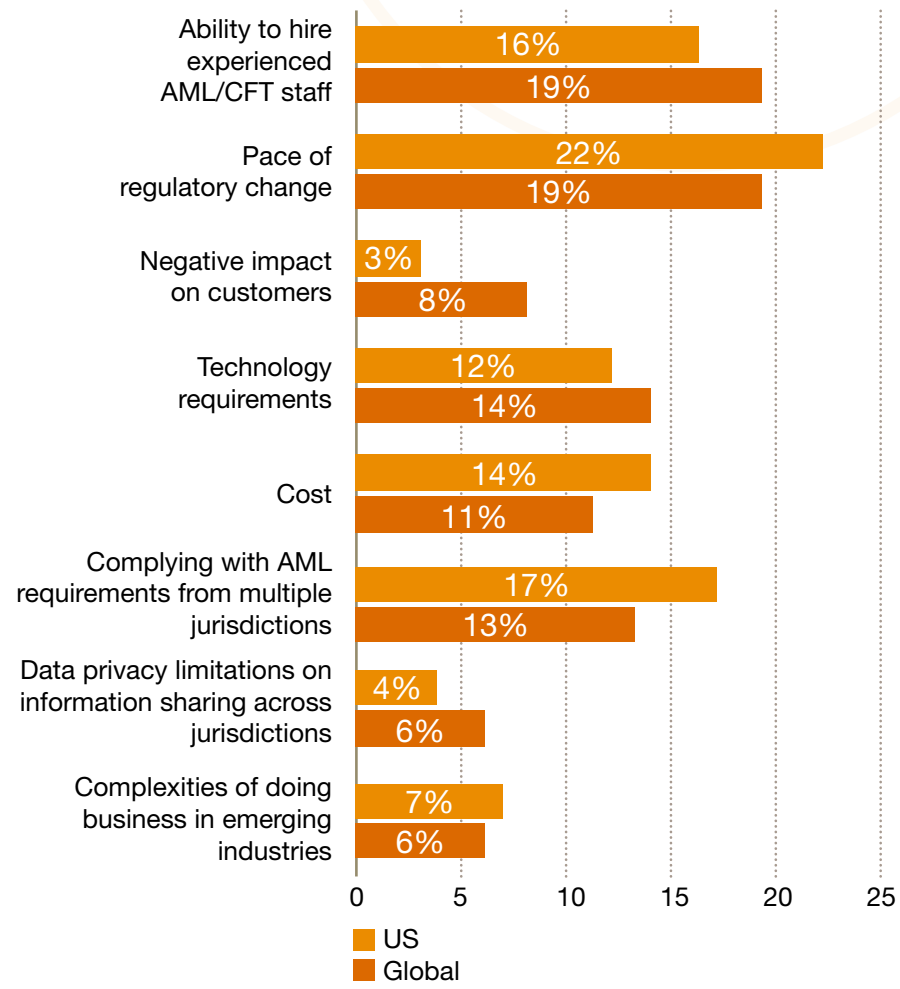
Identify risks everywhere

Over the last decade, improved money laundering control measures have forced criminals to seek new ways to "move" the proceeds of their crimes. Trade-based money laundering, for example — a complex system of false documentation that enables criminals to earn and move value around the world under the guise of legitimate trade — is becoming harder to detect through traditional transaction monitoring systems, despite the efforts of financial services organizations.

That's why regular risk assessments are critical; they enable your organization to identify and address the money laundering and terrorist financing risks you face — wherever and with whomever you do business. As the sophistication of money launderers continues to grow, this is a measure that cannot be put off. Yet despite the clear advantages of doing so, nearly 12% of financial services respondents are not currently conducting an AML/CFT risk assessment across their global business footprint.

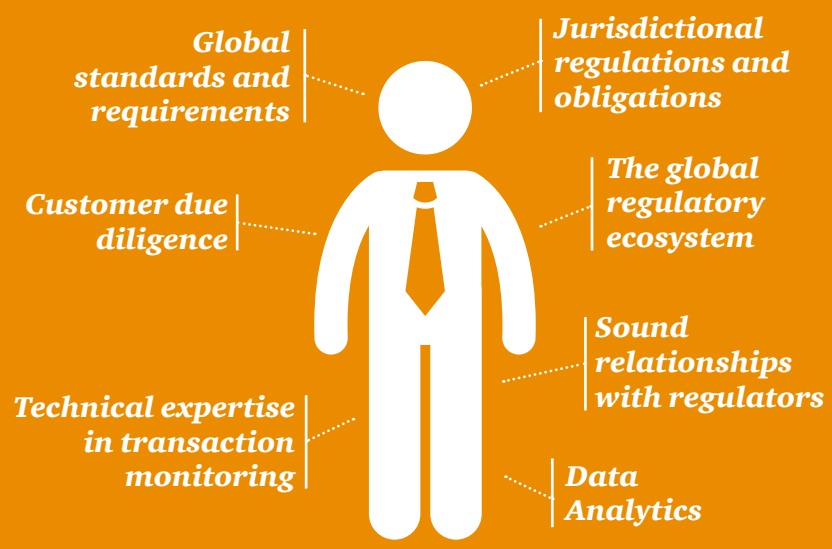
Risk assessments should be conducted on a periodic basis. They should be closely attuned to changed circumstances such as the operating environment, evolving product and service offerings, global standards and regulation in countries of operation. Notably, assessments should also include the profiling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

Fig 15: Challenges to complying with local AML/CFT requirements



What skills do you need?

When your best line of AML defense 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 specialized expertise and skills around:



Know your customer, today and tomorrow

Transparency into your customer base goes beyond merely identifying and verifying the information they provide. It must not be a static act; it must be dynamic with continuous monitoring for red flags and suspected profile changes. 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. In territories outside of the US, customer on-boarding and customer due diligence (CDD) standards are increasingly being heightened, making adherence to multiple standards more complex, particularly for large financial institutions.

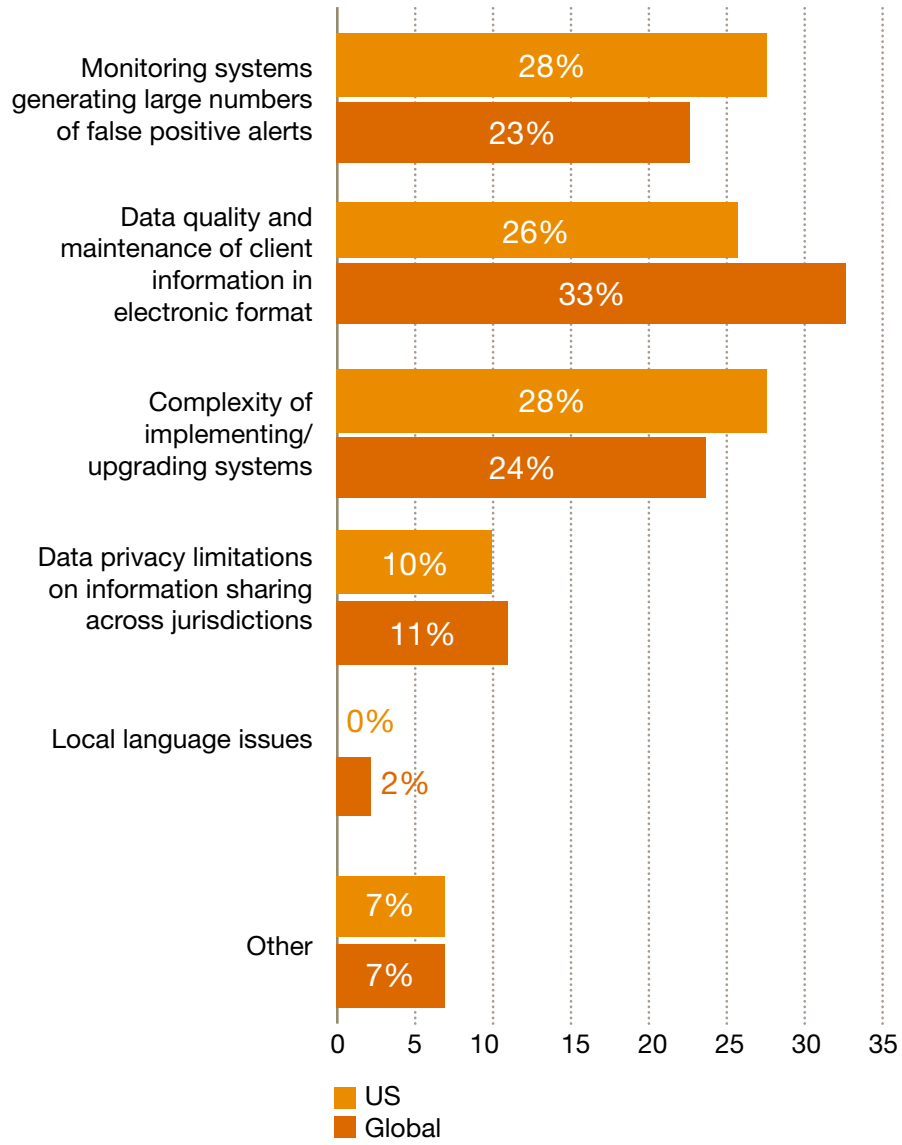
Set a clear systems strategy

Companies across the industry spectrum seem stuck in a bind. Most are facing the hurdle of "rightsizing" their AML programs for their changing business in an ever-advancing regulatory landscape. Yet many are hampered by legacy monitoring systems that are proving to be burdensome and expensive to tune and maintain.

As you refocus on a systems strategy, you may ask "why aren't more organizations making the leap to new systems and technologies?" Some leading reasons include:

- The cost and complexity to implement some of the new sophisticated data analytics platforms can be prohibitive to many. This can stunt organizations trying to move from a cumbersome transactional testing basis to a more strategic and efficient approach.
- AML alert monitoring often yields sub-par performance. Only four in 10 respondents said suspicious money laundering of terrorism financing incidents are being flagged by transaction monitoring systems, putting companies at risk. Current AML typologies might not be catching the nuances and complex structures necessary to identify high-risk transactions.
- Converting to new analytic models and platforms is not yet a widespread phenomenon. This could be an indication that institutions have "priced in" a certain degree of ineffectiveness in their legacy detection systems that they are willing to accept. However, as the volume of transactions continues to grow and the cost of maintaining old systems becomes increasingly onerous, this may well prove to be a disadvantage.
- Institutions may be concerned or skeptical about regulatory acceptance of new and uncharted analytical approaches, which will require rigorous testing and validation.

Fig 16: AML/CFT systems challenges



Back at the office: What can you do now?

Keep your finger on the regulatory pulse

With the globalization of AML/CFT standards, it's important to remember that you may be judged against, and held to, the highest international compliance standards. Ideally, your organization should go beyond mechanical compliance with today's laws. You should look ahead and identify how to properly structure your organization to comply with upcoming legislative trends. Focus on having a viable function within your organization that owns the role and keeps track of pending regulations in this area.

Learn from others' mistakes

Look 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 the penalties imposed. Since most transactions have a multinational financial component, it's a good practice to default to the highest global standard of compliance whenever possible and to undergo more rigorous AML/CFT self-assessments. Establish "enterprise-wide" requirements to ensure consistency across geographies, enforcement jurisdictions and business units.

Reposition your AML approach as proactive

Focus on championing the effective transfer of knowledge through an energized approach to your people, processes and philosophies. By shifting the perception of AML programs from a reactive, problem-solving approach to one that focuses on proactive, enterprise-wide solutions, financial institutions can reposition AML strategies as models for efficiency, consistency and responsibility.

When faced with dynamic AML standards and incumbent challenges, it is wise to aim to lead the pack, not follow. Being in the middle of the pack exposes your organization to the risk of falling behind the regulatory curve. Focus on being strategically nimble and innovative to stay on top of regulatory changes. One thing is abundantly clear: a great deal of judgment will be required in crafting financial crime compliance programs that are manageable today — while protecting you from tomorrow's threats.

FATF: A new focus on effectiveness

FATF has shifted its evaluation standard of countrywide AML/CFT standards from technical compliance to effectiveness, where all organizations 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.

Anti-money laundering: What if you could harness the power of data & advanced analytics?

The legacy systems that many financial services institutions are struggling just to maintain are poised to go through a substantive transformation. At the same time, new technology companies are innovating advanced, cost effective and efficient monitoring systems that will certainly prove disruptive. When will a transformation from standard, mechanical, rules-based systems take place? Who will have the first-mover advantage in streamlining company transaction monitoring systems?

The use of big data can cut through the clutter of existing operational and environmental complexities, but it is clear that a measureable "tipping point" needs to be reached for companies to phase out existing legacy systems and replace them with a tailored, intelligent data-analytics focused approach. However, given the rising costs and effort required to remediate legacy systems to modern Bank Secrecy Act standards, financial services business now have ample reasons to consider big data analytics alternatives.

These big data systems can provide a long list of benefits:

- Cloud-based systems can reduce pre-existing data lineage and degradation issues
- The elimination of data storage and computational processing constraints can enable comprehensive 360-degree entity views and cross-silo activities
- Aggregation of data can enable systems to select and include certain data streams at will (whether transactional or otherwise), and enhanced coverage across products and services
- Enhanced ability to view the data holistically and uncover patterns across jurisdictions, product lines and time periods where none were previously visible
- Modular designs can "right size" systems for company needs and can facilitate customization of logic based on business types (not limited to large financial institutions)
- More sophisticated algorithms that leverage artificial intelligence, machine learning and link analysis can increase efficiencies of detection scenarios, improve effectiveness of alerts and enable the development of newly-discernible data and entity relationships
- Cloud-based systems can be plugged into future multi-bank utilities to leverage everything from common CDD and KYC to actual sharing of select transactions details across several financial institutions
- Global systems can facilitate more effective feedback mechanisms on model productivity and effectiveness, enabling faster, real-time adjustments
- Increased system efficiency will enhance the value and productivity of Suspicious Activity Reports (SARs)

What can you do today to consider these alternatives?

1. Identify which spend components align to Transaction Monitoring Processes
2. Evaluate your AML/CFT spend and compare it to your throughput of SARs to establish a baseline of what you spend on a per SAR and per alert basis
3. Evaluate the age of your systems and versioning of software implementations to better understand when upgrades need to take place
4. Increase your IQ of the competitive vendor landscape, and be informed as to how your current software products compare to other equivalent solutions in the marketplace
5. As you plan for upgrades, consider piloting alternative data analytics processes with new technology in a "sandbox" that can be evaluated side by side with existing product processes
6. Explore tapping into next generation enterprise big data repositories or data lakes being commissioned by chief data officers to incubate AML compliance use cases
7. Develop an adaptation strategy for the medium and long-term

Contributors and Contacts

Survey Team

Didier Lavion
Principal
didier.lavion@pwc.com

Amy Hawkins
Director
amy.hawkins@pwc.com

Pete Zanolin
Director
peter.l.zanolin@pwc.com

Nicholas Holzmacher
Manager
nicholas.d.holzmacher@pwc.com

Lauren Bush
Senior Associate
lauren.r.bush@pwc.com

Lauren Hanat
Senior Associate
lauren.k.hanat@pwc.com

Survey Marketing and Management

Anjali Fehon
US Forensics Strategy Leader
anjali.t.fehon@pwc.com

Kate Glenn
US Forensics Marketing Leader
kate.n.glenn@pwc.com

Ayse Francis
US Forensics Marketing Manager
ayse.m.francis@pwc.com

William Schoeffler
Director
william.l.schoeffler@pwc.com

Forensic Services Contacts

Forensics Services Leadership

Erik Skramstad
US & Asia Pacific Americas (APA) Leader
erik.skramstad@pwc.com

Cybercrime

David Burg
Global Cybersecurity & Privacy Leader
david.b.burg@pwc.com

Sean Joyce
Principal
sean.joyce@pwc.com

Ethics & Compliance

Manny Alas
Partner
manny.a.alas@pwc.com

Glenn Ware
Principal
glenn.ware@pwc.com

Anti-money Laundering

Didier Lavion
Principal
didier.lavion@pwc.com

Brian Castelli
Principal
brian.castelli@pwc.com

www.pwc.com/crimesurvey