Economic crime: a threat to business processes

45%
of U.S. organizations suffered from economic crime in the past two years.

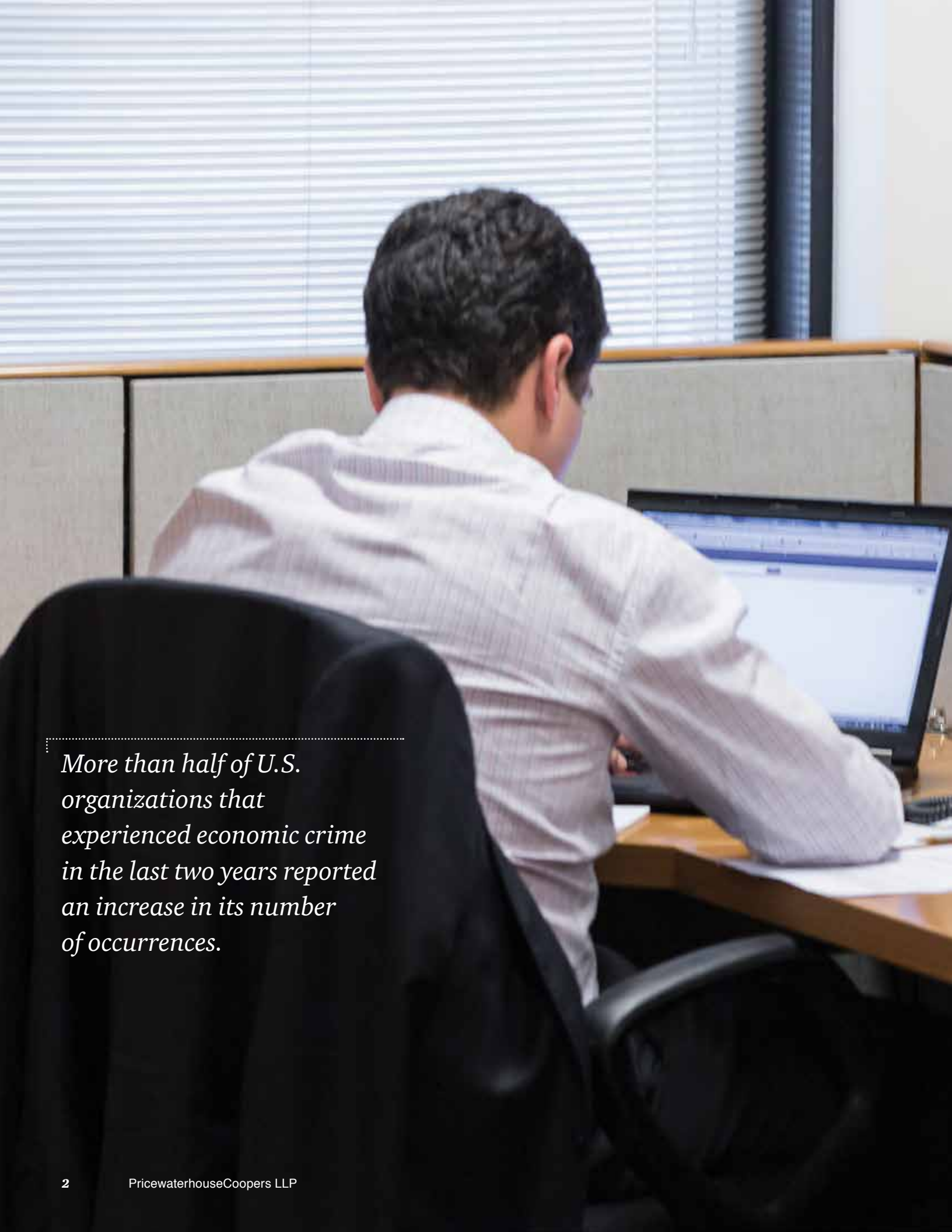
67%
of U.S. organizations currently have or planned to have operations in high-risk markets.

71%
of U.S. respondents perceived an increased risk of cybercrime over the past 24 months.

pwc

Economic crime continues to remain in the forefront of corporate concern, posing a threat to fundamental business processes.

Contents



More than half of U.S. organizations that experienced economic crime in the last two years reported an increase in its number of occurrences.

Foreword
by Sean Joyce

In 2014, the threat posed by economic crime is fresh in our collective memory as we work to recover from a financial meltdown and near economic collapse caused by fraudulent practices in our financial markets. While important strides have been made in recent years, economic crime continues to pose a grave threat to financial interests in the United States as a whole, and to US businesses both at home and abroad. Economic crime is an ever evolving threat, and new criminal trends relentlessly emerge in different sectors and industries as economic events, natural disasters, and innovation re-shape our world.

Economic crime has become a truly borderless threat

The very technology that binds our global economy and facilitates international commerce has created ample opportunities for abuse. Once-novel threats like cyber-attacks are no longer confined to obscure hacker groups operating in the shadows of our economy; but have become a key weapon in the arsenal of common criminals, organized crime rings, and foreign nation-states. Many companies do not appreciate the gravity of the threats they are facing. Many businesses are often unaware that their systems have been probed or penetrated by criminal elements, let alone the implications these security breaches could have on their business activities. Corporate management must increasingly confront a difficult question—how do you protect yourself when you do not even know you are under attack?

Foreign states have also recognized the potential value of cybercrime, and now routinely support efforts to exploit vulnerable networks to steal cutting-edge technology from US companies. Billions of dollars in investment and R&D can be lost in a matter of minutes. With many US companies at the forefront of innovation, we can expect cyber-attacks and related schemes to increase in frequency and magnitude, resulting in substantial intellectual property, trademark, and patent violations in the coming years.

Technology has allowed criminal elements to extend their reach across national boundaries, vastly expanding their pool of potential victims. Securities fraud schemes originating from countries such as Thailand, Spain and Canada can now target vulnerable investors across the globe, including the United States. The promise of the global economy has been distorted to trick unsophisticated investors into purchasing worthless penny stocks or investing in phantom infrastructure projects in foreign countries. Oftentimes the victims of these crimes represent the most vulnerable sectors of our economy—the elderly, the ill-informed, and those most in need of financial good fortune.

Tending our backyard

The United States has proved to be fertile ground for domestic economic crime in recent years. Catastrophic coastal events on the Eastern and Gulf coasts have generated rampant insurance fraud that squanders taxpayer dollars and undermines community relief and reconstruction efforts. Farther inland, natural gas exploration and fracking have led to boom towns sprouting overnight in places like North Dakota, Wyoming, Utah, and Texas. Many of these towns do not have the infrastructure or governance capability to handle the influx of people, and crime, that inevitably accompany boom-town dynamics. Land lease and mineral rights agreements, zoning ordinances, permits, and licenses have become particularly vulnerable to exploitation.

While certain vulnerabilities in the domestic banking sector, such as bank fraud and loan origination fraud has decreased with improved due diligence, criminals have adjusted their tactics to exploit new weaknesses. Loan modification schemes have become increasingly prevalent, including foreclosure rescue and “own your own home” scams that target unsuspecting American consumers. Once again, it is often the most vulnerable segments of our population that suffer the most severe consequences.

These examples demonstrate that economic crime is a dynamic threat to businesses and consumers alike; and requires a nimble and varied response. For businesses in particular these threats require a second look at many aspects of operations—from the beginning of the supply chain to the consumer. How you sell, who you accept as a vendor, who you partner with in foreign markets, how your HR processes like recruiting and training work—are just some of the fundamental business activities that are threatened by economic crime. We hope that the following report will provide valuable insight to help stakeholders in the private and public sector improve their response to this ever-evolving threat.

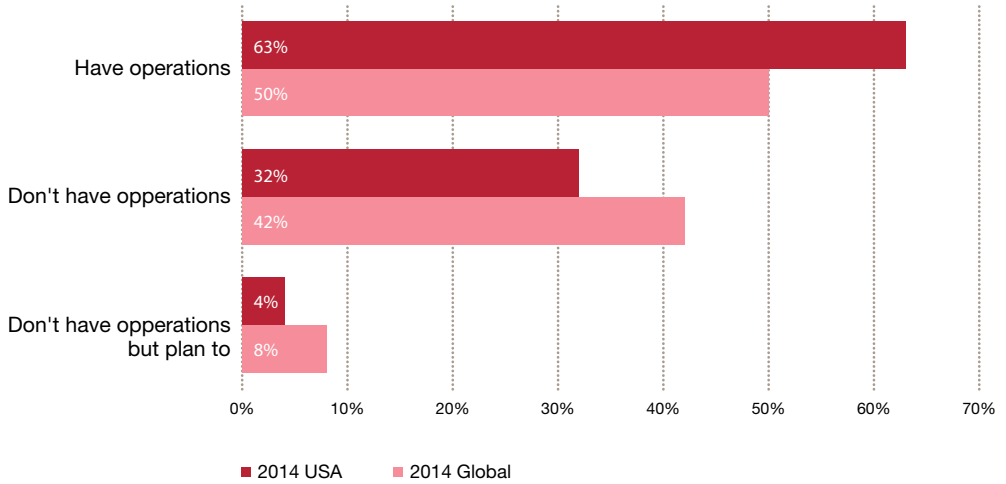
Although US organizations are more likely to have operations and pursue opportunities in high risk markets, they experience less corruption than their global peers.

A global landscape, a global outlook

We are pleased to present the US Supplement to the 2014 Global Economic Crime Survey (GECS). This year's GECS features the perspectives of more than 5,000 respondents from over 100 countries on the prevalence and direction of economic crime. The US Supplement provides an in-depth discussion of the issues facing US-based respondents who participated in the GECS. We will focus on how the perception, incidence, and impact of economic crime changed since our 2011 survey, or differed from global patterns. We will also identify situations that encourage fraud's occurrence and provide methods and strategies to avoid, detect, and mitigate economic crime.

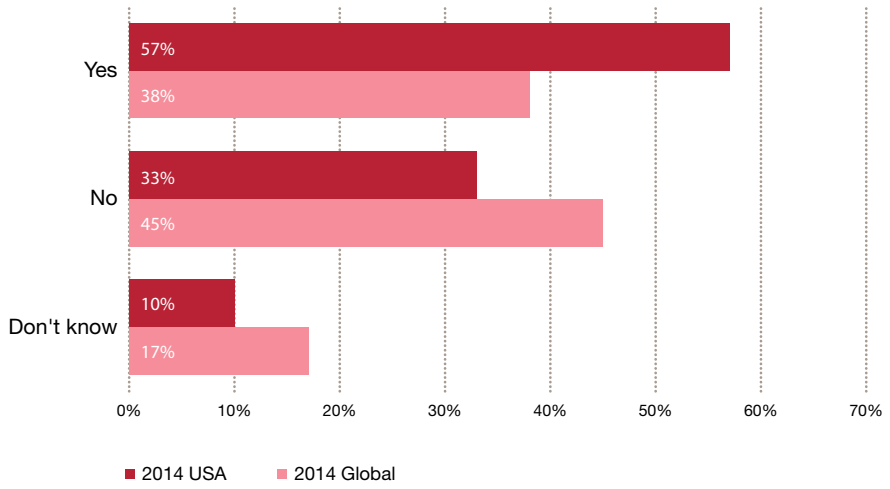
The US respondents' operations differ from those of their global peers in key ways. As in 2011, our US participants reported a larger global footprint, with 80% noting worldwide operations compared to 61% globally. US organizations were also more likely to both have operations and pursue opportunities in markets with high-levels of corruption risk [1] (Figures 1 and 2, respectively). Sixty-seven percent of US respondents indicated their organizations currently have or planned to have operations in high-risk markets, compared to only 58% of global respondents. And 57% of US respondents (versus 38% globally) indicated their organizations pursued opportunities in markets with high-levels of corruption risk within the past 24 months. One reason that so many companies are doing business in high-risk markets is that the economic downturn has pushed businesses to turn their attention to developing markets in order to drive revenue growth. In addition to market opportunity, many developing markets are more likely to present elevated corruption risk.

Figure 1: High level corruption markets



1 Defined as a territory with a Transparency International Corruption Perception Index ("CPI") score of 50 or less.

Figure 2: US organizations pursuing opportunities in market with a high level of corruption risk

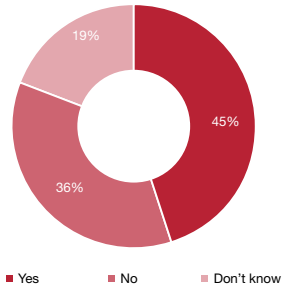


US companies are growing their international operations, and the expanding role of the internet and mobile technology in business can bring risk from beyond their geographic footprint. US employees are equipped with "smart" mobile technology, tablets and laptops which allow for business to be conducted anywhere, anytime. Thus, companies are operating in a "borderless" society in which they may not need to have a bricks-and-mortar operation in a given country to have a presence and possible risk. Additionally, companies may engage sales agents, distributors, consultants and other service providers to drive sales and business operations, which may expose companies to increased risks including corruption, cybercrime, and economic sanctions.

Our 2014 US CEO Survey reveals that executives are seeking more strategic alliances in 2014: 42% plan to enter one this year; only 4% expect they'll exit an existing relationship. They are also planning acquisitions: 39% of US CEOs plan to complete a domestic acquisition this year and 28% are planning on a cross-border deal. As we will see, US respondents are aware of the dangers some third party relationships can present. Whether a company is planning to acquire, partner with or do business through another entity, proper due diligence can help identify and quantify their problems before they become your problems.

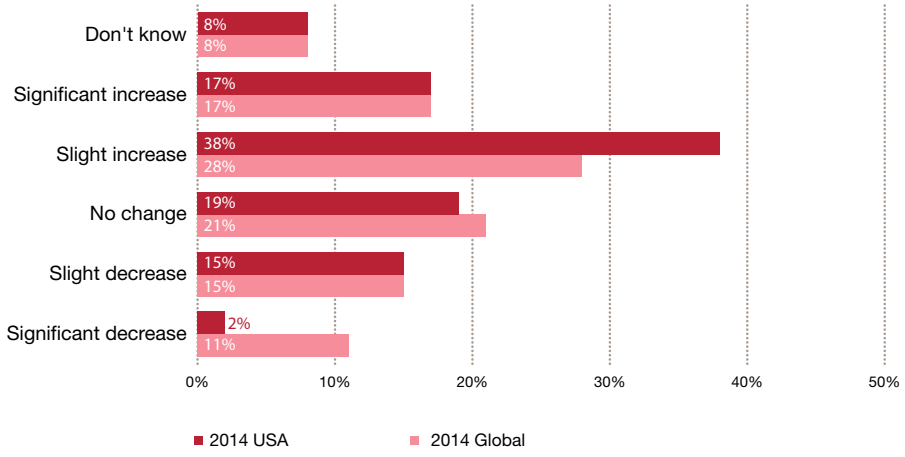
Economic crime remains in the headlines

Figure 3: U.S. Organizations reporting incidents of economic crime



The investigation and prosecution of economic crime, particularly in the wake of the financial crisis, remain at the forefront of public concern. In our 2011 report, we discussed that the additional public scrutiny involving recent high-profile investigations and prosecutions may have heightened the awareness of fraud within organizations, resulting in more organizations reporting fraud (45% in 2011 compared to 35% in 2009). Our 2014 survey results support this idea. As the US economy recovers from the financial crisis, the number of organizations that reported suffering from fraud levelled off at 45% during the survey period (Figure 3).[2] However, over half of respondents who indicated their organizations did suffer fraud reported an increase in the number of occurrences (56%), representing a continuing upward trend in the occurrence and detection of economic crime (Figure 4).

Figure 4: Perceived changes in the number of occurrences of economic crime



2 A note about comparative data: In our 2011 survey, respondents were asked to consider the previous 12-month period. In 2014, to align with the bi-annual nature of the survey, we asked respondents to consider the previous 24 months. While we make no comparisons here involving absolute numbers, readers should take into account the longer analytical timespan of the 2014 survey data in assessing trends.

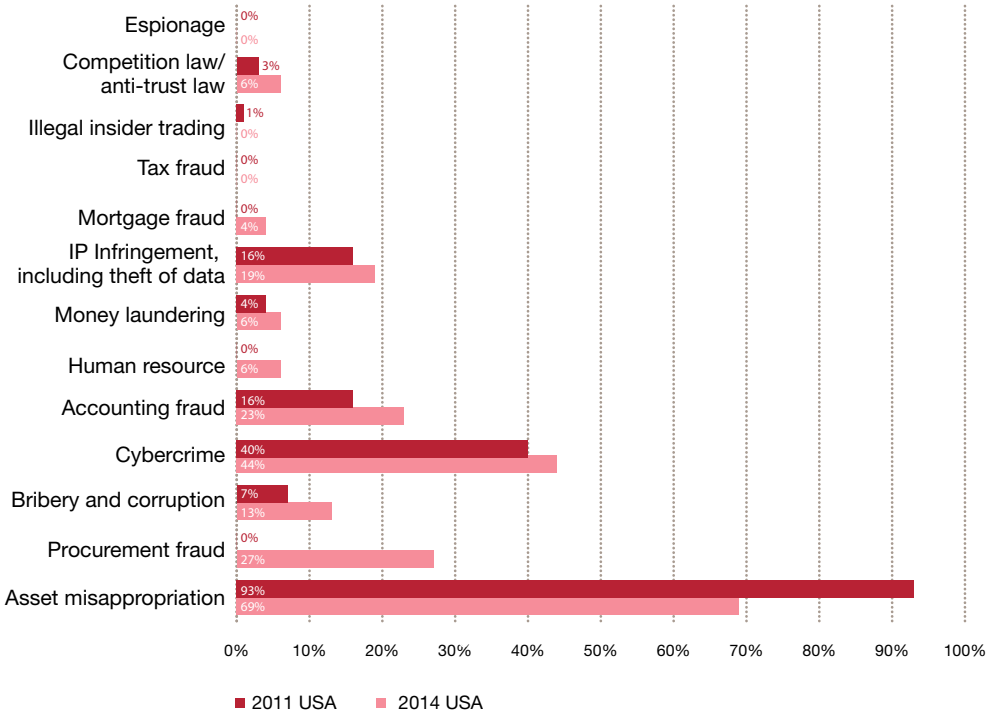
Incidents of asset misappropriation plummeted by 24% during the survey period, and are now in line with the global average (69%).

Charting the landscape of economic crime

The survey results reflect a significant shift in the types of crime suffered by organizations. The distinctions among types of fraud reported by organizations decreased during the survey period, reflecting that organizations are more likely to suffer from a range of economic crimes rather than from one or two discrete types.

As shown in Figure 5, we asked organizations about the types of fraud they experienced. This year, we refined this question by adding three new classifications of economic crime—procurement fraud, human resources fraud, and mortgage fraud. Despite the addition of these new categories, US organizations reported that they experienced increased levels of fraud across all types of economic crime since 2011, except for asset misappropriation and insider trading.

Figure 5: Types of fraud



While asset misappropriation remains the most common fraud US organizations suffered, it plummeted from 93% in 2011 to 69% during the survey period. Incidents of asset misappropriation suffered by US respondents are now in line with those reported globally (also at 69%). However, organizations shouldn't downplay its risks, prevalence or likelihood of occurring.

It is unlikely the decrease in asset misappropriation is due to respondents selecting mortgage fraud since these types of fraud are dissimilar and unlikely to be confused. However, it may be possible that some of the decrease is related to adding human resources fraud and, to a lesser extent, procurement fraud in the survey. Additionally, asset misappropriation may be most directly tied to economic pressures from the global recession, and the decrease in reported instances may partially be explained by an improving economy.

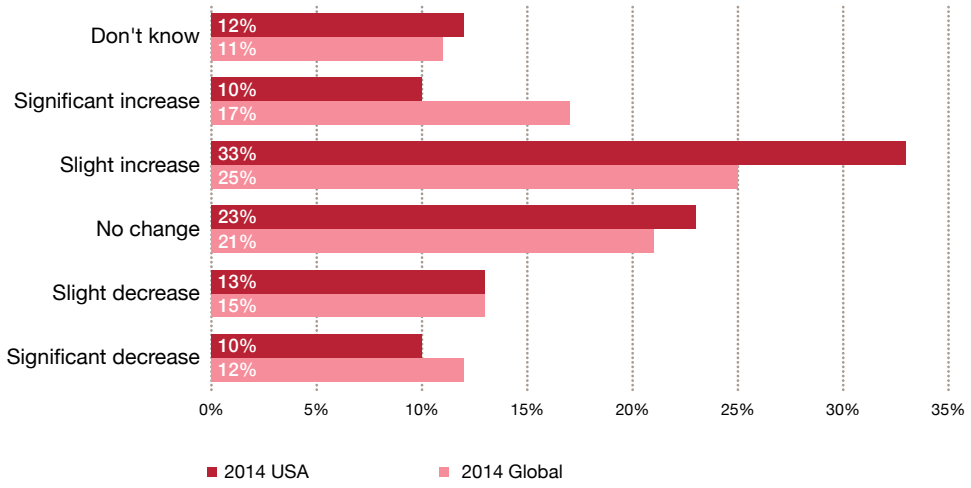
Two types of fraud—accounting fraud and bribery & corruption—made comebacks in 2014. In our 2011 report, we anticipated that these types of fraud would grow in the next few years in the wake of more regulation, stricter enforcement, and increasing investigations. In this survey period, accounting fraud at US businesses essentially rebounded to 2009 levels (23% in 2014 vs. 24% in 2009), after experiencing a drop to 16% in 2011. Similarly, bribery & corruption at 14% doubled from 2011 levels (7%) after dropping by more than a half since 2009 (16%). The increase in accounting fraud and bribery & corruption may be attributable in part to more companies implementing or enhancing internal controls, more robust compliance programs and increased risk assessments, thus leading to more frauds being detected.

Similar to 2011, no US respondents reported suffering from tax fraud or espionage in the survey period and, as previously mentioned, reports of illegal insider trading fell from 1%. Yet companies should remain vigilant; much like lightning, the chances these crimes may affect a business are statistically remote, but they can be potentially devastating should they strike.

What's the bottom line?

The reality of fraud is that it can be as impactful to a company's revenues as other business and market forces. The abilities to prevent, detect and swiftly respond to fraud can be powerful cost-savings tools. The survey revealed that 54% of US respondents reported their companies experienced fraud in excess of $100,000 with 8% reporting fraud in excess of $5 million. Sixty-six percent of the respondents indicated the financial impact of economic crime on their organization remained the same or increased over the past 24 months, compared to only 23% who indicated a decrease (Figure 6). As discussed in further detail later in the report, the statistics support that executing stronger fraud prevention and detection measures could lead to a reduction in fraud and its financial cost. By implementing more robust anti-fraud controls, organizations can prevent losses and increase savings and profitability.

Figure 6: Perceived changes in cost of fraud



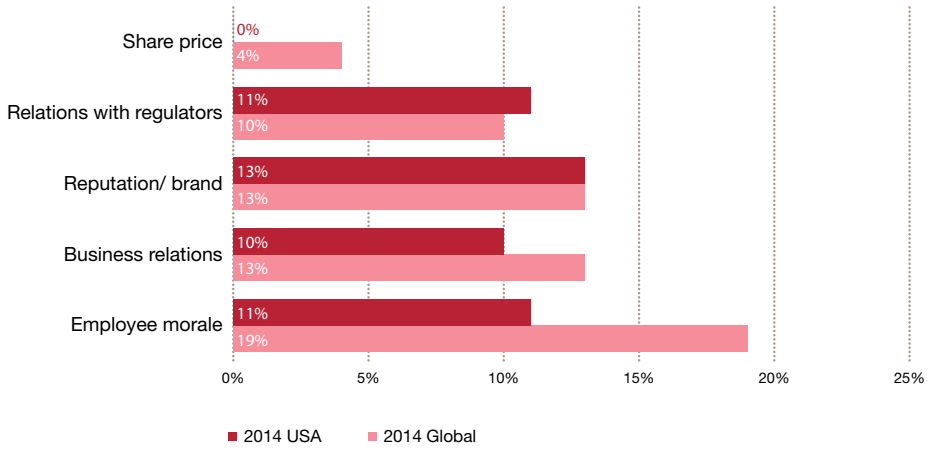
The Department of Justice (DOJ) and Securities Exchange Commission (SEC) both consider a company's existing compliance program and cooperation in determining how to resolve investigations. Having a robust compliance and ethics program, self-reporting, providing full cooperation and accepting responsibility often lead to reductions in an organization's culpability score, possibly reducing fines and penalties. Conversely, unreasonable delays reporting the offense could lead to an increase in a company's culpability score, and the corresponding fine imposed. Companies have the ability to directly influence the cost of fraud by implementing an effective and updated corporate compliance program, and conducting comprehensive internal investigations once wrongdoing is uncovered.

Collateral damage

The effects of fraud cannot be completely measured in dollars alone. In fact, economic crime may have a more damaging effect on intangibles such as brand, reputation, and employee morale than on the immediate bottom line. Ultimately, this collateral damage may impact revenue, earnings and growth years after the crime has been uncovered.

The survey reflects that companies are recognizing the threat of indirect damage. US respondents indicated that the indirect impact of fraud across all categories increased from 2011, with the exception of relations with regulators which experienced a small 1% decline from 2011 (Figure 7).

Figure 7: Impact of fraud



The reality is clear—organizations recognize that rebuilding employee morale, customer goodwill and brand loyalty, and re-establishing trust with business partners and regulators ultimately impact profitability, even if these factors don't appear on organizations' balance sheets or income statements. These kinds of losses, while difficult to quantify in financial terms, can be more significant and longer-lasting than the initial financial impact of fraud, and they can be harder to control. In today's highly connected world where the internet, social media and 24/7 news channels drive the news cycle, it is increasingly difficult for organizations to control the message when bad news occurs. The good news is that companies often emerge stronger and more resilient by building a strong compliance and threat management system, recapturing market share lost as a result of crisis. Often, a thorough review of the compliance environment identifies ways that an organization can improve transparency and the flow of information connected to its business processes, providing benefit and efficiencies to the entire company.

Go to battle against fraud (because your business processes are under attack)

Not only does economic crime expose companies to regulatory and legal peril and monetary loss, but it can also strike at a company's strategic business goals and objectives. For instance, bribery and bid rigging can not only lead to inflated costs, arrest and eroded business relationships, but can also lead to substandard safety. In addition, accounting and tax fraud can not only mask larceny, but can also disrupt the free flow of vital information needed to make strategic business decisions; such as in merger and acquisition deals where misrepresented and falsified financial information can impact a potential acquirer's valuation of a target company. Cybercrime and data theft not only compromise customer data and critical company information, but also may disrupt the confidence a company places in its otherwise innovative IT strategy, hurt its goodwill with customers and can lead to expensive remediation costs when an attack does occur.

Every business unit has a stake in minimizing the company's exposure to economic crime. What this means is that responsibility for fraud control and prevention belongs to everyone in an organization, not just its legal or compliance functions. Additionally, those on the front lines such as controllers, IT technicians and salespeople are the company's "eyes and ears" and are also most likely to be the first responders in the wake of a crisis. Treating economic crime as a business concept, and integrating prevention into business strategies, can maximize compliance and detection and help ensure that a company will remain vigilant on all fronts.

The perils of economic crime

Fraud and economic crime can cause financial harm, but sometimes it can endanger employee and public health. Shortcuts and inferior product substitution can affect the structural stability of construction projects. Bid rigging and kickbacks can lead to the selection of substandard contractors or unskilled labor. Environmental crimes can often be traced back to efforts to cut costs or extract revenue. Product substitution or counterfeiting can impact automobile and aircraft safety. Pharmaceutical crime is growing according to Interpol, and counterfeit medication puts lives at risk. Disruption to municipal computer systems by cyber criminals or hacktivists can compromise public security systems. Lead contamination and food borne illnesses can result from supply chain fraud or negligence.

Macro trend: urbanization

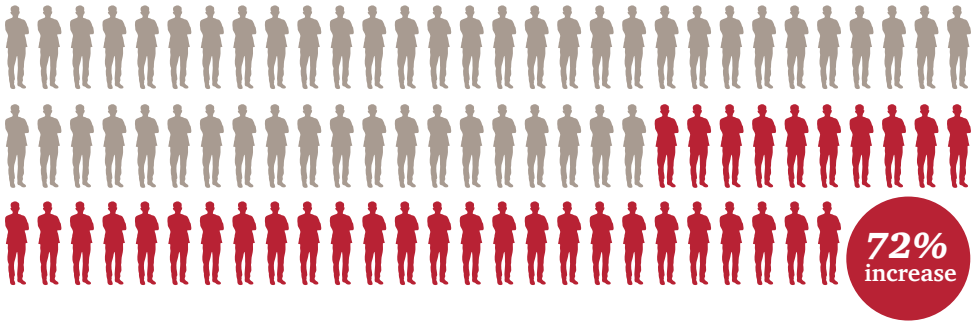
"The 19th century was a century of empires, 20th century was a century of nations and 21st century will be a century of cities."

—Wellington E. Webb, former mayor of Denver.

As we continue to move closer together, cities create opportunities for greater connectivity, culture, innovation, productivity and energy efficiency. However, as cities grow and change, they may have an effect on the economic crime landscape.

The demand for infrastructure as well as residential and commercial construction will increase; however those projects often bring high levels of interaction with government officials, heavy reliance on third parties and an industry (Construction & Engineering) with historically high corruption risk. Companies and municipalities alike should ensure they have adequate safeguards in place to prevent and detect such crimes as bribery, bid rigging, kickbacks and contract fraud.

World urban population



The world urban population is expected to increase by 72% by 2050

Source: World Urbanization Prospects: 2011 Revision, produced by the UN Department of Economic and Social Affairs

Cybercrime is here to stay

Our 2011 survey focused on the increasing prevalence of cybercrime—and the 2014 results confirmed this trend. Forty-four percent of US organizations that suffered from economic crime in the past 24 months identified cybercrime as one of the frauds experienced, while 44% of all US organizations indicated they thought it was likely they would suffer from cybercrime within the next 24 months.

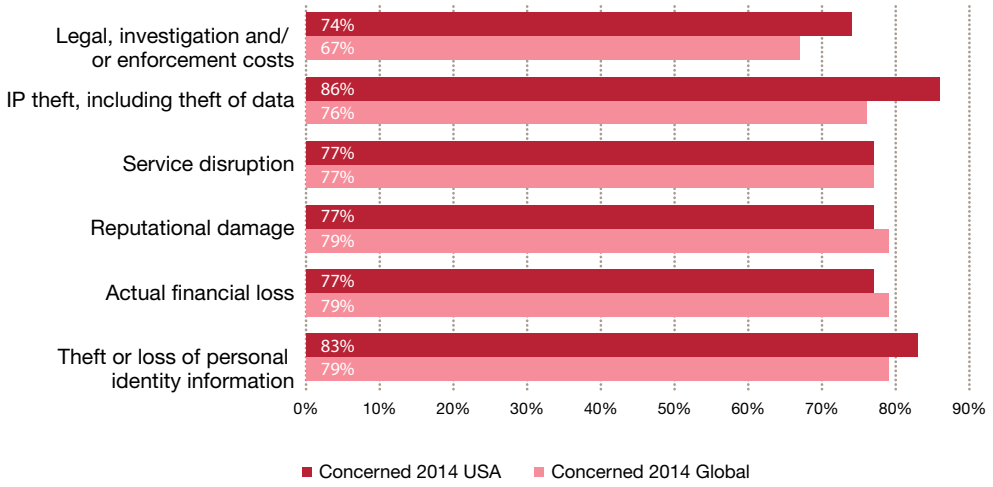
The Internet has changed the way the marketplace operates since virtually all organizations somehow rely on it to conduct business. Additionally, more business processes are automated and more customer and proprietary data are available in digital form. Mobile technology has become an accepted medium for commerce. More organizations and consumers rely on cloud computing and storage for both internal processes and customer data, a trend that will continue to increase over time. It is not surprising that cybercrime has moved to the forefront of companies' concerns. Companies are beginning to change how they think about cybersecurity—viewing it as a business issue, not just an IT issue:

- Seventy-one percent of US respondents indicated their perception of the risks of cybercrime increased over the past 24 months, rising 10% from 2011.
- US respondents' perception of the risks of cybercrime exceeded the global average by 23%.
- US respondents still perceive the greatest cybercrime threat coming exclusively from the external cybercriminal. However, this trend is shifting from 2011 and the internal cybercriminal is closing the margin.
- Compared to their global counterparts, US organizations lost more through cybercrime in financial terms: 7% of US organizations lost $1 million or more, compared to 3% of global organizations; 19% of US organizations lost $50,000 to $1 million, compared to 8% of global respondents.
- Despite having more to lose, US respondents were generally less aware of the cost of cybercrime: 42% of US respondents were unaware of cybercrime's cost to their organizations, compared to 33% of global respondents.

Cybercrime: Respondents believe the greatest threats to be theft or loss of IP, data or personal identity information.

More organizations are collecting and maintaining personal and financial data on their customers (real and potential) and employees (past, present, and prospective). Data mining allows companies to gain better insight to their customer's spending habits in order to better inform marketing and other business strategies; however, data mining can pose a cybersecurity threat as it has been a prime target of hackers, as evidenced by multiple major personal data breaches recently in the headlines. Similarly, governments are engaging in both intra-border and cross-border cyber-surveillance programs. It's not surprising, therefore, that our respondents were most concerned about the risks of cybercrime directed at their data processing and storage systems: 86% of US respondents were concerned with cybercrime allowing intellectual property (IP) infringement, including theft of data; 83% were concerned with it leading to theft or loss of personal identity information (Figure 8). Given this trend along with a myriad of cyber incidents making the headlines, many governments are debating data-center localization strategies along with internet framework bills.

Figure 8: Threats of cybercrime



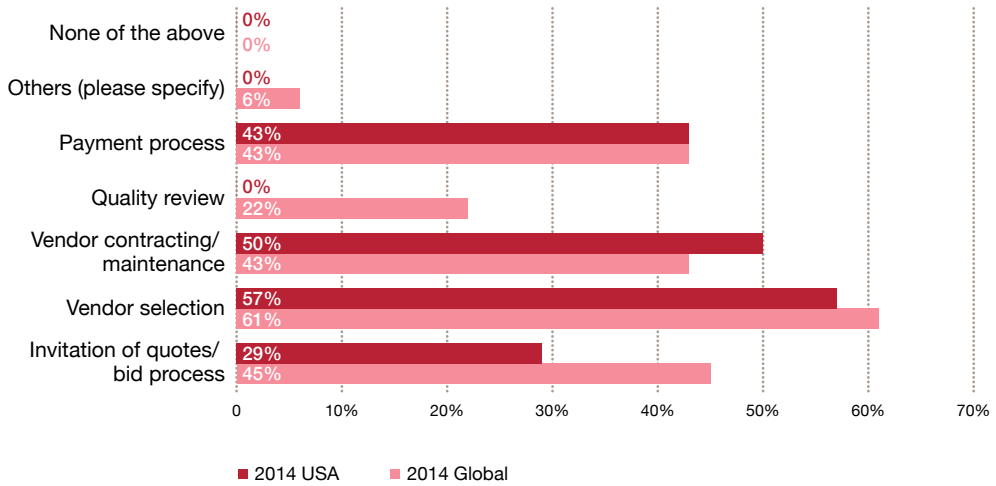
Today's circumstances and risks mean that both companies and governments should walk the fine line between enhanced security and protecting their own economic interests within the country. Critical cyber data is valuable and appealing to organized criminal enterprises for economic gain, to nation states for political espionage, to competitors for a business advantage, and to the rogue individual for purported social motivations. Social collaboration, expanding use of mobile devices, moving information storage to the cloud, digitizing sensitive information, moving to smart grid technologies, and embracing workforce mobility alternatives expose companies to fraud and also provide opportunities to strengthen their cybersecurity profiles. Thus, US corporations need to better leverage and implement the computational and analytical power of cybersecurity technologies to help combat the increasing global presence of cybercrime. US business leaders seem to understand the threat: our 2014 US CEO Survey shows that respondents were more concerned about cyber threats (including the lack of data security) and the speed of technological change than their global peers. Technological advances do not just present challenges- they can bring opportunities to better protect organizations from fraud. The upside is that technology may allow companies to better monitor their processes and implement real time controls. Automation, dashboard compliance strategies and improved inventory controls are all tools which companies can use to safeguard their assets, information and brands.

Procurement fraud

As previously noted, for the first time we specifically asked respondents about procurement fraud—illegal conduct by which the offender gains an advantage, avoids an obligation, or causes damage to his organization. The results were stark—more than 1/4 of US respondents reported suffering from procurement fraud (27%), thus immediately placing it as the third most frequent type of fraud experienced by US organizations. The US results regarding procurement fraud generally mirrored the global average of 29% of organizations reporting they experienced procurement fraud within the past 24 months.

The high response-rate in connection with procurement fraud reflects the increasing interconnectedness of companies and ongoing trend toward outsourcing more aspects of their businesses. Organizations are especially vulnerable to procurement fraud when their purchasing, supply, and payment processes are susceptible to circumvention. In order to remain economically competitive, companies are often forced to lengthen their supply chain and rely heavily on the manufacturing of their goods outside of their own countries to capture the benefits of cheaper labor. This further complicates matters as the compliance function must now expand into sometimes unchartered foreign territories, thus enabling more opportunity for procurement fraud in various forms. Economic pressures set by headquarters can sometimes lead to unintended consequences of procurement fraud.

Figure 9: Where did the procurement fraud primarily occur



Most procurement fraud occurred at the vendor level, whereby key stakeholders in the procurement sometimes influence vendor selection or maintenance through bribery, rigged bids and kickback schemes. Procurement fraud during the payment process occurred in almost half of the instances, both in the US and globally (43% each). These statistics support the need for organizations to engage in robust vendor due diligence before pursuing outside business opportunities and partnerships. Clearly, companies that have existing robust global compliance programs that are scalable are better adapted to procuring goods and services in new territories. Often is the case that the companies that have not previously operated in foreign high risk territories fall victim to these schemes. But sometimes, compliance failures can lead to reputational damage when contracting with third parties that themselves commit procurement fraud, often unbeknownst to the company. These frauds can lead to reputational damage by association. Companies must remain vigilant regarding who they do business with, both on the inside and the outside.

Procurement fraud

A few of the mechanisms by which procurement fraud can occur:

Bid Rigging: Fraud that impedes competitive bidding and disallows free and open competition in order to obtain the best goods and services at the lowest price.

Kickbacks: Any money, fee, commission, credit, gift, gratuity, any item of value, or compensation of any kind that is provided, directly or indirectly, in exchange for preferential treatment.

Bribery: The offering, giving, receiving, or soliciting of any thing of value to influence action as official or in discharge of legal or public duty.

Collusion: The secret combination, conspiracy, or concert of action between two or more persons for fraudulent or deceitful purpose.

Source: US General Services Administration Office of Inspector General

Bribery and corruption is on the rebound

Although only 14% of US respondents suffered from bribery & corruption, organizations shouldn't downplay its risks, prevalence, or likelihood of occurrence. In our 2011 report, we anticipated that reported bribery & corruption would grow in the next few years in the wake of growing global regulation and increasing investigations uncovering more instances of corruption. In fact, 14% of organizations that experienced economic crime within the past 24 months identified bribery & corruption as a type of fraud suffered (doubling from 2011 level of 7%).

Bribery & corruption persists despite efforts of US organizations, law enforcement and regulators, and antifraud practitioners:

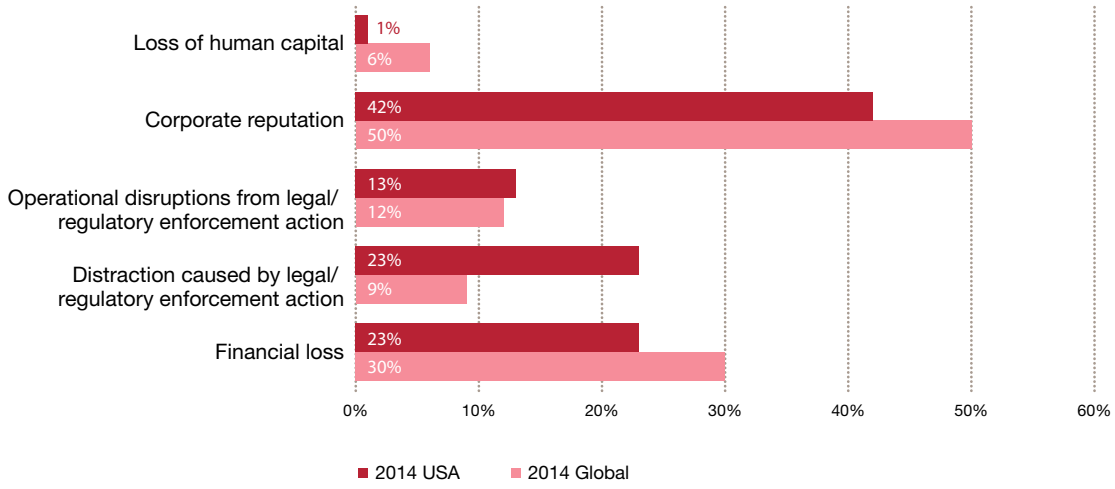
- US and global organizations experienced similar financial losses[3] through bribery & corruption: 4% of US organizations lost $1 million or more, compared to 5% of global organizations; and 28% of US organizations lost $50,000 to $1 million, compared to 27% of global respondents. US and global respondents were also similarly unaware of the cost of bribery & corruption on their organizations: 36% of US respondents were unaware of the cost, compared to 34% of global respondents.
- US respondents were more likely than their global counterparts to report that bribery & corruption presented a higher risk than money laundering and anti-competitive practices: 58% of US respondents indicated bribery & corruption posed the highest risk compared with 53% of global respondents; 26% of US respondents indicated anti-competitive practices posed the highest risk, compared with 21% of global respondents; and 10% of US respondents indicated money laundering posed the highest risk, compared with 22% of global respondents.
- Seventeen percent of both US and global respondents reported their organization had been asked to pay a bribe within the past 24 months; in addition, 15% of US respondents reported their organization lost an opportunity to a competitor they believed paid a bribe, compared with 22% of global respondents.

The risk of bribery & corruption grows as US organizations increasingly operate in and pursue opportunities in high-risk markets. Organizations are doing more business with and in territories that have cultures and histories relatively more tolerant of bribery & corruption, and officials who may be predisposed to expect payment of bribes. Bribery & corruption attacks the sales and marketing processes – and while the risk of bribery & corruption exists in most transactions, it is of particular concern when dealing with government officials in emerging markets.

As US organizations extract themselves from the economic crisis and vie for global competitive advantage and increased market share, sales and marketing staffs often experience increased pressure to deliver higher sales and drive profitability. This can make them particularly susceptible to offering bribes or kickbacks, or otherwise rigging the sales process. US organizations are taking note – 42% of respondents perceived that bribery & corruption had the most severe impact on corporate reputation, whereas 23% of respondents perceived it had the most severe impact on financial loss and distraction caused by legal/regulatory enforcement (Figure 10).

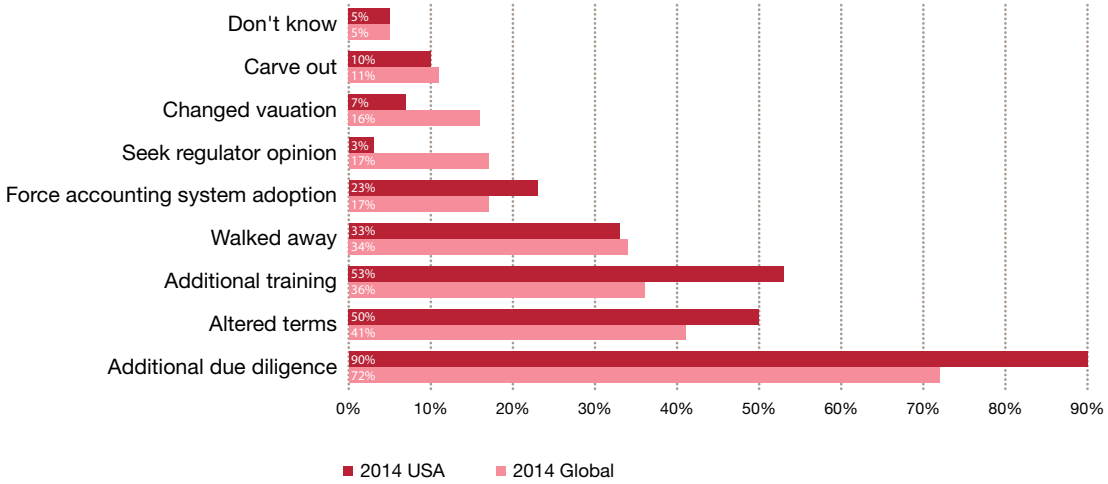
3 The GECS—US Supplement defined "financial loss" as including both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to "loss of business opportunity".

Figure 10: Perceived threat of corruption



Bribery & corruption also impacts the way US organizations pursue business opportunities. In pursuing opportunities in high-risk markets, US organizations altered their business plans or strategies more often than the global average (46% US, 39% Global), and engaged in disparate methods of altering their business plans or strategies (Figure 11).

Figure 11: Method of alteration of business plan or stratagy



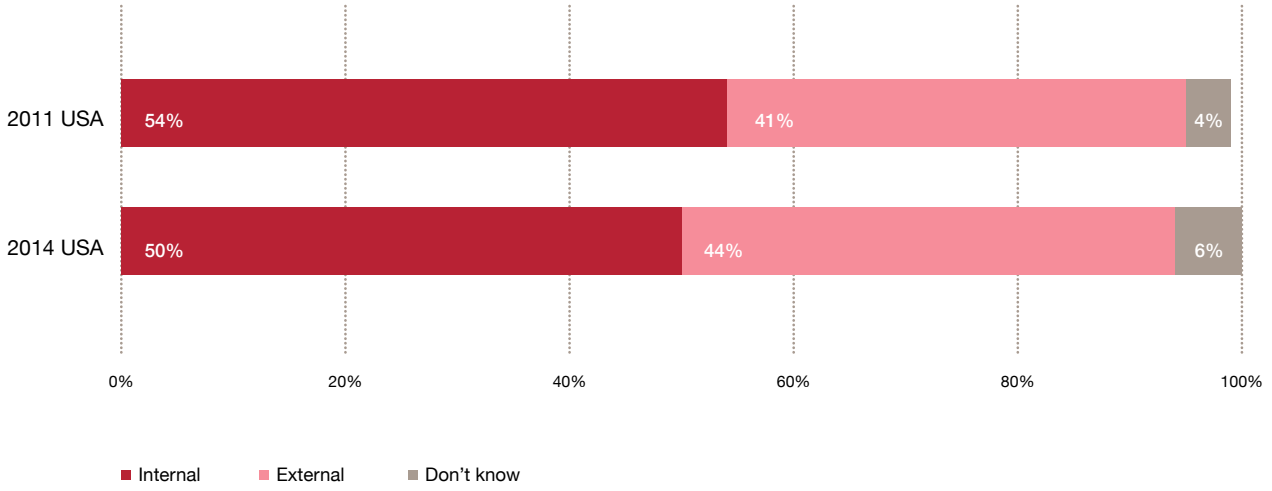
More than 1/3 of US organizations walked away from potential opportunities when doing business in high-risk markets, losing out on immeasurable benefits. The numbers don't necessarily need to be that high. Many situations can be remediated and a company with a strong, robust compliance system already in place will find it easier to understand the scope of potential corruption risk and navigate through it successfully. Luckily, US companies understand the benefit of having a robust compliance program and are outperforming their global peers (US 90% vs Global 72%) in terms of performing additional due diligence. By increasing additional due diligence in M&A deals, companies can promptly identify, understand and minimize the risks of a potential walk away late in the deal process which could prove costly. It appears that a benefit of US companies doing more global business, in riskier areas, than their global peers may cause them to adopt stronger compliance programs. This can be a competitive advantage that allows US companies to move more quickly and with better confidence in identifying business opportunities.

The good news is U.S. organizations are out-pacing their global counterparts in performing additional due diligence.

Profile of the perp

Our survey results reflect that the "external enemy" is almost as likely as the "internal enemy" to commit fraud. Although US respondents reported that the most serious economic crime experienced within the past 24 months was more likely committed by an internal actor (50%) than an external actor (44%), the external fraudster is closing the gap (Figure 12).

Figure 12: Main perpetrator of fraud



This trend is consistent with more organizations pursuing and engaging in business opportunities in high-risk markets. Additionally, as organizations rely more on technology, they increasingly do business in a "borderless economy" where they are more susceptible to threats from all sides. The results are clear – while companies certainly should not lose sight of the internal perpetrator of fraud, they need to remain wary of the external perpetrator.

We asked respondents what factor they felt contributed most to the economic crimes committed by internal actors. Using the common "fraud triangle" model, respondents could choose from ability/opportunity, rationalization, and incentive/pressure to commit fraud. Organizations have limited ability to implement controls that reduce incentives and pressures to commit fraud or the perpetrators' ability to rationalize their actions since these factors are more likely "personal" to the

perpetrator. However, organizations do have the power to take away the opportunity and ability to commit fraud by introducing and implementing tougher internal controls. The responses reflect that organizations are losing out on their potential to effectively mitigate fraud committed by internal actors. At 73%, US respondents indicated that ability/opportunity far outpaced rationalization (at 15%) and incentive /pressure as a factor to commit fraud (at 12%)(Figure 13).

Figure 13: Factors of fraud

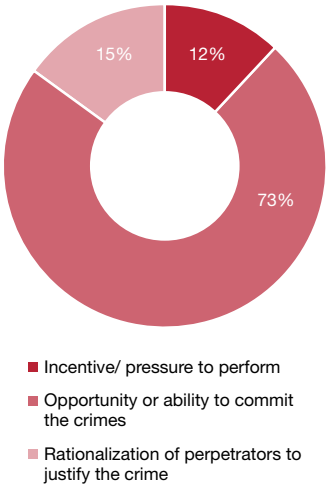
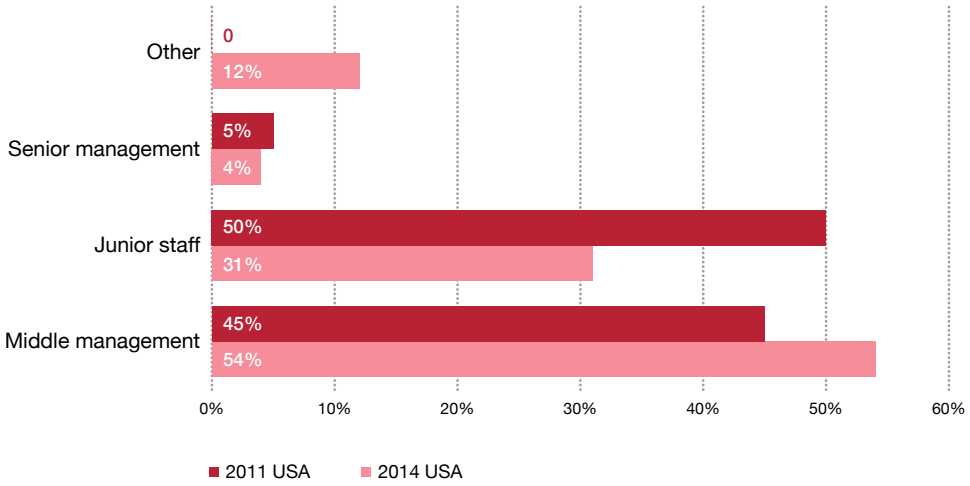


Figure 14: Main perpetrator of internal fraud



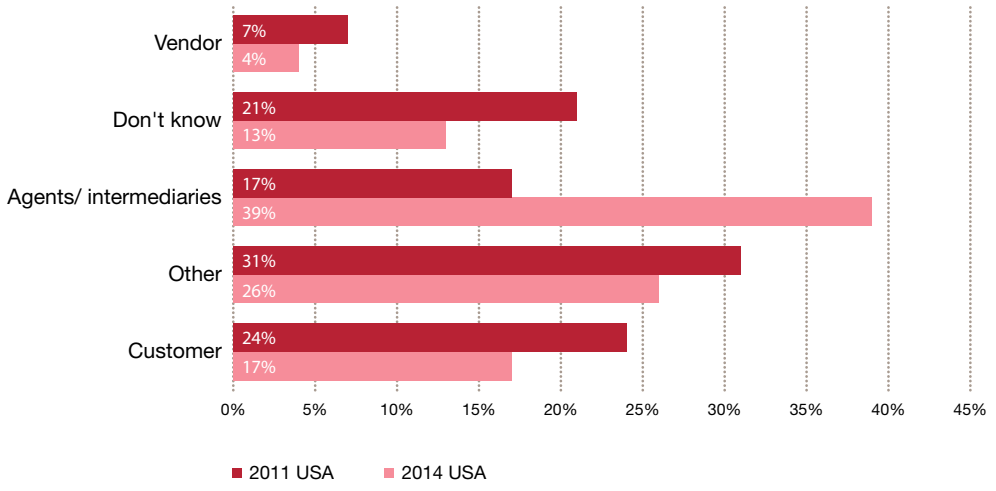
As shown in Figure 14, the US survey results also reflect a sharp rise in internal fraud committed by middle management (54%) compared to junior staff (31%). Economic downturns often disproportionately affect new employees and lower paid personnel, causing increased financial pressures which may contribute to the incentives to commit fraud; as we experience an economic recovery, the financial pressures on junior staff may decrease, and thus the incentives for fraud. Middle management overtaking junior staff as the main perpetrators of reported fraud may correlate with the respondents' indication that ability/opportunity is the leading factor contributing to economic crime.

Common profile characteristics of internal fraudsters

Both US and global respondents most frequently identified the following characteristics of internal fraudsters:

- Gender: Male (77% US, 77% Global)
- Age: 31 to 40 years old (39% US, 40% Global)
- Length of Service: Employed between three and five years (27% US, 29% Global)
- Education: College degree (35% US, 35% Global)

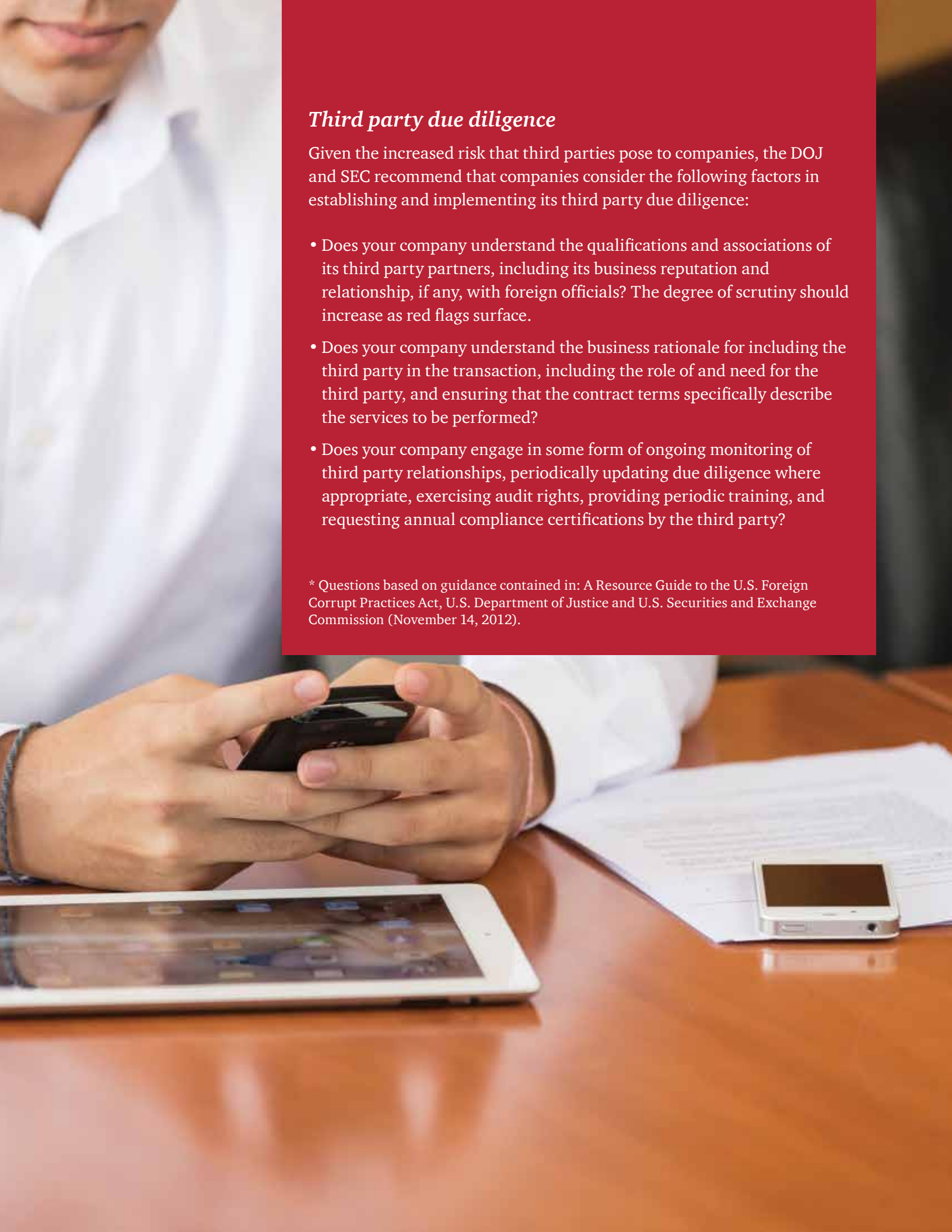
Figure 15: Main perpetrator of external fraud



Meanwhile, fraud committed by US senior management remained relatively low at 4% (up from 3% in 2011) compared to the global average where 20% of respondents cited senior management as the main perpetrator of internal fraud. This finding could be related to the relatively smaller sizes of global respondents' companies, which may have proportionately more senior staff than the larger US companies.

As previously noted, the external fraudster poses an increased threat to organizations, and companies are taking heed. Fewer respondents reported they didn't know the profile of the main perpetrator of external crime during the survey period (13%) compared to 2011 (21%). However, as revealed by Figure 15 , the profile of the external fraudster underwent a major shift since 2011, reflecting an ongoing need for organizations to understand with whom they do business.

Our US results show that respondents rated agents/intermediaries as the leading perpetrator of external fraud (39%) - and more than double the rate of the 2011 survey. This also differs from the global average which experienced the opposite – customers were most often reported as the main perpetrator of external fraud (33%), followed by others (24%) and agents/intermediaries (18%). Agents/intermediaries often function as extensions of the organization, acting as the company's "face" to end-customers and reflecting the organization's brand to the world; their misdeeds can be attributed to the company itself and cause serious damage to a company's reputation. In certain circumstances, legal liability may attach as well. Agents and intermediaries are likely to operate outside of companies' compliance environment and there is often limited transparency as to their interactions with government officials. The need to curb external fraud committed by agents/ intermediaries is critical with organizations increasingly concerned about the impact of fraud on their reputation.



Third party due diligence

Given the increased risk that third parties pose to companies, the DOJ and SEC recommend that companies consider the following factors in establishing and implementing its third party due diligence:

- Does your company understand the qualifications and associations of its third party partners, including its business reputation and relationship, if any, with foreign officials? The degree of scrutiny should increase as red flags surface.
- Does your company understand the business rationale for including the third party in the transaction, including the role of and need for the third party, and ensuring that the contract terms specifically describe the services to be performed?
- Does your company engage in some form of ongoing monitoring of third party relationships, periodically updating due diligence where appropriate, exercising audit rights, providing periodic training, and requesting annual compliance certifications by the third party?

* Questions based on guidance contained in: A Resource Guide to the U.S. Foreign Corrupt Practices Act, U.S. Department of Justice and U.S. Securities and Exchange Commission (November 14, 2012).

Tough on the outside, but soft on the inside

Although we continue to see that US respondents generally reported taking tougher action than did global peers against both internal and external fraudsters, there was a noticeable divergence in the US treatment of internal and external perpetrators. US companies took fewer actions against internal fraudsters during the survey period compared to 2011. The decreases were across all categories except civil action taken and warning/reprimand. In addition, 4% of US respondents reported taking no action against internal fraudsters during the survey period, whereas no respondents reported taking no action in 2011 (Figures 16 and 17).

Figure 16: Action taken against internal perpetrator of fraud

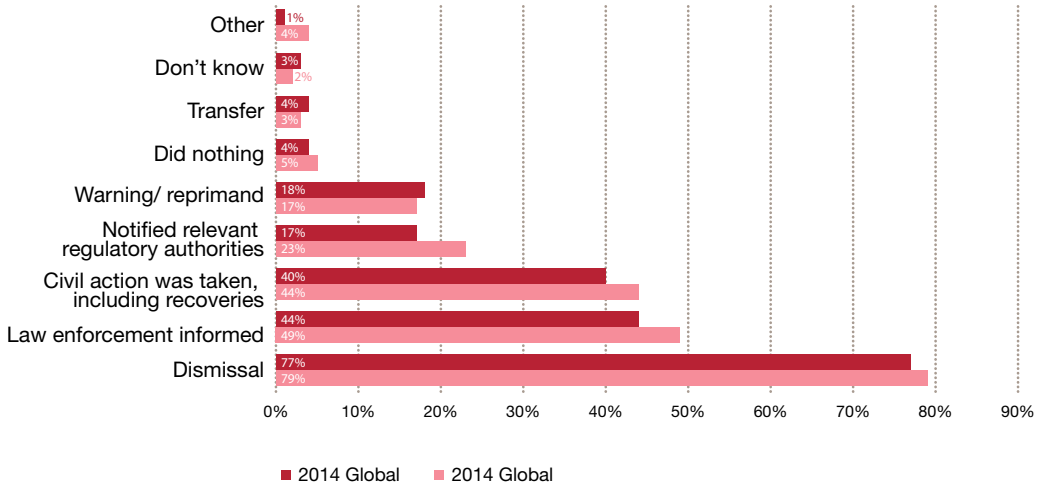
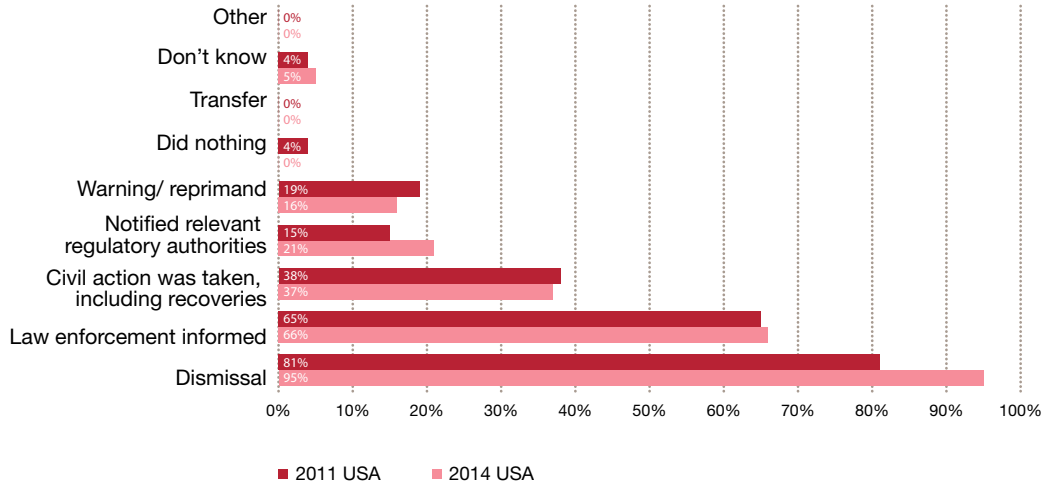


Figure 17: Action taken against internal perpetrator of fraud



Meanwhile, US companies took greater action against external fraudsters compared to 2011 with increases across all categories, and the number of respondents who reported taking no action against external fraudsters decreased to 4% from 7% in 2011. (Figures 18 and 19).

Figure 18: Action taken against external perpetrator of fraud

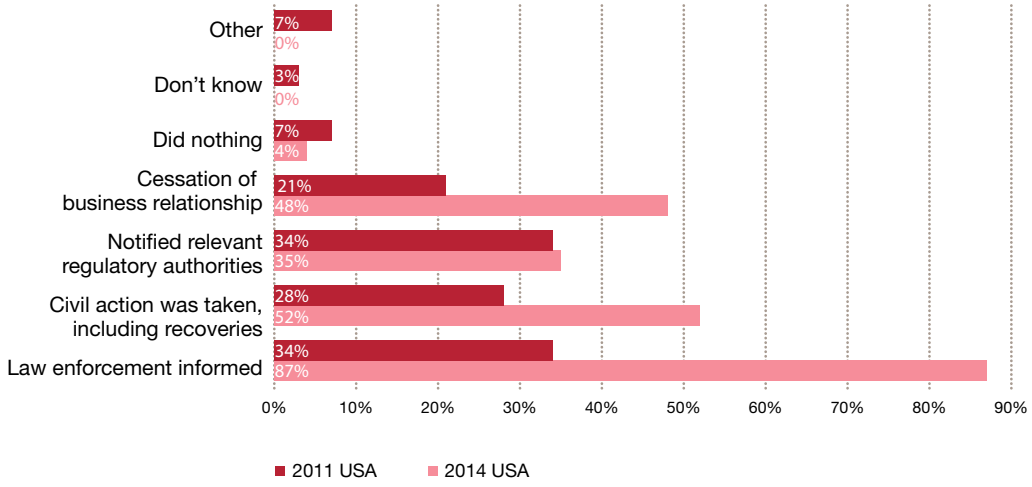
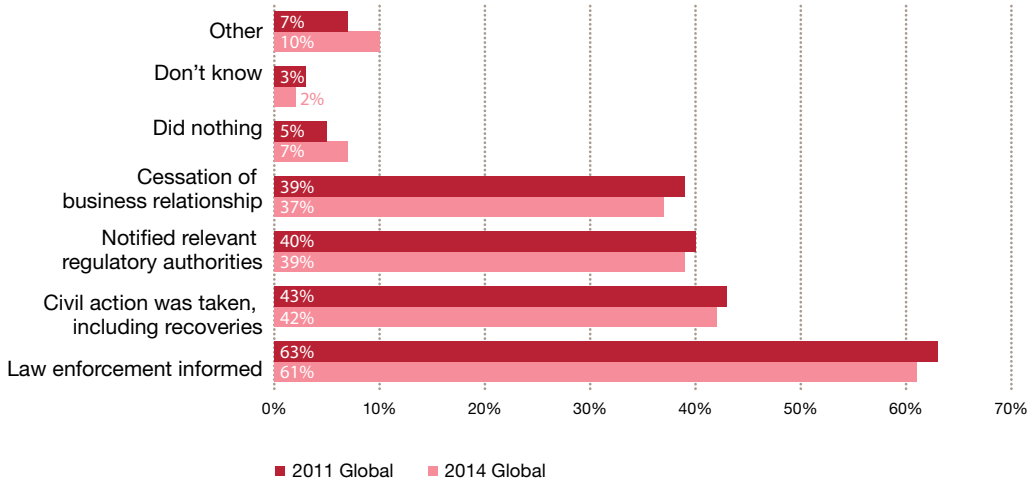


Figure 19: Action taken against external perpetrator of fraud



There are also notable differences when comparing equivalent actions taken by US companies against internal and external perpetrators. Organizations informed law enforcement about external perpetrators 22% more often than internal perpetrators (87% external, 65% internal), notified relevant regulatory agencies about external perpetrators 20% more often than internal perpetrators (35% external, 15% internal), and took civil actions, including recoveries, against external perpetrators 13% more often than against internal perpetrators (52% external, 39% internal). Organizations did report terminating the business relationship with internal perpetrators more often than with external perpetrators, with 81% of organizations terminating internal fraudsters compared with 48% of organizations ceasing business relationships with external fraudsters. However, the margin is narrowing from 2011, with dismissal of the internal perpetrator dropping 14% and cessation of the business relationship with the external perpetrator increasing 27% from 2011.

These trends are consistent with the corresponding decrease in frauds committed by internal actors and the increase in frauds committed by external actors to the extent that organizations may be increasingly focusing their efforts against the external fraudster. However, it will be interesting to see if the weaker actions taken against internal actors and stronger actions taken against external actors will lead to an increase in frauds perpetrated by internal fraudsters and decrease in frauds perpetrated by external fraudsters in our next survey.

Under relevant guidelines, both the SEC and DOJ place a high premium on self-reporting, along with cooperation and remedial efforts in determining the appropriate resolution of Foreign Corrupt Practices Act (FCPA) matters. They specifically consider whether the company made a timely and voluntary disclosure and the company's remedial actions, including efforts to improve existing compliance programs or appropriate disciplining of wrongdoers ("A company's remedial measures should be meaningful and illustrate its recognition of the seriousness of the misconduct, for example, by taking steps to implement the personnel, operational and organizational changes necessary to establish an awareness among employees that criminal conduct will not be tolerated.").[4] By implementing tougher actions against fraudsters, companies have the opportunity to mitigate the collateral effects of economic crime, and their criminal and civil liability.

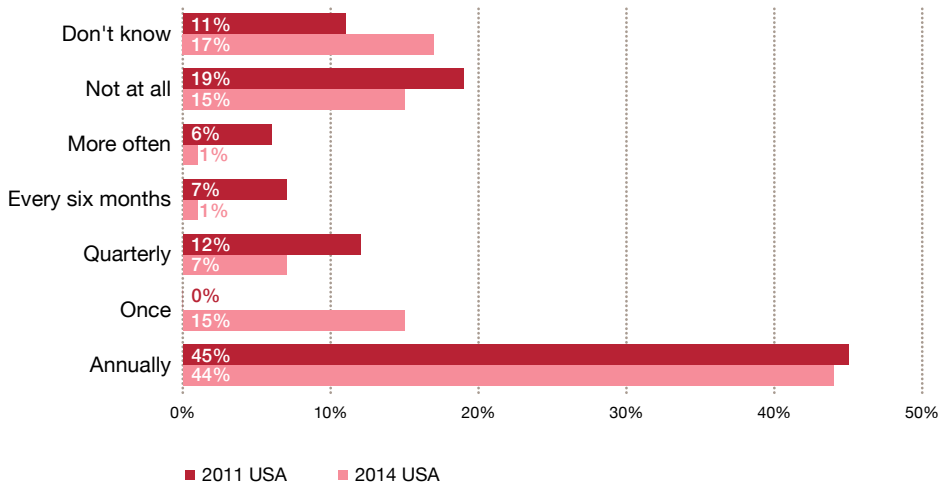
4 A Resource Guide to the U.S. Foreign Corrupt Practices Act, U.S. Department of Justice and U.S. Securities and Exchange Commission (November 14, 2012).

Performing fraud triage

Our 2014 survey results reflect that US organizations took a less proactive approach to fraud prevention than in 2011, consistent with the uptick in economic crime experienced across most fraud categories since 2011.

Although more US organizations reported performing fraud risk assessments than in 2011 (during the survey period 15% of respondents reported performing "none at all" down from 19% in 2011), those organizations that did make fraud risk assessments performed them less frequently than reported in 2011.[5] Additionally, the number of respondents that were not aware of whether their organization performed fraud risk assessments increased to 17% from 11% in 2011 (Figure 20).

Figure 20: Frequency of fraud risk assessments



The frequency with which US respondents performed fraud risk assessments decreased across all categories since 2011. A little over a half of organizations performed fraud risk assessments annually or more often (53%), a significant drop from 2011 when 70% of organizations performed fraud risk assessments annually or more often. More US organizations reported performing at least one fraud risk assessment within the past 24 months (68%) compared with the global average (63%). However, of the organizations that did perform fraud risk assessments, the US trails the global average in performing the most frequent fraud risk assessments with 9% of US organizations performing fraud risk assessments at least once every six months compared with the global average of 19%.

5 In the 2014 survey, respondents were asked whether and how often they had performed a fraud risk assessment in the previous 24 months; in the 2011 survey, respondents were asked whether and how often they had performed a fraud risk assessment in the previous 12 months. Therefore, organizations responding to our survey that did perform fraud risk assessments once every two years, but not annually, would have selected performing "none at all" in 2011, whereas organizations responding to our 2014 survey would have had the option of selecting "once every two years."

Should your company prove to have potential exposure in a criminal or regulatory investigation, often the best thing it can do is uncover issues as early as possible and self-disclose. To do so, the proper trip-wires need to be in place, as well as a response strategy. The very first step is a comprehensive risk assessment

Drive the bus—don't fall under it

Being aware of your risk environment is critical for maximizing the opportunity to prevent and detect economic crime. Identifying, investigating, and promptly disclosing misconduct or potential criminal activity could ensure that your company gets credit from regulators and prosecutors, and possibly a seat at the table instead of in the corner. The DOJ and SEC recommend that companies should consider the following factors in establishing and implementing compliance procedures:*

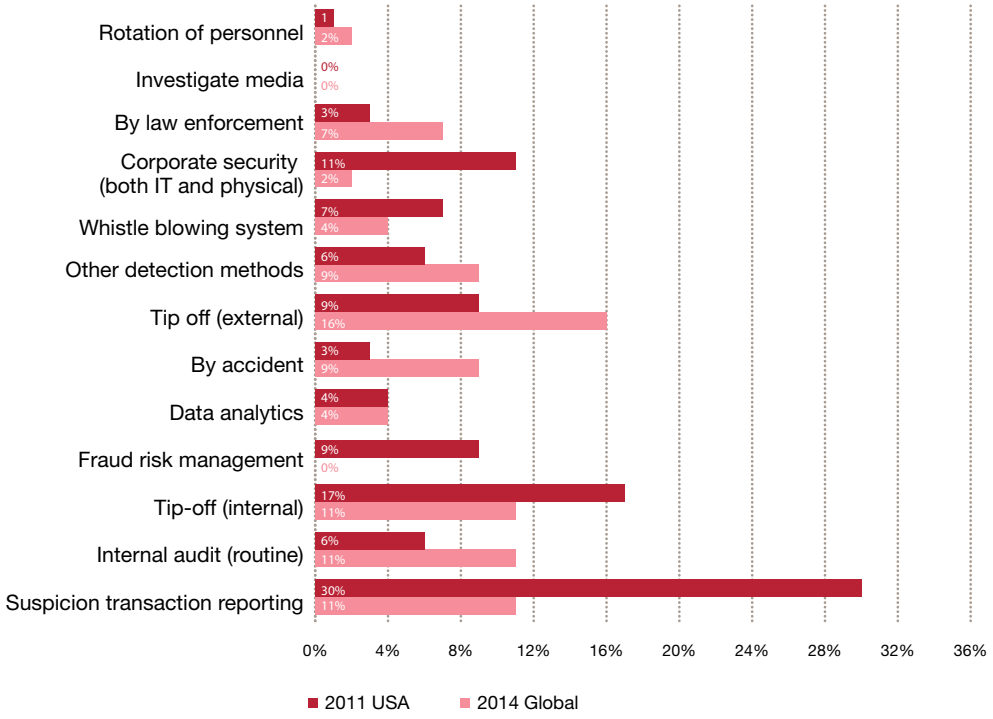
- Risks presented by the country and industry sector;
- The business opportunity;
- The potential business partners;
- The level of involvement with governments;
- The amount of government regulation and oversight; and
- The exposure to customs and immigration in conducting business affairs.

* Based on guidance contained in: A Resource Guide to the U.S. Foreign Corrupt Practices Act, U.S. Department of Justice and U.S. Securities and Exchange Commission (November 14, 2012).

The best defense is a good offense

In addition to asking companies about their fraud prevention measures, we asked organizations how they initially detected the most serious economic crime their organization experienced in the last 24 months (Figure 21). Consistent with the decrease in frequency of organizations performing fraud risk assessments, frauds detected by external measures[6] or by accident (32%) more than doubled from 2011 (15%).

Figure 21: Method by which most serious fraud was initially detected



The shift away from internal detection measures to external ones should be a wake-up call – costs can be staggering when frauds are increasingly detected by external methods rather than internal ones. The sooner organizations identify fraud or its susceptibility to fraud, the more opportunities they have to mitigate its potential consequences. The earlier such activity can be detected, the more opportunity there is to control the course of events through internal investigation and, if necessary, self-disclosure to authorities. When such activity is discovered only when there is a "knock at the door" by regulators or prosecutors, one of the best opportunities to gain meaningful consideration in the face of an investigation is lost.

6 External measures are defined as those identified by "external tip-offs," "law enforcement" or "investigamedia."

DOJ/SEC Hallmarks of effective compliance programs*	Take away questions
Commitment from Senior Management and a Clearly Articulated Policy Against Corruption:	Does senior management have clearly articulated company standards that are communicated in unambiguous terms, adhered to scrupulously and disseminated throughout the organization?
Code of Conduct and Compliance Policies and Procedures:	Does senior management periodically review and update its code of conduct to ensure that it remains current and effective, including: outlining responsibilities for compliance within the company; detailing proper internal controls, due diligence practices, and documentation policies; and setting forth disciplinary procedures?
Code of Conduct and Compliance Policies and Procedures:	Has your company assigned responsibility for oversight and implementation of its compliance program to one or more specific senior executives who have the proper authority, adequate autonomy from management, and sufficient resources to ensure your company's compliance program is implemented effectively?
Oversight, Autonomy and Resources:	Has your company, in good faith, implemented a comprehensive, risk-based compliance program that is tailored to its industry, size, nature of transaction, and method and amount of third-party compensation?
Risk Assessment:	Does your company provide periodic training and certification for all directors, officers, employees, and, where appropriate, agents and business partners, consistent with the size and sophistication of your company?
Training and Continuing Advice:	Does your company provide guidance and advice on complying with your company's ethics and compliance program, including when such advice is needed urgently?
Incentives and Disciplinary Measures:	Does your company have appropriate and clear disciplinary procedures that are applied reliably and are commensurate with the violation and applied fairly and consistently across the organization?
Third-Party Due Diligence and Payments:	Does your company engage in risk-based due diligence on third parties, inform third parties of your company's compliance program and commitment to ethical and lawful business practices, and where appropriate, seek assurances from third parties, through certifications or otherwise, of reciprocal commitments?
Continuous Improvement—Periodic Testing and Review:	Does your company regularly review and improve its compliance programs in light of any changes to the business, the environments in which it operates, the nature of its customers and the laws that govern its actions and standards of the industry?
Mergers & Acquisitions—Pre-Acquisition Due Diligence and Post Acquisition Integration:	Does your company conduct effective due diligence on its acquisition targets? Does your company ensure the acquired company promptly incorporated its internal controls and compliance programs, trained new employees, re-evaluated third parties under company standards and, where appropriate, conducted due diligence on new business?

*Source: A Resource Guide to the US Foreign Corrupt Practices Act, US Department of Justice and US Securities and Exchange Commission (November 14, 2012)

US companies reported that fraud was initially detected most often through external tip-offs (16%), taking the top spot from suspicious transaction reporting which plummeted by almost two thirds (30% vs. 11%) since our last survey. However, viewed together with the 2009 survey results, it appears as if this could be a reversion to the mean and that the 2011 results represented a "spike". This may have been due, in part, to an increase in historical fraudulent activity being uncovered and reported through "look backs" in the mortgage and financial industries as a result of the economic crisis.

Interestingly, despite the decrease in frequency of fraud risk assessments performed by US organizations discussed above, the statistics reflect that performing fraud risk assessments succeeds in preventing and detecting fraud – frauds initially detected by fraud risk management more than doubled to 9%, up from 4% in 2011. When regulators and prosecutors decide whether and to what extent to investigate and pursue actions against organizations for fraud, they consider the existence and comprehensiveness of the organizations' internal controls and whether the fraud was self-reported or discovered outside of corporate governance efforts. In addition, the sanctions, penalties, judgments and government-mandated corporate compliance programs imposed on organizations as a result of a fraud scandal add substantial, and avoidable, costs to organizations. Since 2011, there has been an observed inverse relationship between whistle-blowers and law enforcement; fraud being reported by whistle-blowing declined whereas fraud being reported to law enforcement has increased. This could be due to whistleblowers feeling incentivised through Dodd Frank to report directly to law enforcement or regulators rather than attempting to report internally.

Blowing the whistle on fraud

In the wake of Dodd-Frank implementation, we added questions about organizations' whistleblower mechanisms:

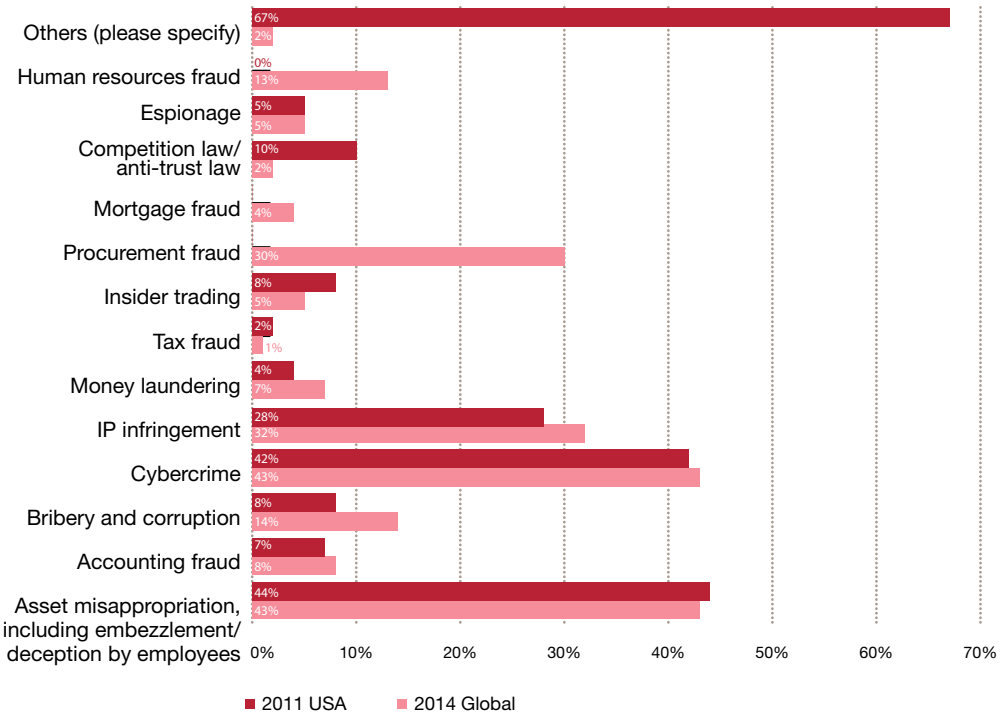
- 86% of respondents indicated their organization had a whistleblower mechanism
- Regarding frequency of use within the past 24 months, organizations reported using their whistleblower mechanism:
  - More than 100 times: 12%
  - 11-100 times: 21%
  - 1-10 times: 24%
  - Zero times: 9%
  - Don't know: 34%
- Regarding effectiveness in preventing and detecting economic crime, organizations evaluated their whistleblower mechanisms as:
  - Effective: 83%
  - Not effective: 5%
  - Don't know: 12%

All eyes on the horizon

US respondents think it's more likely they will experience dangers from fraud across almost all categories of economic crime than they did in 2011 (Figure 22). This trend is likely driven by organizations' actual experiences with fraud over the past 24 months, as organizations became more aware of and increasingly impacted by the significant financial cost and collateral damage associated with economic crime.

Respondents are more worried about bribery & corruption than they were in 2011. This may be due in part to the continued robust enforcement of the FCPA as well as the first cases stemming from the UK Bribery Act. In addition to these laws, other countries such as Spain, India, and Brazil have adopted new anti-corruption measures.

Figure 22: Likely frauds to be suffered

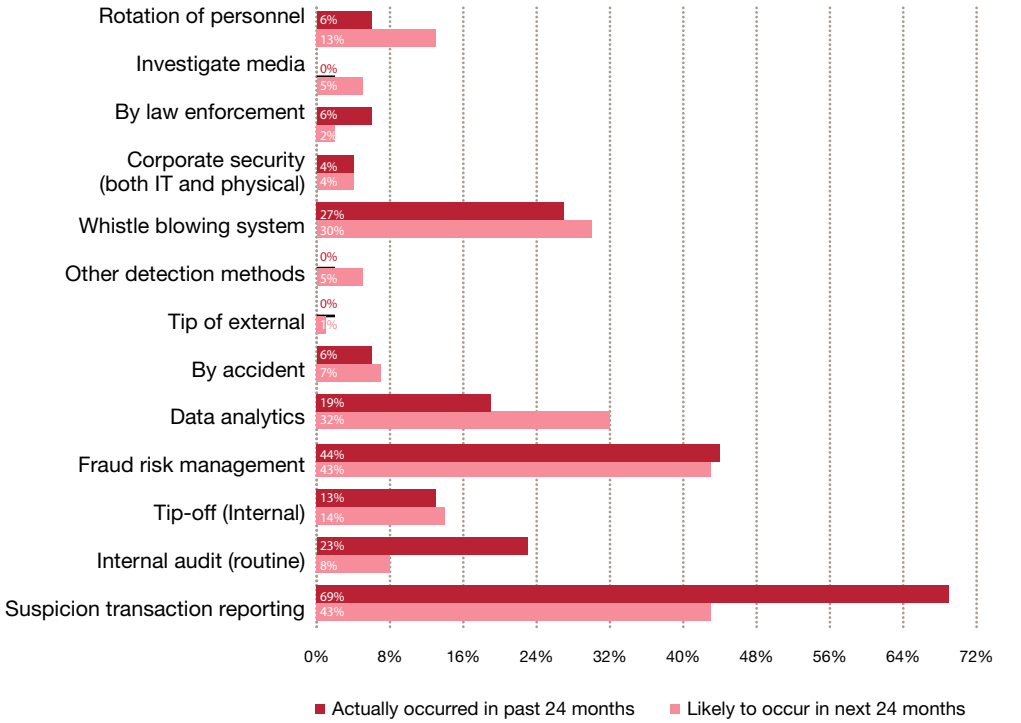


Comparing US respondents' experiences with fraud with their projections for the future (Figure 23), a few striking paradoxes emerge.

First, although 69% of respondents experienced asset misappropriation in the survey period, only 43% predict that it is likely to affect their companies in the next two years. Also, while 23% reported experiencing accounting fraud in the survey period, only 8% predict that it may strike over the next two years. These differences could reflect the confidence some respondents have in new anti-fraud controls and policies their organizations adopted after being victimized.

Second, over twice as many respondents expect to experience human resources fraud in the next two years as experienced it in the survey period. Similarly, 32% expect to experience IP infringement even though only 19% experienced it in the survey period. This heightened awareness may reflect a growing concern that such crime is on the rise, or that the respondents' organizations may not be equipped with adequate controls to protect against such threats.

Figure 23: Comparison of types of fraud actually suffered to types of fraud likely to be suffered



With more opportunities come more risks; no longer can organizations focus their fraud prevention and detection strategies on only a few types of fraud, a certain profile of fraudster, or certain perceived threats. They must be prepared to cast a wider net, for the threats associated with fraud are growing.

Certainly, the interplay among enhanced global regulatory scrutiny, more skilled and technologically-sophisticated fraudsters, and the emergence of an increasingly borderless business environment presents ongoing challenges to organizations as they combat fraud during the economic recovery period. However, organizations simply cannot afford to take a passive or reactive approach toward fraud. In addition to the initial financial impact, our survey respondents were acutely attuned to the collateral and potentially irreparable damage fraud causes to their organization's brand and reputation among its present and prospective customers, employees, and business partners. Ideally, this heightened awareness will prompt organizations to make the up-front investment in fraud prevention and detection methods, which continuously prove less costly than implementing damage control measures after the fact. By taking a pre-emptive and proactive approach to fraud, organizations can gain a competitive advantage and set themselves up for sustained success.

Acknowledgments

A core team at PwC worked diligently on the US Supplement of the 2014 Global Survey. We'd like to acknowledge the contributions of:

Didier Lavion
Principal
didier.lavion@us.pwc.com
(646) 471-8440

Steven Skalak
Partner
steven.skalak@us.pwc.com
(646) 471-5950

Sean Joyce
Principal
sean.joyce@us.pwc.com
(703) 918-3528

Peter Zanolin
Manager
peter.l.zanolin@us.pwc.com
(646) 471-4815

Lauren Bush
Experienced Associate
lauren.r.bush@us.pwc.com
(646) 471-1903

Paul Charbonnet
Experienced Associate
paul.d.charbonnet@us.pwc.com
(646) 471-9879

Forensic Leadership

Chris Barbee
Global Advisory Forensics Leader
chris.barbee@us.pwc.com
(267) 330-3020

Erik Skramstad
U.S. Advisory Forensics Leader
erik.skramstad@us.pwc.com
(617) 530-6156

Contacts

PwC Forensic Services

Atlanta

Robert Gallagher
robert.e.gallagher@us.pwc.com
(678) 419-4314

Boston

Chris Barry
christopher.c.barry@us.pwc.com
(617) 530-6304

John May
john.m.may@us.pwc.com
(617)-530-5340

Florida

Mona Clayton
mona.m.clayton@us.pwc.com
(305)-347-3510

Chicago

James Bucrek
james.bucrek@us.pwc.com
(312) 298-3907

Ted Hawkins
ted.hawkins@us.pwc.com
(312) 298-3181

Kevin Kreb
kevin.kreb@us.pwc.com
(312)298 -2587

Ryan Murphy
ryan.murphy@us.pwc.com
(312) 298-3109

Kris Swanson
kris.swanson@us.pwc.com
(773) 551-0293

Dallas

Todd Ranta
todd.c.ranta@us.pwc.com
(214) 754-4513

Charles Reddin
charles.reddin@us.pwc.com
(214) 754-5173

Houston

Karyl Van Tassel
karyl.van.tassel@us.pwc.com
(713) 356-4242

Brian Wycliff
brian.wycliff@us.pwc.com
(713) 356-5499

Los Angeles

Alexandre Blanc
alexander.blanc@us.pwc.com
(213) 217-3384

Owen Murray
owen.w.murray@us.pwc.com
(213) 356-6097

New York

Manny Alas
manny.a.alas@us.pwc.com
(646) 471-3242

Frank Badalamenti
frank.badalamenti@us.pwc.com
(646) 471-1460

Kevin Bandoian
kevin.bandoian@us.pwc.com
(646) 471-2058

Emanuel Bulone
emanuel.bulone@us.pwc.com

Brian Castelli
brian.castelli@us.pwc.com
(646) 471-2563

Dyan Decker
dyan.a.decker@us.pwc.com
(646) 313-3636

Patricia Etzold
patricia.a.etzold@us.pwc.com
(646) 471-3691

Brian Fox
brian.t.fox@us.pwc.com
(646) 471- 3398

Joe Guistino
joe.guistino@us.pwc.com
(646) 471-8523

Charles Hacker
charles.r.hacker@us.pwc.com
(646) 471-8580

David Jansen
david.jansen@us.pwc.com
(646) 471-8329

Philip Koos
philip.koos@us.pwc.com
(646) 471-2454

Grace Lamont
grace.lamont@us.pwc.com
(646) 471-7449

Didier Lavion
didier.lavion@us.pwc.com
(646) 471-8440

Ted Martens
ted.martens@us.pwc.com
(646) 471-7340

Dana McIlwain
dana.mcilwain@us.pwc.com

SandraMaria Parrado
sandra.maria.t.parrado@us.pwc.com
(646) 471-5552

Matthew Shelhorse
matthew.j.shelhorse@us.pwc.com
(646) 471-5749

Steven Skalak
steven.skalak@us.pwc.com
(646) 471-5950

Darren Tapp
darren.j.tapp
(646) 471-1384

Philip Upton
philip.upton@us.pwc.com
(646) 471-7508

Orange County

Jeff Leedom
jeff.leedom@us.pwc.com
(949) 437-5774

Philadelphia Metro

Chris Barbee
chris.barbee@us.pwc.com
(267)-330-3020

Mark Gerber
mark.gerber@us.pwc.com
(267) 440-1888

San Francisco

Jane Allen
jane.allen@us.pwc.com
(415) 498-5656

James Meehan
james.r.meehan@us.pwc.com
(415) 498-6531

Kristin Rivera
kristin.d.rivera@us.pwc.com
(415) 498-6566

Bruce Vanderbush
bruce.a.vanderbush@us.pwc.com
(415) 498-6595

Kim Wiatrak
kim.wiatrak@us.pwc.com
(415) 498-6528

San Jose

David Marston
david.l.marston@us.pwc.com
(408) 817-3803

Washington Metro

Charles Beard
charles.e.beard@us.pwc.com
(703) 918-3318

David Burg
david.b.burg@us.pwc.com
(703) 918-1067

Mike Hamilton
mike.hamilton@us.pwc.com
(202) 756-1778

Sean Joyce
sean.joyce@us.pwc.com
(703) 918-3528

Neil Keenan
neil.keenan@us.pwc.com
(703) 918-1216

Frederic Miller
frederic.r.miller@us.pwc.com
(703) 918-1564

Shane Sims
shane.sims@us.pwc.com
(703) 918-6219

Sanjay Subramanian
sanjay.subramanian@us.pwc.com
(703) 918-1509

James Thomas
james.w.thomas@us.pwc.com
(703) 918-3050

Al Vondra
al.vondra@us.pwc.com
(703) 918-1534

Glenn Ware
glenn.ware@us.pwc.com
(703) 918-1555

www.pwc.com/us/crimesurvey

This publication is printed on McCoy Silk. It is a Forest Stewardship Council™ (FSC®) certified stock containing 10% post consumer waste (PCW) fiber and manufactured with 100% Green-e certified renewable energy

LA-14-0127 US Global Economic Crime Survey