Kroll

GLOBAL FRAUD & RISK REPORT

Building Resilience in a Volatile World

ANNUAL EDITION **2016/17**

FORRESTER®

Commissioned research conducted by Forrester Consulting.

About the research methodology

For the 2016/2017 Global Fraud and Risk Report, Kroll commissioned Forrester Consulting to conduct 10 in-depth interviews and an additional online survey with 545 senior executives worldwide across multiple industries and geographies. The survey was fielded through July and August 2016.

In addition to building on coverage of fraud from prior Kroll surveys, the scope of research this year was expanded to cover perceptions of and experiences with cyber and security risk. As with prior surveys, respondents represented a variety of industries, including Technology, Media, and Telecoms; Professional Services; Manufacturing; Natural Resources; Construction, Engineering, and Infrastructure; Consumer Goods; Financial Services; Retail, Wholesale, and Distribution; Transportation, Leisure, and Tourism; and Healthcare, Pharmaceuticals, and Biotechnology.

Respondents held senior positions within their companies, with 70% of respondents representing the C-suite. 61% of companies had annual revenues of $500 million or more.

Respondents represented all major global geographies, including 25% from Europe, 20% from the Asia-Pacific region, 20% from North America, 19% from the Middle East/Africa, and 16% from Latin America.

All listed monetary values are in U.S. dollars.

Foreword

We have expanded the scope of this year's Report—it's now the annual Kroll Fraud and Risk Report, breaking out specific cyber and security threats to better reflect the growing challenges that our clients are facing around the world.

One thing that has become even more pronounced is the importance of anticipating and addressing the insider threats. The results of our survey underscore and highlight this conclusion. Whether it's fraud, cyber threats, or security risk … whether it's Asia, Europe, or the Americas … or whether it's services, finance, retail, or manufacturing, the figures show companies are most at risk from an employee, a former employee, or a temporary employee/contractor.

There is good and bad news in this conclusion. The good news is that companies have a better chance of managing their risk exposure to insiders than an anonymous outsider, once the threat is recognized and understood. They also have a better chance of successfully investigating the problem and securing recoveries, having greater access to and control of the evidence trail inside the company.

The bad news is that the impact on reputation, both inside and outside the company, may be greater if an insider threat or incident is not handled carefully—indeed, our survey shows that one of the most serious consequences of fraud and risk issues is the impact on employee morale. In a regulated business, the relevant regulators will also almost certainly take an interest: Poor controls in one area may be viewed as a trigger for closer scrutiny, even when the problem has no relevance to safety or customer data or funds.

Concerns over staff morale and regulatory attention can push in opposite directions when it comes to considering how to investigate the problem. Reputational fears and employee reactions may dictate a more discreet, lower key "let's not rock the boat and make the problem worse" response. But mitigation of regulatory risk (and potential litigation risk) demands a swift and rigorous effort to fully investigate the problem, determine the root cause, and resolve it: Regulators are generally not particularly sympathetic to your concerns regarding image and staff morale. Making the judgment on the balance between the two requires experience: an understanding of the nature of the problem, appreciation of different available investigative techniques and approaches, and mindfulness of the significance of possible outcomes.

It also requires familiarity with local culture and legal requirements, especially when dealing with foreign operations. Privacy issues, employment laws, and legal privilege requirements—which may be important to protect the results of an investigation—all vary by jurisdiction. Failure to appreciate these rules of engagement have the potential to make the results of an investigation useless and perhaps make the problem worse.

There are also "soft" factors—i.e., cultural nuances—between countries, and sometimes regions within countries, that can be critical to a successful outcome: respect for hierarchies, loyalty to a local manager rather than the company, willingness to talk to an outsider, propensity to tell interviewers what it's perceived they will want to hear or, alternatively unwillingness to say anything at all. To understand these differences requires local knowledge and experience—and you may not be able to rely on local management for guidance and execution as they may well be part of the problem.

This "human factor" is equally important in prevention as it is in investigation. In cyber security, for example, a purely technical approach offers false comfort: It can only be as good as the people who are using it, whatever the salesman tells you. Where sophisticated cyber security systems can help is in limiting and mitigating the damage if (or perhaps when) there is a problem. Human behavior must be addressed first.

For businesses that operate multinationally, a one-size-fits-all policy and procedures manual may be so dysfunctional as to provide the same sort of false comfort. The policy may be misunderstood in one country, roundly ignored in a second, and contrary to local customs—and even laws—in a third. Regardless, even those which operate overseas through joint ventures, agents, or distributors need to have something in place. For example, in many countries now, anti-bribery laws make you potentially liable for the actions of JVs and agents, and misrepresentation by a distributor will at the very least damage your reputation.

It's becoming an increasingly risky world. That's why we added "risk" into the title of this Report, and as always, we would be happy to offer our international experience to help you navigate this complex global landscape.

TOMMY HELSBY
Co-Chairman, Investigations and Disputes, Kroll

Research Summary

Introduction

For a decade, the Kroll Global Fraud Report has assessed the current fraud environment and shared findings from senior executives surveyed around the world who operate in a wide variety of sectors and functions. In this year's survey, Kroll expanded the scope of inquiry to include a broader range of risks facing the business community, namely, fraud, cyber, and security risks. The resulting inaugural Kroll Global Fraud & Risk Report includes trend data related to the incidence of fraud and baseline data for cyber and security risks. The Report is in four sections: Research Summary, Commentary, Region Overviews, and Industry Overviews.

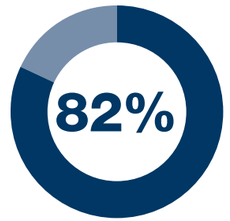
The findings of this year's survey paint a picture of a global business environment fraught with high and mounting risks and repercussions; increasing complexity in the types of risk, perpetrators, and means of attack; and adoption of risk mitigation policies and procedures to help build corporate resilience. Some key insights follow.

1 High incidence and widespread repercussions

Incidence

FRAUD

According to this year's survey, the incidence of fraud continued to climb markedly. Overall, 82% of surveyed executives reported falling victim to at least one instance of fraud in the past year, up from 75% in 2015. This continues the trend revealed in prior Kroll Global Fraud Reports, with executives reporting fraud incidence levels at 61% in 2012 and 70% in 2013.



of respondents reported a fraud incident

Percentage of respondents who reported experiencing fraud in the last 12 months

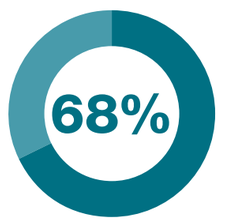
CYBER SECURITY

An astounding 85% of surveyed executives said that their company experienced a cyber attack or information theft, loss, or attack in the last 12 months.

of respondents reported a cyber attack or information loss, theft, or attack

SECURITY

Over two-thirds (68%) of respondents reported the occurrence of at least one security incident during the last year.



of respondents reported a security incident

Repercussions

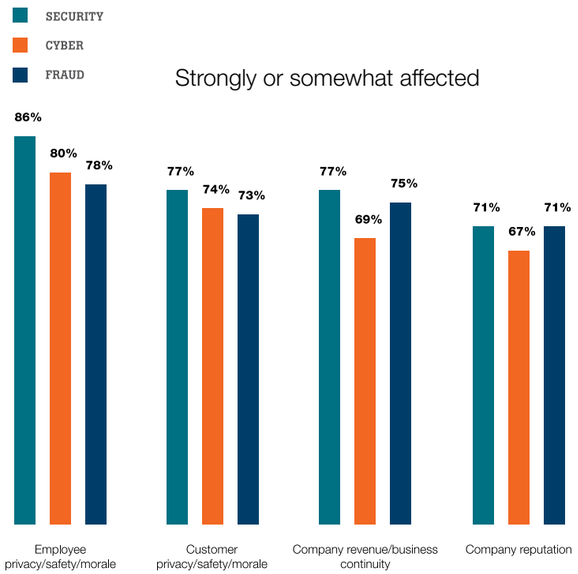
The survey indicates that the experience of a fraud, cyber, or security incident has widespread repercussions for a company's employees and customers as well as its revenue and reputation.

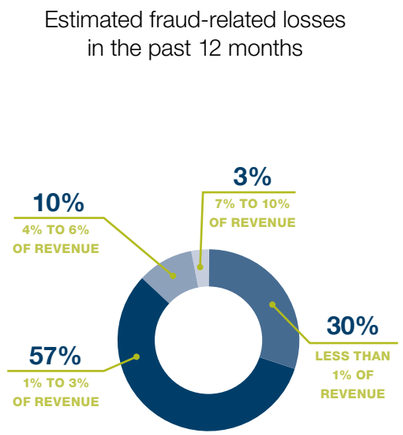
- The most common repercussion noted was the impact on employees: 86% of respondents who reported experiencing a security incident said that employee privacy/safety/morale was strongly or somewhat affected. This level of employee impact was reported by 80% of respondents who cited a cyber incident and by 78% of those who cited a fraud incident.

- While the overall prevalence of security incidents is lower than that of fraud or cyber, the impact is somewhat broader. In addition to the impact on employees, 77% of those who reported suffering a security incident stated that customers and revenue were somewhat or strongly affected, and 71% claimed their company's reputation was strongly or somewhat impacted.

- Among those who experienced a cyber incident, nearly three-quarters (74%) noted that customer privacy/safety/satisfaction was strongly or somewhat affected. Kroll expert Brian Lapidus writes in his article on page 37 that it is critical in the aftermath of a data breach to focus on customer needs, and he lays out guidelines to help rebuild customers' trust.

- Respondents claimed significant economic damage from fraud. A majority (57%) of executives estimated fraud-related losses between 1%-3% of revenue, and one in 10 businesses reported a loss equivalent to 4%-6% of revenue.





Regional risks

The globalization of business has brought strategic expansion opportunities as well as a broad array of regional risks. Indeed, in the last year, 69% of executives said they were dissuaded from operating in a particular country or region because it would bring heightened exposure to fraud. Similarly, 63% of respondents turned away from certain regions due to security concerns.

Concerns are highest regarding operating in China and India. Kroll experts Violet Ho and Reshmi Khurana, based in China and India, respectively, write in their articles on page 57 and 61 of this report about ways to mitigate risks in these countries.

Survey respondents from the manufacturing sector indicated they were some of the worst affected by fraud incidents (89% reported an incident in the past year). Over half the manufacturing participants (51%) felt that entry into new and riskier markets was a key driver of increased fraud risk. However, as Kroll experts Brian Weihs, Nicole Lamb-Hale, and Brian Sperling outline in their article on page 79, there are steps manufacturing companies, and others working in different sectors, can take to reduce the risk of operating in emerging markets.

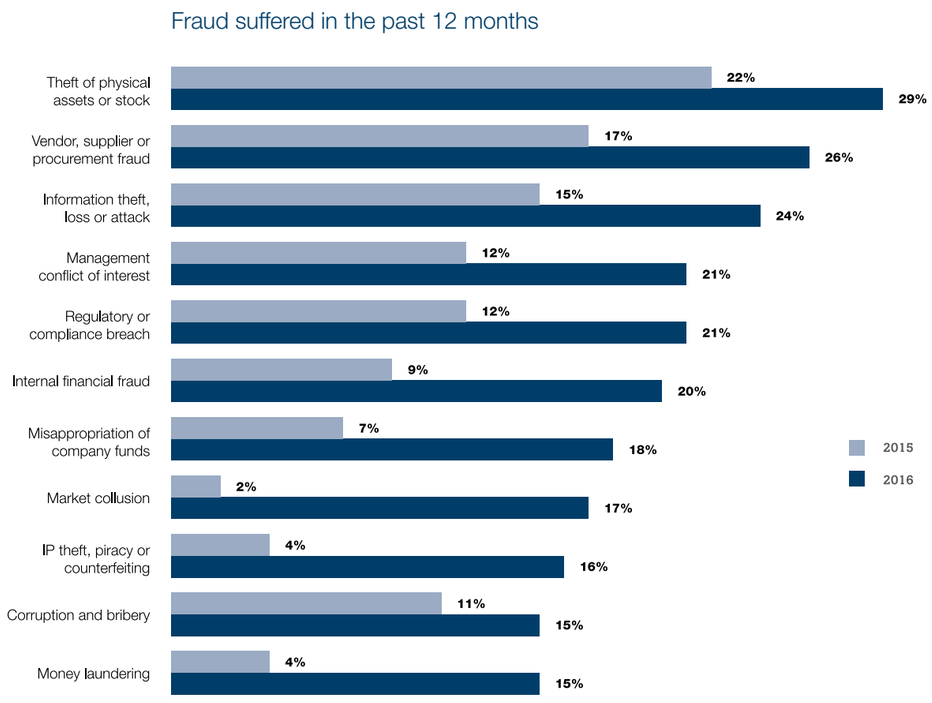
2 The complexity of the threat

The array of incidents, perpetrators, and means of attack reflect an increasingly complex risk management environment for businesses. It is notable that the internal threat from current, freelance, or ex-employees is still the most prevalent.

Types of incidents impacting business

TYPES OF FRAUD

In the past year, respondents reported experiencing more of every type of fraud than was cited in the 2015 survey. Moreover, the stated incidence of every type has now reached double-digit levels.



Theft of physical assets remained the most prevalent type of fraud experienced in the last year, reported by 29% of respondents, and up 7 percentage points from 22% of respondents in the last survey. Vendor, supplier, or procurement fraud (26%) and information theft, loss, or attack (24%) are the next two most common types of fraud cited, each up 9 percentage points year on year.

TYPES OF CYBER INCIDENTS

The survey shows that companies experienced a broad range of cyber incidents with many levels of complexity.

A third (33%) of all surveyed executives said they had been hit by a virus or worm infestation, the most frequent type of cyber incident named in this year's Report. The second most frequent type of cyber incident, an email-based phishing attack, was cited by just over a quarter (26%) of all participants.

In the age of big data, the survey showed extensive loss or theft of data via cyber-related incidents that include, among other types, data breach, data deletion, and loss of equipment with sensitive data.

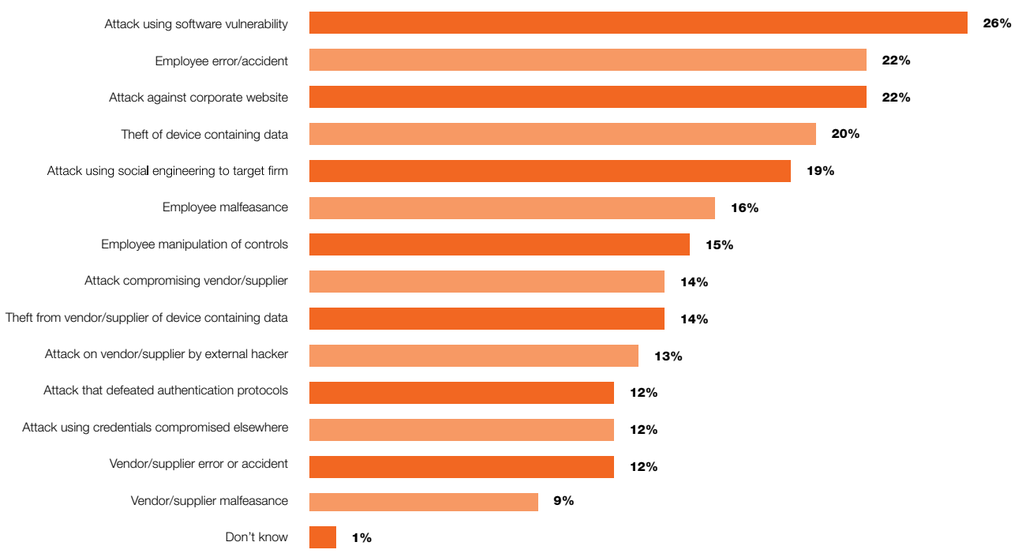
- **Data breach:** Nearly a quarter (23%) of respondents said data breaches resulted in loss of customer or employee data, while 19% cited loss of IP/trade secrets/R&D from a data breach.
- **Data deletion:** 24% of surveyed executives indicated they had experienced data deletion incidents due to system issues, 22% experienced data deletion or corruption caused by malware or system issues, and 19% were victims of data deletion by a malicious insider.
- **Loss of equipment:** 17% reported equipment with sensitive data was lost and 13% reported such equipment was stolen.

How cyber incidents happen

The survey also reveals that most cyber incidents involve more than one attack vector. Multiple, interwoven attack vectors were identified – directly on company software, systems, and websites; via third parties through malfeasance, attacks on their own systems, or in error; through employee error or malfeasance; and from device theft.

The highest reported attack vector was via software vulnerability, experienced by over a quarter of respondents (26%). Employee error or accident played a role according to 22% of respondents. And attacks on the corporate website were noted by 22% of respondents as well.

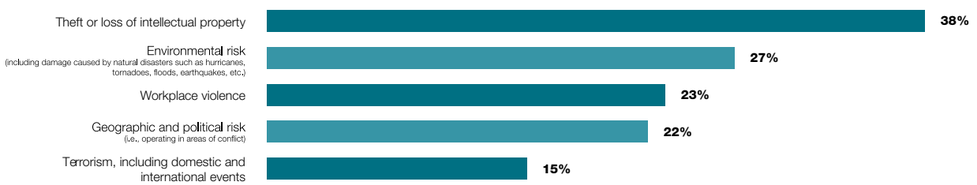
If your company has suffered from cyber attack or information loss, theft, or attack in the past 12 months, which best describes how this took place?
(Participants were asked to select up to three responses.)



TYPES OF SECURITY INCIDENTS

Theft or loss of intellectual property was the most common type of security incident, cited by 38% of those who experienced a security incident in the last 12 months. Environmental risks such as natural disasters took their toll on 27% of respondents who had a security incident, with notably high levels reported in Canada (46%) and China (45%). Nearly a quarter (23%) of respondents who indicated they had experienced a security incident cited workplace violence. Geographic/political risk and terrorism have lower incidences, 22% and 15%, respectively, and yet – underscoring the notion of volatility – it's important to recognize that both these types of security events were reported in double-digit levels.

Security incidents suffered in the past 12 months



Perpetrators

The findings reveal that threats most commonly come from within. Current and ex-employees were the most frequently cited perpetrators of fraud, cyber, and security incidents over the past 12 months. Notwithstanding this finding, external parties were identified as active perpetrators as well.

PERPETRATORS OF FRAUD

Nearly 8 out of 10 respondents (79%) cited one of the following categories as the key perpetrator:

- Senior or middle management employees of our own company
- Junior employees of our own company
- Ex-employees
- Freelance/temporary employees

Reflecting the complexity of fraud risks, the majority (60%) of executives who reported suffering fraud incidents identified some combination of perpetrators, including current employees, ex-employees, and third parties, with almost half (49%) involving all three groups. Nearly four in ten respondents (39%) who were victims experienced fraud at the hands of a junior employee, 30% at the hands of senior or middle management, 27% by ex-employees, and 27% by freelance/temporary employees. Agents and/or intermediaries, who are sometimes considered quasi-employees, were also cited by 27% of respondents as involved in carrying out fraud.

While insiders are cited as the main perpetrators of fraud, they are also identified as the most likely to discover it. Almost half (44%) of respondents said that recent fraud had been discovered through a whistleblowing system and 39% said it had been detected through an internal audit.

Kroll experts Alex Volcic and Yaser Dajani write in their article on page 33 that it is important to triage whistle-blower reports appropriately and test methods of escalation to run an effective system.

PERPETRATORS OF CYBER INCIDENTS

Overall, 44% of respondents reported that insiders were the key perpetrators of a cyber incident, citing ex-employees (20%), freelance/temporary employees (14%), and permanent employees (10%). If we also consider agents/ intermediaries as quasi-employees, noted by 13% of respondents, then the percent indicating that insiders were the key perpetrators rises to a majority, 57%. Nearly one in three (29%) identified external players as the key perpetrators.

PERPETRATORS OF SECURITY INCIDENTS

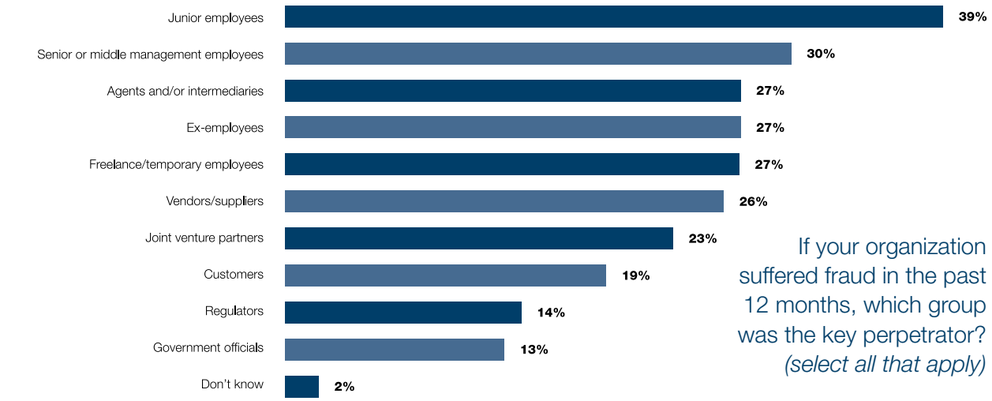
In total, 56% of executives surveyed said insiders were the key perpetrators of security incidents, citing ex-employees (23%), permanent employees (17%), and temporary/freelance employees (16%).

Interestingly, of the external perpetrators, more than one in ten (12%) respondents reported competitors were the key group and 10% pointed to random perpetrators. Political activists, nation states, and terrorists combined were named by 20% of respondents.

MANAGING THE THREAT FROM EX-EMPLOYEES

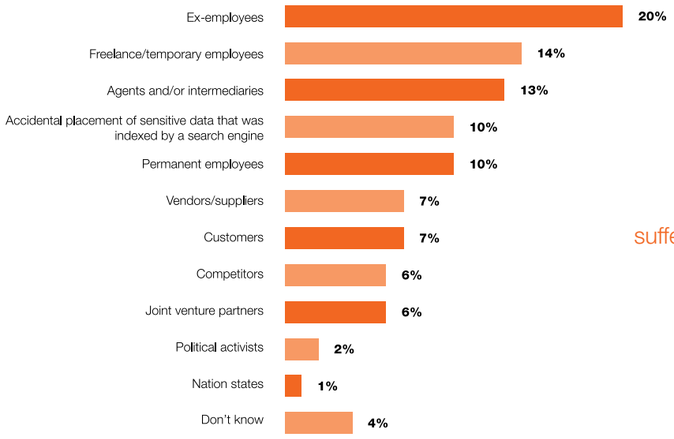
The survey showed a consistently high percent of respondents who disclosed that ex-employees were key perpetrators of fraud (27%), cyber incidents (20%), and security incidents (23%). Kroll experts Marianna Vintiadis and Tadashi Kageyama take on this topic in their article on page 25, in which they discuss some ways companies can carefully manage employee exits.

Perpetrators of fraud



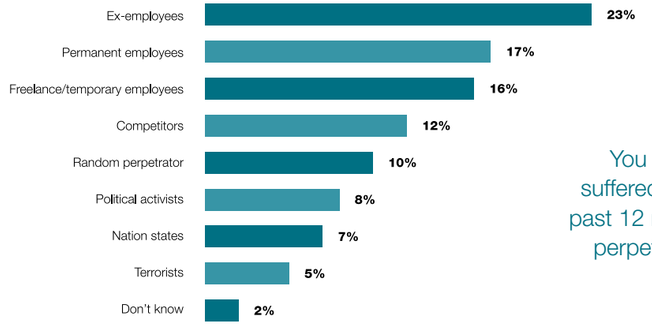
If your organization suffered fraud in the past 12 months, which group was the key perpetrator? *(select all that apply)*

Perpetrators of cyber attack or information theft, loss, and attack



You stated your company has suffered cyber attack or information loss, theft, or attack in the past 12 months, who was the key perpetrator? *(select one option)*

Perpetrators of security incidents



You stated your company has suffered a security incident in the past 12 months, who was the key perpetrator? *(select one option)*

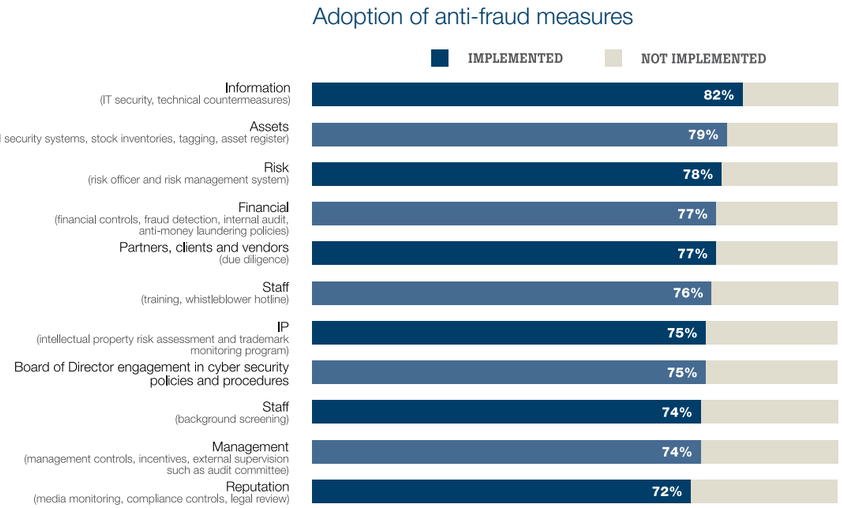
3 The road to resilience

Facing high levels of business risk, significant costs, and widespread impact on stakeholders and reputation, companies have demonstrated broad adoption of risk mitigation measures. It is clear, however, that more and continuous effort is needed to build and sustain resilience.

Below is a summary of measures many companies have already adopted—often with a plan to expand further.

Risk mitigation measures adopted

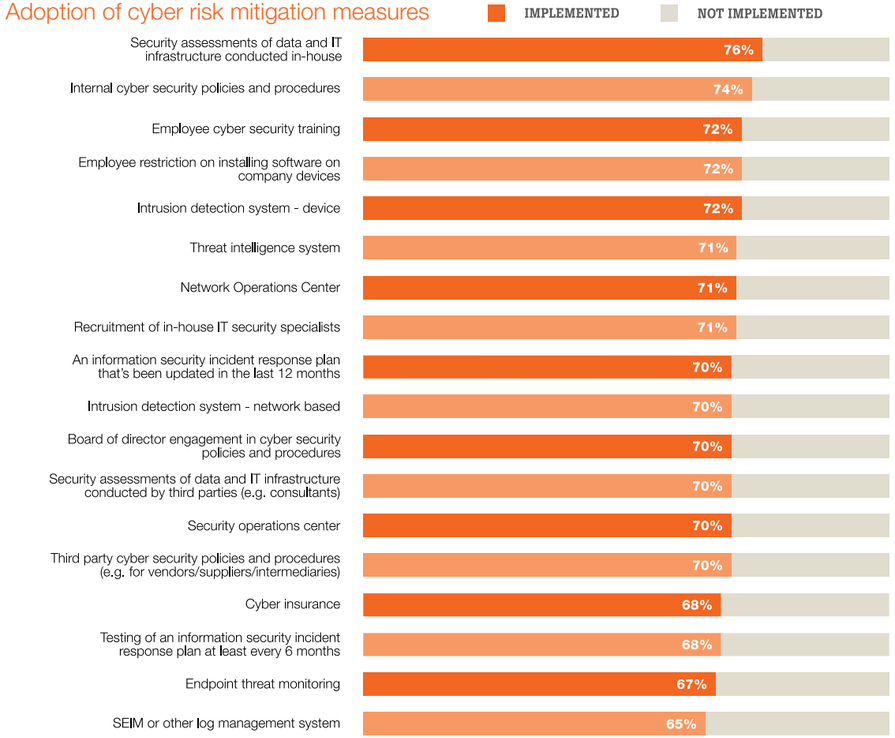
FRAUD RISK MITIGATION MEASURES



Among anti-fraud measures, the widest adoption—reported by 82% of surveyed executives—focused on information, such as IT security and technical countermeasures. The converse of that finding is concerning, meaning nearly a fifth of respondents (18%) have not adopted such protections. As noted earlier in this report, theft of physical assets or stock was the most frequently experienced type of fraud (29% of executives surveyed); accordingly, the second highest anti-fraud measures relate to assets, for example, deploying physical security systems and tagging. Interestingly, the third highest adoption was the appointment of a risk officer and installing a formal risk management system. Implementation of financial controls follows next (77%), with an equal level of adoption for third party due diligence.

The mountain of internal data that companies hold can be invaluable in the fight against fraud. For example, data analytics tools and expert analysis often reveal important red flags and anomalies in bribery and corruption investigations, as explained by Kroll experts Zoë Newman, John Slavek, and Peter Glanville in their article on page 29.

CYBER RISK MITIGATION MEASURES



The most commonly reported cyber risk mitigation action was conducting *in-house* security assessments of data and IT infrastructure, cited by 76% of surveyed executives. It is notable that 70% of respondents also cited implementing a *third party/consultant* security assessment of data and IT infrastructure. Nearly three-quarters (74%) of respondents say their company has deployed internal cyber security policies and procedures.

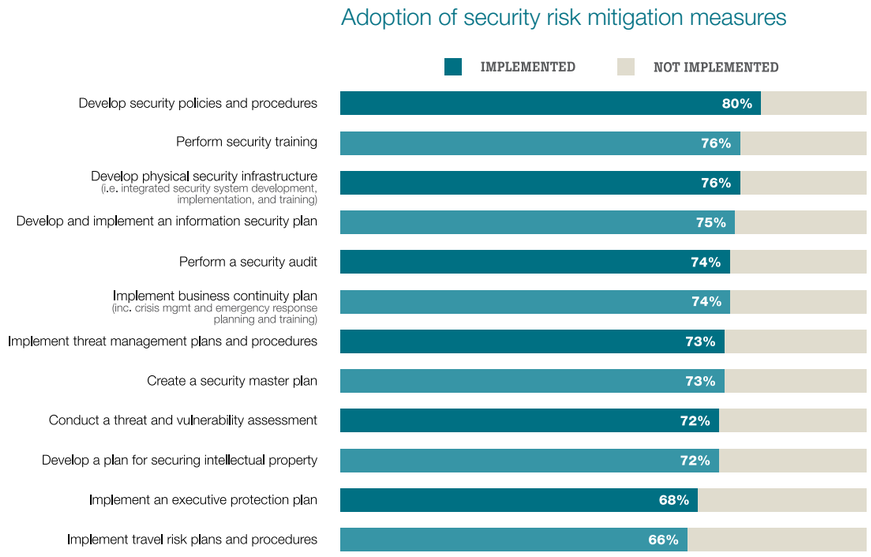
As discussed previously, 44% of cyber incidents were perpetrated by insiders (permanent staff, temporary/freelancers, ex-employees), and this reality is reflected in the adoption of internal training and policies: 72% have introduced employee cyber security training and an equal percentage have employee restrictions on installing software on company devices.

Detection methods rank high on the list, with intrusion detection systems, threat intelligence systems, and network operations centers next in magnitude of adoption.

Given the overall 85% prevalence of cyber incidents in the last 12 months, it is concerning that only 70% of respondents report their firms have an information security incident response plan that's been updated in the last 12 months and only 68% test their incident response plan every six months. Kroll experts, Andrew Beckett, Michael Quinn and Lucie Hayward, address the importance of a robust, tested incident response plan in their article on page 35.

Strikingly, reflecting the importance of cyber governance issues, 70% of survey participants say their board of directors is engaged in cyber security policies and procedures.

SECURITY RISK MITIGATION MEASURES



Overall, 80% of surveyed executives say their company has developed security policies and procedures, 76% say they perform security training, and 76% report that their company has developed physical security infrastructure. However, there is more work to do—for example, given that theft or loss of intellectual property was the most frequently experienced type of security incident (38%), it is concerning that 28% of respondents indicate they have not developed a plan for securing intellectual property. And, in a global business environment, over a third (34%) of surveyed executives say they have not implemented travel risk plans and procedures.

Kroll experts, Nick Doyle and Rafael Lopez, in their article Security Risks in Emerging Markets on page 27, say that by taking an enterprise security risk management approach, companies can identify, consider, and treat vulnerabilities more effectively and efficiently. The great strength in this approach is the ability to analyze risk in context throughout the business.

Conclusion

Risks abound, complexity multiplies, perpetrators collaborate, attack methodologies morph, and techniques to hide grow more sophisticated. All the while, companies are under more scrutiny than ever before for how effectively they manage risk and respond to incidents. Spurred by the need to both catch up and get ahead of these realities, companies have taken significant strides toward building resiliency. More is needed.

Kroll expert Jordan Strauss writes in his article on page 23 that the ability of an organization to be flexible and nimble in the face of unpredictability may depend largely on having a leadership team that is willing to make resilience a core value.

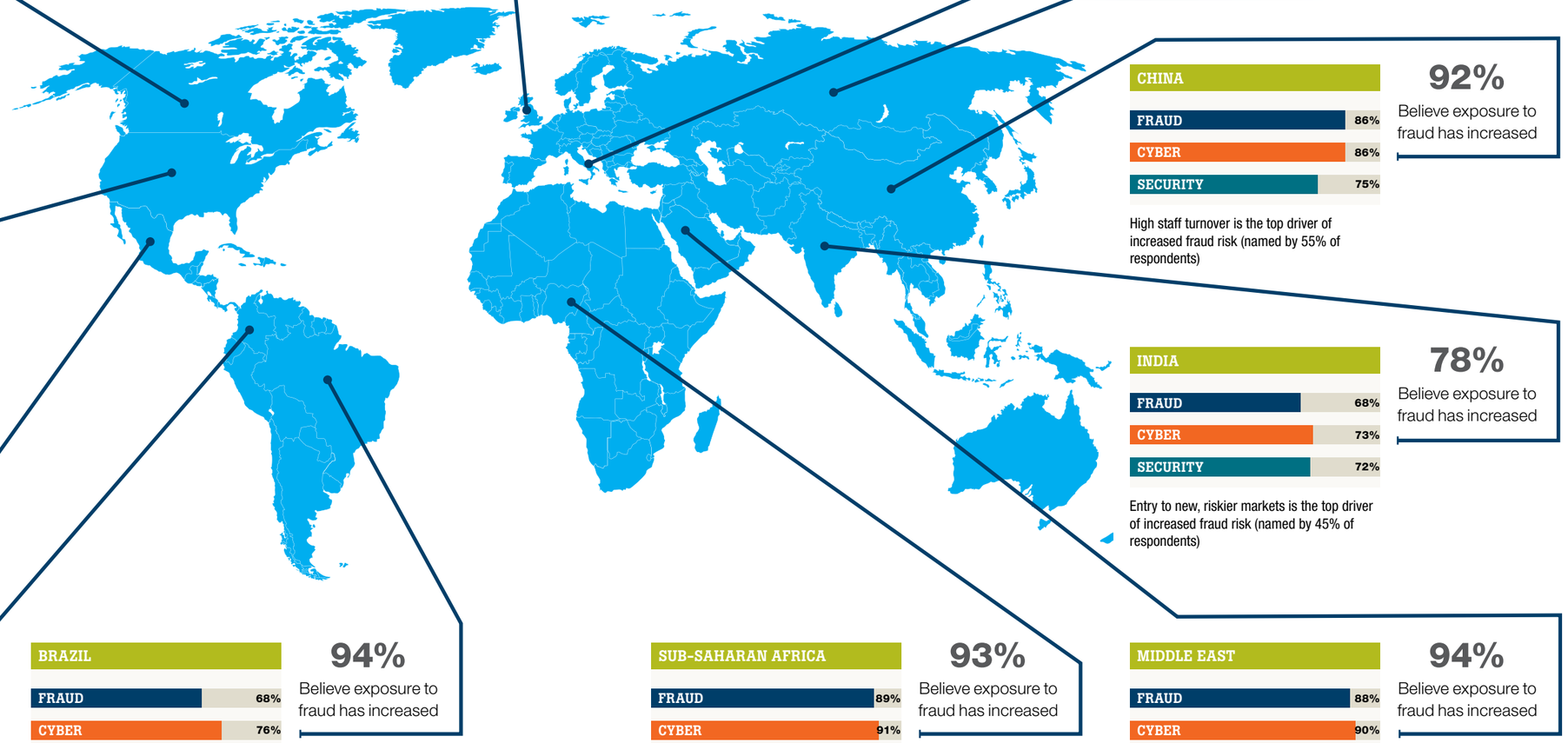
Indeed, the road to resiliency requires resources, analytics, creativity, understanding of human behavior, and sheer vigilance to continuously enhance each firm's ability to prevent, prepare, respond, investigate, and remediate fraud and risk. In an ever-changing risk environment, it is understandable that we see a growing reliance on outside experts to both achieve a deeper understanding of underlying facts and to assist with solutions.

Global Risk Map

The map shows the percentage of respondents based in each country or region whose companies experienced fraud, cyber or security incidents in the last 12 months.

Base: 545 executive-level decision-makers who influence or are responsible for their company's risk and fraud strategy

Source: A commissioned study conducted by Forrester Consulting on behalf of Kroll, August 2016



CANADA

FRAUD	88%
CYBER	85%
SECURITY	78%

93% Believe exposure to fraud has increased

Increasing exposure to public digital touch-points is the top driver of increased fraud risk (named by 54% of respondents)

UNITED STATES

FRAUD	80%
CYBER	88%
SECURITY	58%

94% Believe exposure to fraud has increased

Complexity of IT infrastrucutre is the top driver of increased fraud risk (named by 50% of respondents)

MEXICO

FRAUD	82%
CYBER	82%
SECURITY	48%

94% Believe exposure to fraud has increased

Increased outsourcing and offshoring is the top driver of increased fraud risk (named by 45% of respondents)

COLOMBIA

FRAUD	95%
CYBER	95%
SECURITY	62%

100% Believe exposure to fraud has increased

Entry to new, riskier markets and complexity of IT infrastructure are the top drivers of fraud (each named by 29% of respondents)

UK

FRAUD	90%
CYBER	92%
SECURITY	82%

92% Believe exposure to fraud has increased

High staff turnover is the top driver of increased fraud risk (named by 47% of respondents)

BRAZIL

FRAUD	68%
CYBER	76%
SECURITY	53%

94% Believe exposure to fraud has increased

Entry to new, riskier markets and complexity of IT infrastructure are the top drivers of fraud (each named by 29% of respondents)

ITALY

FRAUD	77%
CYBER	79%
SECURITY	68%

91% Believe exposure to fraud has increased

Entry to new, riskier markets is the top driver of increased fraud risk (named by 36% of respondents)

SUB-SAHARAN AFRICA

FRAUD	89%
CYBER	91%
SECURITY	74%

93% Believe exposure to fraud has increased

Increasing exposure to public digital touch-points is the top driver of increased fraud risk (named by 33% of respondents)

RUSSIA

FRAUD	82%
CYBER	82%
SECURITY	59%

85% Believe exposure to fraud has increased

High staff turnover is the top driver of increased fraud risk (named by 31% of respondents)

CHINA

FRAUD	86%
CYBER	86%
SECURITY	75%

92% Believe exposure to fraud has increased

High staff turnover is the top driver of increased fraud risk (named by 55% of respondents)

INDIA

FRAUD	68%
CYBER	73%
SECURITY	72%

78% Believe exposure to fraud has increased

Entry to new, riskier markets is the top driver of increased fraud risk (named by 45% of respondents)

MIDDLE EAST

FRAUD	88%
CYBER	90%
SECURITY	82%

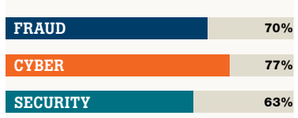
94% Believe exposure to fraud has increased

Complexity of IT infrastructure and lack of budget/resource for compliance infrastructure are the top drivers of increased fraud risk (each named by 34% of respondents)

Industry Risk Map

The map shows the percentage of participants from each industry group whose companies experienced fraud, cyber or security incidents in the last 12 months.

CONSTRUCTION, ENGINEERING AND INFRASTRUCTURE

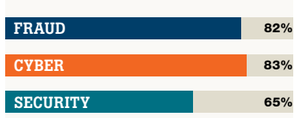


High staff turnover is the top driver of increased fraud risk (named by 40% of respondents)

86%

Believe exposure to fraud has increased

CONSUMER GOODS

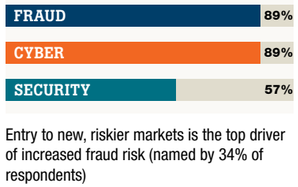


Entry to new, riskier markets is the top driver of increased fraud risk (named by 40% of respondents)

92%

Believe exposure to fraud has increased

FINANCIAL SERVICES

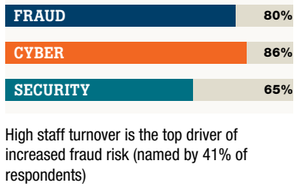


Entry to new, riskier markets is the top driver of increased fraud risk (named by 34% of respondents)

91%

Believe exposure to fraud has increased

HEALTHCARE, PHARMACEUTICALS AND BIOTECHNOLOGY

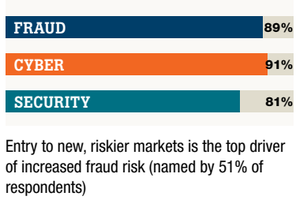


High staff turnover is the top driver of increased fraud risk (named by 41% of respondents)

88%

Believe exposure to fraud has increased

MANUFACTURING

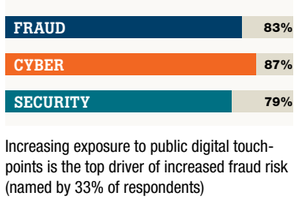


Entry to new, riskier markets is the top driver of increased fraud risk (named by 51% of respondents)

96%

Believe exposure to fraud has increased

RETAIL, WHOLESALE AND DISTRIBUTION



Increasing exposure to public digital touch-points is the top driver of increased fraud risk (named by 33% of respondents)

87%

Believe exposure to fraud has increased

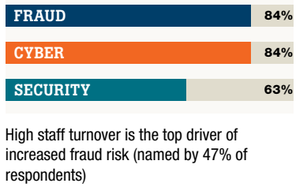
NATURAL RESOURCES

High staff turnover is the top driver of increased fraud risk (named by 40% of respondents)

92%

Believe exposure to fraud has increased

PROFESSIONAL SERVICES



High staff turnover is the top driver of increased fraud risk (named by 47% of respondents)

96%

Believe exposure to fraud has increased

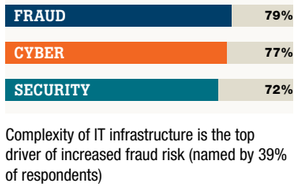
TRANSPORATION, LEISURE AND TOURISM

High staff turnover is the top driver of increased fraud risk (named by 43% of respondents)

96%

Believe exposure to fraud has increased

TECHNOLOGY, MEDIA AND TELECOMS



Complexity of IT infrastructure is the top driver of increased fraud risk (named by 39% of respondents)

86%

Believe exposure to fraud has increased

Base: 545 executive-level decision-makers who influence or are responsible for their company's risk and fraud strategy

Source: A commissioned study conducted by Forrester Consulting on behalf of Kroll, August 2016

Building Business Resilience

BY JORDAN STRAUSS

In March 2011, a powerful earthquake and subsequent tsunami in Japan caused a chain of events that resulted in the worst radioactive crisis since Chernobyl. Across the Pacific, and hidden from public view, a group of senior U.S. government leaders and their staff met nonstop. The day-to-day responsibilities of many of these leaders had nothing to do with crisis response. Among them were environmental lawyers, physicians, meteorologists, and policy specialists. Most knew each other by face and name, because only months earlier they had participated in a quarterly exercise that addressed a hypothetical nuclear emergency inside the United States. Many had also worked together during the BP Deepwater Horizon disaster, so when a crisis occurred, no time was lost building relationships.

While the benefit of planning ahead seems obvious, a quarter of all respondents to Kroll's 2016 Global Fraud and Risk survey have not implemented or planned preparedness measures for possible threats such as natural disasters, terrorist incidents, data breaches, or workplace disruptions.

Business readers could learn from government in this space. In planning for resiliency in the event of a crisis, there are three principles to consider:

Crisis planning is crucial for every organization and sector.

JORDAN STRAUSS
Jordan Strauss is an Associate Managing Director with Kroll's Investigations and Disputes practice. Jordan has served as a Director at the White House National Security Council, the Deputy Justice Attaché and Senior Legal Advisor to the U.S. Justice Department in Kabul, Afghanistan, and as a federal prosecutor and trial attorney with the U.S. Department of Justice. An experienced trial attorney, he was also the most senior crisis and emergency lawyer in the Department of Justice. A published author and accomplished speaker, Jordan has provided sworn testimony and led and participated in countless table-top and full-scale exercises relating to disaster preparedness and cyber attacks.

1 Think of preparedness as a process, not a state, and commit to ongoing improvement.
Strive to be more prepared tomorrow than you are today. Give careful thought to the relationships you may need in a crisis before something happens. Because the hours immediately after a crisis are the most important, it is critical to plan how such an event will influence your people and reputation. Consider moderated exercises with a cross-section of your leadership. Carefully study the fall-out from a competitor's critical incident. Those interested in building stronger enterprises should find themselves asking "what would we do if that happened to us?" There are many low and no-cost ways of conducting drills to gauge your readiness. The next time you have a "bad weather day," for example, analyze whether your employee notification system worked – assuming you have one, it's the same notification system you would use for an active shooter. Building a culture of resilience within your organization starts at the top. The CEO's commitment to corporate readiness and resilience should be visible to all employees, and one way to achieve this is to demonstrate C-suite interest in the success of things like employee alert and notification programs.

2 The most visible issue is not always the biggest risk – think hard about risk as a function of both likelihood and consequence.
Determining the likelihood of a specific event is actuarial and informed by intelligence: It is not an exercise in worrying about the most recent headlines. "Risk" is calculated as likelihood multiplied by consequences, so a deep understanding of likely consequences is critical to making risk-informed decisions. It requires substantial input from a cross-section of leadership.

For example, in addition to damaging employee morale, data breaches can also result in legal liability, regulatory problems, and severe and lasting reputational damage. In assessing the consequences of an event, all of these aspects should be included, along with the costs (consulting, legal, settlement, and public relations) of resolving it. Consideration of the transaction costs associated with crisis navigation is also critical – legal fees, public relations fees, and outside crisis management services are expensive.

Similarly, a campus sexual assault profoundly affects a school's community, damages the life of a young person, and carries a host of reputational, liability, and morale problems for the school. Advance planning that takes into account the full impact of these problems, including legal and public relations costs, can help mitigate negative impacts.

Tabletop exercises are an excellent tool for advance planning, as are guided discussions and brainstorming sessions. Capturing knowledge gained from past experiences and observing other enterprises is critical.

3 Ensure that actual risks inform resource allocation.
During the Japan disaster, U.S. government leaders worried first about life safety issues and second about collateral consequences. They made a risk-informed and defensible decision about how to spend their time, which ultimately is their most valuable resource.

Senior government leaders had access to the necessary data to make careful and crucial decisions. They were aided by multi-agency legal response teams that had learned from the Deepwater Horizon crisis. The relationships built on the margins of exercises and disaster sped up the response. There is no reason businesses should be any less prepared for an uncertain future.

Crisis planning is crucial for every organization and sector. Thus, a stadium operator or professional sports franchise dealing with a limited budget should assess the likelihood and consequences of a terrorist attack vs. an active shooter or medical emergency. They need to resource against the highest-risk event – not necessarily the highest-profile event. Risk-informed decision-making provides leaders with a logical and defensible way of triaging resources, and should be observed ahead of time – not during a crisis.

Employee Exits: Reducing the Loss of Confidential Information and Intellectual Property

BY MARIANNA VINTIADIS AND TADASHI KAGEYAMA

The plant manager of a high-tech company in Asia was eating his dinner one night and flicking through the television channels, when a news item made him choke. It was the face of one of his former engineers, working for one of the company's key competitors. The engineer had told him that he was returning to his home town to help his aging parents run their small fishing business. The plant manager went to bed that night feeling concerned. His concerns were compounded when he got to work the following morning and realized that 12 more engineers had also left to go to the same competitor.

He reached out to Kroll for help. We found that a total of 25 engineers working in design, production, and quality control had been systematically recruited by the competitor through employee networks and recruiters. These employees had taken valuable know-how, confidential engineering data, drawings, vendor lists, and process manuals with them when they left.

Many companies are waking up to the risk of valuable trade secrets and technologies being stolen or leaked through their employees. This risk is becoming particularly acute in the fast growing Asian countries. An increasingly favored route to acquiring confidential commercial or trade secrets from a competitor is by recruiting their staff.

However, in our experience, managers often ask the wrong questions. They say, "How can I stop my good employees going to my competitors?" Their questions should really be focused on "Are we doing enough to make them stay?"

The best way to retain confidential information and know-how is to treat employees well so that even when they do leave, they leave well. Any initiative that can keep employee turnover low will lead to better corporate integrity in every sense of the word. This is borne out by the Kroll survey, which shows that the most common driver suggested for the increase of fraud risk was high staff turnover, mentioned by 37% of companies.

However, even though companies may have taken rigorous steps to create a positive working culture, events can still lead to employee dissatisfaction. In Europe, for example, many companies are family owned. When there is a shift in ownership or a generational change over, the atmosphere in the company can change overnight. M&A transactions are also a cause of disgruntled employees as jobs amalgamate or disappear entirely.

MARIANNA VINTIADIS
Marianna Vintiadis is Kroll's Country Manager in Italy and is also responsible for Kroll's operations in Austria and Greece. Since taking over Kroll's Italian office, Marianna has successfully developed Kroll's local client base which today includes the country's largest corporations and financial institutions as well as its leading law firms. She has also opened Kroll's services to the Italian SME market, which forms the backbone of the Italian economy.

TADASHI KAGEYAMA
Tadashi Kageyama is a Regional Managing Director and Head of Kroll's Asia operations. Tadashi helps clients mitigate the risk of fraud, respond to regulatory and compliance violations, and resolve disputes and litigation matters. He also helps clients manage their intellectual property by providing investigative services and advice on global enforcement actions. Tadashi has over 15 years of experience conducting sensitive and complex business intelligence assignments across multiple jurisdictions.

Seven common mistakes companies make in dealing with employee-related risks of information theft are:

1 Underestimating the purpose of the exit interview.
The exit interview serves many purposes. When an employee is leaving, the employer should use the interview to assess the risk of information or IP theft. It is an opportunity to assess employee morale, and to remind the employee of the company's information and IP security and non-compete/non-solicitation policies. Gauging morale can flag whether there is a deeper malaise and the potential for more employee exits. Too often, companies underestimate the unhappiness of their employees.

2 Destroying critical evidence.
When employees leave, companies tend to reutilize computers, delete email accounts and fail to archive telephone logs. In Asia, we often deal with cases where exiting employees are allowed to keep their computer and mobile as part of the severance package. All data and devices, including company access logs and CCTV (where permitted by law), should be kept for a period of time as it can often take months to discover a breach. If employees are allowed to retain any devices, these devices must be thoroughly wiped or reset to ensure that no confidential information is left on them that could be used by the departing employee for the benefit of another business.

3 Assigning responsibility too narrowly.
Often, companies only task Information Security or Human Resources departments with assessing the threat and designing plans and policies. However, the risk should be addressed by multiple stakeholders including, Legal, IP, Marketing, the business itself, and even the CEO if the potential loss is of strategic importance, large scale or likely to result in negative publicity.

4 Allowing employees to use their own devices for company work.
With the increase in overtime, home, and flexible working, it has become more important to establish clear rules about employee devices. It is rarely, if ever, possible to investigate personal computers and mobile phones belonging to employees. We advise that clients only allow employees to work on company devices and not on personal devices. Moreover, programs and work documents should be stored on the company server at all times and not locally. It is also important to take decisions out of the employee's hands through robust policies and configurations. For example, it may be a deterrent to issue a regulation banning USB memory sticks. However, if all devices issued to staff have their USB ports deactivated, inappropriate use - whether by mistake or by design - becomes significantly more difficult.

5 Focusing on digital theft.
Too often, companies focus on the theft of digital information, but physical records are also an important conduit of loss.

6 Rewarding bad behavior.
Companies might hire an employee who brings information from a previous employer such as client lists or product information. What they fail to consider is that individuals who have behaved badly once are likely to do so again. Kroll recently worked with an engineering company whose key engineer had left and taken some important plans to the competition. During the investigation, we learned that the employee had done the same with their previous employer.

7 Neglecting the impact of an investigation.
When an employee leaves under suspicion of information theft, an ensuing investigation can damage the morale of other employees. It is important to make sure that any steps the company takes to legitimately protect its assets do not appear vindictive. People do not like to be investigated or to participate in the investigations of their colleagues. Companies often bring in external investigators to avoid the disruption of employees being investigated by their coworkers, and to ensure that the investigation is run as efficiently as possible. It is also important to keep in mind that internal investigations must be conducted in accordance with applicable law including (but not limited to) employment, data privacy, and whistle-blowing laws, if applicable, and that laws differ from country to country. An external investigator would work alongside internal or external counsel to ensure that the investigation is conducted in accordance with all applicable laws and that any evidence obtained is not compromised.

As always, prevention is better than cure. Maintaining the right culture and having the appropriate processes in place will help protect your company's most valuable assets.

Security Risks in Emerging Markets

BY NICK DOYLE AND RAFAEL LOPEZ

Today, global companies have a dual challenge when operating in emerging markets: they face heightened security risks such as terrorism, weak government institutions and public security, social unrest and corruption, and they have to deal with them with diminished local resources.

Faced with these challenges, global and local companies are concerned about their duty of care to their employees, protecting asset value for shareholders, and their legal and social obligations to the local community.

There are also significant risks to a company's reputation and "license to operate." There is civil and international scrutiny of potential human rights violations or threats to local communities. Companies may not have adequately protected themselves against identifiable risks, all of which could lead to media, industry, or investor scrutiny.

In one example, a Canadian mining company faced allegations that its security personnel in Guatemala had killed an outspoken opponent to the mine and permanently crippled another in 2009. The company denies the allegations and is still fighting the case (even though it no longer owns the mine).

In another, a company with a distribution center outside Mexico City contacted Kroll after it had been the victim of an armed robbery. Two trucks arrived in broad daylight and removed the company's most valuable inventory. Several of the bandits were tentatively identified as security guards who worked for the company. They knew their way around the facility and knew exactly what to take. After the local state police declined to investigate, it was discovered that they were the owners of the security company.

Given the difficulty of operating in unfamiliar markets, companies often turn to global security consultants for advice on how to manage these "enterprise risks." They may have experienced a serious and sudden business-critical event and urgently require advice, assistance, and support. Or they might have identified potential risks and threats in new markets or existing operations, but lack the adequate internal resources, experience, knowledge, or capability to address them.

NICK DOYLE
Nick Doyle is a Managing Director and Head of Security Risk Management in Kroll's Investigations and Disputes practice, based in the London office. Nick leads the delivery of Kroll's security offerings across EMEA. Since joining Kroll in 2008 after serving with distinction in the military and law enforcement, Nick has project managed over 350 assignments in 50 countries.

RAFAEL LOPEZ
Rafael Lopez is a Director with Kroll's Investigations and Disputes practice in Mexico. Rafael has developed tailored journey management and security programs for expatriates, and led executive protection teams in Mexico, Chile, and Venezuela. He has also conducted security awareness seminars and risk management workshops on extortion, kidnapping, and criminal activity trends. Additionally, he has conducted site security reviews throughout the U.S., México, Panamá, Guatemala, Colombia, Ecuador, and Venezuela.

By adopting an enterprise security risk management approach, companies can identify, consider, and treat vulnerabilities in a structured and holistic way. The great strength of this approach is the ability to analyze risk in context, throughout the business. It spans the physical and cyber worlds, which is essential to ensure risk is treated in a balanced and calibrated way, and to avoid false assurance or wasteful expenditure.

Enterprise security risk management in its simplest form is a means of identifying, communicating, and categorizing risks so that resources can be optimally allocated. Some risks, when understood, will be accepted. Others will require a careful deployment of skills, resources, or management supervision. Systems or measures of managing risk across an enterprise need to be embraced and continually maintained.

Ultimately, clients are the experts on their organization's activities, objectives, and capabilities. External consultants can bring knowledge and experience of how to identify and mitigate vulnerabilities. The combined result is a more effective and nuanced way to allocate resources. Companies that take a holistic approach to enterprise risk management often identify and discontinue wasteful and ineffective activities, thus saving time and money.

Case Study – Crisis Response

Kroll was called in to support a corporate advisory and restructuring firm that was dealing with a bank that eventually went into bankruptcy due to a major fraud. We dynamically assessed the risks to the bank, its employees, and the corporate team of advisors and lawyers. We established a security risk management framework that allocated resources such as crisis managers, surveillance operatives, and executive protection personnel during various stages of the project. The work involved the assessment of:

- Facility management
- Safe movement of personnel
- Oversight of the transfer of cash from branches to the central bank and the destruction of credit cards
- Building security
- Operational security of assets
- Information security
- Cyber security
- Serving of court orders
- Planning and security management for large creditor meetings

As a result, the corporate advisors were able to work effectively with the confidence that they were in a safe environment.

Data Analytics: The Needle in the Haystack Isn't Always So Hard to Find

BY ZOE NEWMAN, PETER GLANVILLE AND JOHN SLAVEK

Kroll's Global Fraud and Risk Report survey found that 44% of fraud had been discovered by a whistle-blower, while 39% had been discovered by internal audit, and 32% by management at the company. Detecting and dealing with issues before they trigger whistle-blower or regulatory procedures has clear financial, reputational, and resource benefits. How can companies stay on the front foot when combating fraud, bribery, and corruption?

Using your company's data to detect fraud, bribery, and corruption

'Data analytics' has become a buzz word in consultant speak in recent years. But there is little explanation of its practical applications for companies. At a basic level, data analytics is simply taking raw data from a company's operational and financial systems and analyzing it to draw conclusions. Most of us have been doing this for years.

The key is how to analyze the data in an efficient and effective manner to identify trends and anomalies for the end user and employ the best available tools.

ZOE NEWMAN
Zoë Newman is a Managing Director in Kroll's Investigations and Disputes practice, based in the London office. Zoë is responsible for financial investigations across the EMEA region. She has extensive experience in leading complex, cross-border forensic investigations into matters of fraud, corruption, and potential regulatory breaches, including those relating to the Foreign Corrupt Practices Act (FCPA) and UK Bribery Act. She also advises clients on how to best implement controls to mitigate these risks.

PETER GLANVILLE
Peter Glanville is a Managing Director in Kroll's Investigations and Disputes practice, based in the Hong Kong office and specializing in advising clients on forensic accounting and financial crime matters. Peter is a chartered accountant with over 15 years of experience assisting clients with contentious financial matters, including bribery & corruption and fraud investigations, contract audits, control reviews, assessments of financial crime & compliance programs, and providing expert accounting advice. Peter has worked in the UK, Europe, Asia, and Australia assisting clients across many industries.

JOHN SLAVEK
John Slavek is a CPA and Managing Director in Kroll's Philadelphia office. Since joining Kroll in 1998, John has helped clients confront a wide range of finance and accounting issues, including FCPA investigations, embezzlement, bankruptcy, contractual disputes and internal control evaluations. He also has extensive experience working on due diligence projects, investigating financial statement manipulation and quantifying potential lost profits in commercial litigation.

Historically, fraud, bribery, and corruption investigations were carried out through a sampling approach to transactions and supporting documentation. However, data analytics can now be applied to interrogate a company's financial records for red-flag transactions, to focus investigative activities.

The issue is how to interrogate this data to identify risks of bribery and corruption and to assess what constitutes a red-flag transaction.

Highly skilled data analysts are required to undertake such analyses. For instance, if millions of transactions from a company's accounting system have to be reviewed, such an analysis would not be possible using basic tools such as Excel. Experts would use more sophisticated data analytics tools such as SQL to find patterns that reveal potential wrong-doing.

How can companies use data analytics to detect fraud, bribery, and corruption?

Companies are becoming aware that the volumes of historical financial and operational records available to them can be a valuable source of supplementary data to a more proactive anti-bribery and corruption compliance program.

The issue is how to interrogate this data to identify risks of bribery and corruption and to assess what constitutes a red-flag transaction.

When this happens, we at Kroll take extracts of accounting ledgers, in some cases the entire system, and mine that data (sometimes combining it with data external to the organization) to identify questionable transactions.

This process involves highly skilled data analysts, but most importantly we apply a suite of queries developed over years of conducting such investigations. These are designed to quickly identify transactions and relationships that display the attributes of a fraudulent or corrupt payment. The queries are supplemented with company or industry-specific queries in order to identify other potentially suspicious transactions.

Not every red-flag transaction is problematic. The purpose of the exercise is to highlight unusual trends, customer or supplier relationship patterns, or specific payments that the business can explore and investigate further. While some may be justified, others represent a cause for concern.

This risk-based approach delivers cost and time efficiencies, enabling the company to manage the process and outcome. If an issue is identified, the company can investigate and assess it, seek advice, and proactively take control of the situation – a far preferable environment than an out-of-the-blue whistle-blower email or letter from a regulator.

What are the current trends and best practices, and how is this practice evolving?

Bribery and corruption risk remains one of the greatest concerns to businesses. Kroll's survey identified that 23% of respondents were dissuaded from doing business in foreign markets due to the perceived risk of bribery and corruption. However, by completely discounting overseas markets, potentially significant opportunities can be missed.

Bribery and corruption risk can be managed, with the right controls and an effective compliance program in place. Corporate functions are getting smarter about how they identify and manage such risks. This is reflected in the proactivity with which they take on risk assessments and embed third-party due diligence programs, to gain further insight into the history of a third party's relationship with the company.

Are perpetrators of fraud becoming more sophisticated at covering their data trails?

As companies get smarter at managing bribery and corruption risk, so do the wrong-doers. They are aware that due diligence will be conducted on third parties and agents, and find creative ways to accept bribes and other corrupt payments.

Five years ago, suspicious transactions were relatively easy to spot. They included:

- Offshore registered vendors
- Bank accounts in red-flag jurisdictions
- One-off, round sum payments
- Transactions recorded in consultant expense general ledger accounts

Wrong-doers are aware that these are typical red flags. Now, Kroll sees far more creative ways to disguise payments, including:

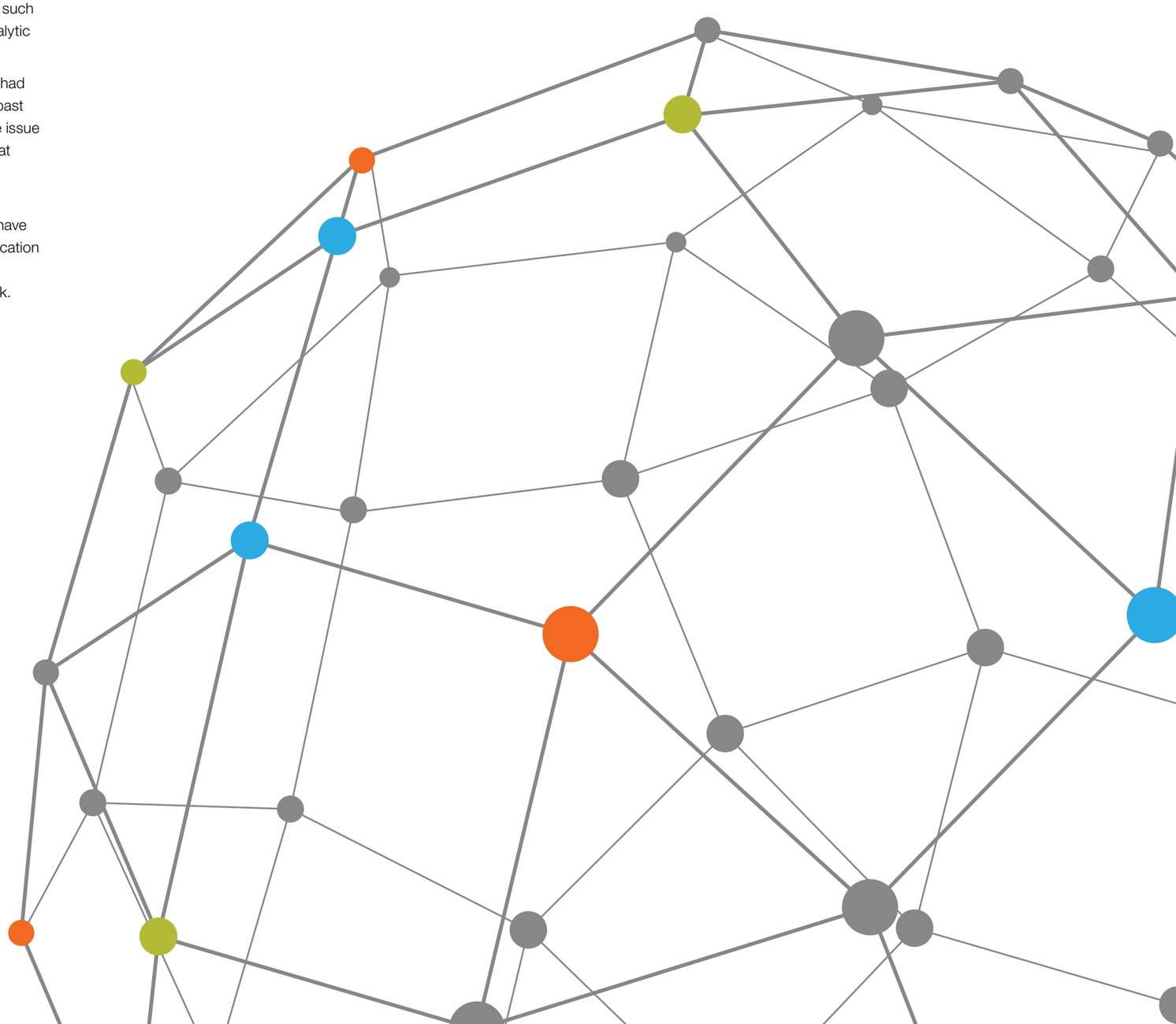
- Empty invoicing to known third parties, in order to build a slush fund
- Above-average discounting to customers and distributors
- The provision of rebates resulting from invoicing excessive amounts for goods delivered
- Well-known and trusted third parties such as travel agents are being encouraged to act as intermediaries

The good news is that these disguises are identifiable when using data analytics techniques.

Take a supplier relationship in a subsidiary with which business suddenly increases 20-fold in the last two years out of ten. Corporate head office internal audit, compliance, and finance functions won't necessarily notice such trends in their day-to-day business. But such an anomaly is easily flagged when applying data analytic techniques across the group's accounting data.

Only 15% of respondents to Kroll's survey said they had suffered bribery and corruption related fraud in the past 12 months. However, unlike other types of fraud, the issue is that most corporate organisations aren't aware that such payments have occurred, until it's too late.

In the majority of Kroll's investigations, the relevant payments often relate to an acquired subsidiary, or have taken place many years previously. Proactive identification of such risks using data analytics means these transactions do not need to be needles in a haystack.



Responding to Whistle-blower Allegations

BY ALEX VOLCIC AND YASER DAJANI

Companies rely on information from whistle-blowers as one of the key methods of fraud detection. The latest Kroll Global Fraud and Risk Report survey showed that 44% of identified fraud was reported by an internal whistle-blower. Given that 79% of fraud involved current, former, or temporary employees, internal staff are a key line of defense in the fight against fraud. It is therefore surprising that a relatively large number of respondents with whistle-blower programs already in place (36%) do not intend to revise, modify, or expand them in the next 12 months.

The *Princeton Dictionary* defines "whistle-blower" as "[a]n informant who exposes wrongdoing within an organization in the hope of stopping it." However, there is no consistent definition of the term in the corporate world. Depending on the definition of "whistle-blower" within a company's policies, an internal whistle-blower at one organization may not be considered a whistle-blower at another organization. It is therefore important for companies to have the term clearly defined in their policies.

Companies are inundated with advice on how to set up whistle-blower hotlines, and their reactions to allegations of wrongdoing vary widely. Many companies grapple internally about which function should handle whistle-blowing reports. Unfortunately, there are no uniform standards for handling these allegations, which means the crucial initial triaging phase isn't always managed in the most effective way.

The initial response to whistle-blower allegations is critical, and many things can (and do) go wrong at this stage. For example, in a recent Kroll investigation in the UAE, a CEO wanted to immediately, and personally, interview the alleged wrong-doer after being informed of an allegation. Fortunately, after discussions with the Kroll team, the client heeded our advice and decided against this approach. Interviewing a suspect before all facts are known risks giving the game away and possibly alienating a potentially loyal and innocent employee.

The first 24 hours after a whistle-blower comes forward are critical. A senior response team should be formed, comprised of individuals who are not directly associated with the employee whose conduct has been questioned. Companies need to have policies and procedures in place to respond to allegations through set mechanisms, which should be flexible enough to allow for rapid escalations of truly material matters. A swift response can also help limit financial and reputational damage and, where appropriate, recover or avoid losses.

ALEX VOLCIC
Alex Volcic is a Managing Director, and head of Kroll's Moscow office. Alex leads the firm's Russia and CIS team and serves clients across Central and Eastern Europe as well as the Nordics. He manages a wide range of investigations for corporates and financial institutions, and their advisers, including pre-transactional due diligence, background investigations, market entry studies, internal corruption and bribery investigations, forensic accounting, compliance-driven third party screenings, and asset traces.

YASER DAJANI
Yaser Dajani is a Managing Director in Kroll's Dubai Office and Head of the Middle East region. He manages investigations for regional and international businesses and government clients, and oversees a team of forensic investigators and business intelligence specialists in the Dubai office. Yaser's core areas of expertise include complex business intelligence, internal investigations, dispute advisory, litigation support, and asset tracing, anti-counterfeit support and corruption risk assessments.

The initial evaluation should assess the credibility and gravity of the alleged issues. It is key to establish these factors before launching a full investigation.

Allegations are frequently difficult to verify due to insufficient information being provided by the whistle-blower. For example, a whistle-blower may allege that a procurement manager has taken cash from suppliers, but it may be difficult to prove that a "brown envelope" has been given to the manager. In one such case, email analysis successfully showed wrong-doing, but was unable to corroborate the specific accusation of kickbacks. This case was further complicated by another common feature: the whistle-blower was seriously underperforming and was not a credible or well-intentioned witness.

Sometimes, whistle-blowing allegations simply cannot be substantiated, making it very difficult to ascertain whether the whistle-blower is acting in good faith. Kroll recently investigated a whistle-blower who was considered to be a credible and well-respected source by senior management. The individual was convinced that a sales manager was colluding with a key distributor. However, a thorough analysis of the alleged wrong-doer's lifestyle revealed nothing out of the ordinary and a forensic review of emails did not disclose any evidence of impropriety.

It is important to think about the following questions when triaging or assessing allegations:

- How specific are the facts in the allegations?
- How serious are the consequences, if the allegations are true?
- How full and frank is the disclosure of the whistle-blower?
- Is it helpful to have a third party assess credibility for the record?
- How do these allegations fit with other whistle-blower allegations?

If an investigation is deemed necessary, it is vital to execute it in phases and, where possible, conduct a covert credibility assessment first. After the data has been analyzed, appropriately qualified personnel can start to conduct fact-finding interviews with individuals who may know about the alleged wrongdoing. Typically, interviews with a suspected wrong-doer are the final step.

Investigating whistle-blower allegations is often complex; it is crucial that the credibility of the whistle-blower is examined as part of the process, as their allegations may be without merit.

To further complicate the investigation process, even where a company has invested in resources to encourage staff to speak up and use whistle-blower hotlines, some cultures have a negative view of whistle-blowing. For example, employees in Russia and other countries may be hesitant to come forward.

Whistle-blowers often choose to remain anonymous when making a report due to cultural reasons, fear of retaliation by their peers or the company, or for other reasons altogether. Despite legal protections, in some jurisdictions the consequences for genuine whistle-blowers are often severe and long-lasting. Although companies need to maintain whistle-blowers' right to remain anonymous, this anonymity generally makes investigations more difficult.

Corporate culture is an important part of creating an environment in which employees feel free to raise an issue without fear of retaliation. Companies are encouraged to include anti-retaliation language in their policies and to inform their employees that no form of retaliation will be tolerated for any report made in good faith. Our investigations have repeatedly revealed that a key issue for employees deciding whether to come forward is whether they have confidence in their company's internal whistle-blower process.

Building an Incident Response Plan: How Will You Respond to a Cyber Attack?

BY ANDREW BECKETT, MICHAEL QUINN AND LUCIE HAYWARD

Kroll's latest Global Fraud and Risk Report survey revealed that, while 85% of respondents said they had suffered a cyber attack in the last year, the adoption of internal cyber security policies and procedures to combat the risk is shockingly low. Only 36% of executives surveyed said their company has implemented internal policies and procedures and has plans to expand. An additional 38% have implemented such policies and procedures, but they have no plans to expand. 25% have not implemented internal policies and procedures at all.

Policies and procedures are important because they are an organization's articulation of what it expects from its employees. Having them in place means employees have somewhere to look for guidance on what they should (and should not) be doing. For example, what information can they share on social media? What should they do if they receive a phishing email or notice suspicious network activity?

Kroll's findings are supported by a September 2016 report from Lloyds of London on cyber risk[1], which reported that 92% of European companies have been breached in the last five years, but only 42% were worried about it happening again. Earlier this year, the UK Government Cyber Security Breaches survey[2] found that 69% of UK businesses say cyber security is a high priority, but far less consider it an actionable priority. Only 29% had written cyber security policies, and a mere 10% had an incident response plan (IRP).

ANDREW BECKETT
Andrew Beckett is a Managing Director in Kroll's Cyber Security and Investigations practice, based in the London office. Throughout a distinguished career that has bridged both government service and private enterprise, Andrew has excelled at developing and implementing cyber, information assurance and incident response solutions for the most complex of organizational needs. His strong skills in business management, analytics, knowledge management, and project management complement his technical expertise, ensuring a pragmatic approach to the complex cyber-related challenges that companies now face on a daily basis.

MICHAEL QUINN
Michael Quinn is an Associate Managing Director in Kroll's Cyber Investigations practice. He joined Kroll from the Federal Bureau of Investigation (FBI), where he most recently served as a Supervisory Special Agent in the Cyber Division. Michael managed a variety of state-sponsored and criminal intrusion matters for several FBI field offices and was responsible for some of the first-ever indictments against state-sponsored cyber attackers.

LUCIE HAYWARD
Lucie Hayward is a Managing Consultant with Kroll's Cyber Security and Investigations practice in Nashville. Lucie manages incident response, forensics, and consulting projects for clients, and additionally helps clients proactively validate and test their plans through tabletop exercises. She has wide-ranging experience in project management, security administration, security awareness and training, and incident response.

1 Lloyd's 'Facing the Cyber Risk Challenge' survey, http://bit.ly/2cPV5jo
2 Cyber Security Breaches Survey 2016, http://bit.ly/1T4MveX

IRPs are a crucial component of the fight against cyber crime. They are a company's first port of call in the event of an attack. The good news is that building one that includes both internal and external players and their various roles does not have to be an arduous task.

Companies should consider building seven important steps into their IRPs:

1 Determine authority to declare an incident. Designate an individual who has the authority to declare an incident, invoke the IRP, and convene the response team.

2 Assign team responsibilities. Clearly outline all team roles in the plan so that if an incident occurs, it makes tough decisions easier to make. Choose external advisers in advance and include them in the plan. Having to build those important trust relationships for the first time during a crisis is not ideal.

3 Avoid assigning severity levels. It may initially seem helpful to describe categories of severity, but the risk of mislabeling an incident is too great. Companies are encouraged to consider each incident as a top priority.

4 Establish communication procedures and responsibilities. Determine who will deal with external and internal stakeholders and how the information will flow. For example, where will the team meet? In a breach situation, it is important to establish the timeline of the incident and know the scale of the breach before setting the communication plan in motion. Overestimating the scale of the damage could lead to unnecessary panic. Underestimating it might cause additional harm, for example if passwords are not changed before criminals gain access to accounts. In both cases, rushing to make inaccurate statements is likely to have severe repercussions.

5 Gather pertinent information in advance. Where possible, compiling critical information before an incident is very helpful. Basic details such as the contact numbers of all incident response team members are critical, as incidents often happen outside of business hours.

6 Outline the process. Teams naturally want to solve the problem when they find it. However, this "dwell" time can be hurtful to an organization and impede the process. We suggest that all the steps — from when the team is convened to the escalation point — are clearly outlined as a robust process. It is important for IT and security teams to know the process by heart.

7 Review and test the plan. We recommend quarterly reviews and updating as needed. These are good opportunities to update the contact numbers and pay attention to changes in technology or policies that might affect the IRP.

Having an IRP in which all critical stakeholders understand the lifecycle of an incident and have rehearsed it at all levels of the business, including the boardroom, goes a long way towards being prepared to mitigate the damage of an attack.

Data Breach Response: Seven Guidelines for Regaining Customer Trust After a Breach

BY BRIAN LAPIDUS

Your organization works hard to produce an outstanding product or service. You go the extra mile to give customers a great experience. You're always looking ahead to what you can do better. And then a data breach hits. Maybe someone on the team loses a laptop or device that is loaded with customer data. All that good will and trust built on your performance is at risk of evaporating before your eyes.

You wouldn't be alone. More than 85% of respondents to Kroll's 2016 Global Fraud and Risk survey said they had been a victim of a cyber attack in the past 12 months. Equally troubling, 67% also indicated that the event had a significant negative impact on their organization's reputation.

There may never be a more critical time to focus on your customers' needs than in the aftermath of a data breach. A careful response that incorporates the following seven guidelines will help regain your customers' trust, rebuild confidence, and ultimately strengthen the relationship.

1 Notify in a timely, but responsible, manner. If you have complete certainty about the scope and nature of the compromised data, you should move swiftly. Customers expect you to inform them as soon as you know. However, it is counterproductive to underreport and have to follow up with additional disclosures, or to distress customers with false alarms. It's better to investigate with urgency and then notify as necessary. For example, a Kroll client had 35 laptops stolen, and initially believed data for 2 million people had been compromised. Our investigation proved that data for only 1,500 customers had been taken.

2 Build credibility. Be sure to cleanse your data; sending multiple notifications to an individual can cause them to question your overall ability to manage their data. Your credibility can be at stake in many other ways. Kroll worked with one company that spent several months chasing the "best deal" from numerous vendors to handle the various components of a large breach. While the ultimate response covered all regulatory bases, the company suffered considerable criticism for its slow actions and eventually settled a related class-action suit. It had conveyed a message that saving money was more important than protecting its customers.

3 Customize your communications for segments of the affected population. While it is tempting to set up a one-size-fits-all solution and get letters out, take the extra step to fully understand the impacted population and address any special needs. For instance, Kroll had a client whose affected customers included individuals for whom Korean was their native language. Accordingly, not only were their notification letters written in Korean, but the call centers were also staffed with Korean translators.

4 Demonstrate empathy. Be careful to tailor your message for the unique characteristics or circumstances of the affected groups. This approach is especially critical if your organization serves individuals who are simultaneously dealing with grave personal challenges or losses, for example terminally ill patients and their families who might be affected by a hospice breach.

5 Provide relevant, useful services and guidance. Identity theft will be a valid concern for your customers, so be prepared with services that match their risks. For example, a recent client lost the credit card numbers, user names, and passwords of its customers. In addition to credit monitoring services, the client offered non-credit monitoring, which searched the dark web for instances where those numbers were being sold, an indicator that these consumers were in danger of someone using their information. In another case where a client lost Social Security numbers (SSNs) belonging to minors, Kroll's licensed investigators consulted with parents to show them how to put a credit freeze on their children's SSNs. Otherwise, illegal activity on the minor's SSN could go undetected until the child turned 18, when he or she might apply for student loans or a credit card.

6 Create a consistent customer experience. Recently, one of our clients inadvertently disclosed personally identifiable patient information, including medical diagnosis data, medication records, and medical history. The incident was abhorrent to the CEO, who recognized that it ran counter to the organization's core values. The client committed to train each Kroll call center, ensuring our team could express that cultural value to the individuals calling. Remember, the experience you provide during a breach can define how your customers feel about your organization for many years to come.

7 Anticipate competitors' behavior. Competitors know that you are most vulnerable to losing customers in the aftermath of a data breach. Consider setting up teams to anticipate and monitor the promotional activities of your competitors at this time, and then create plans to preempt or counter them. Likewise, you may want to consider offering your own special promotions, such as free services, discounts, or coupons to encourage your customers to stay.

The process of rebuilding trust with customers after a data breach is a multifaceted, long-term endeavor. But don't wait until an incident strikes to put these seven steps into action. Much of the work involved in each step can be accomplished in advance, putting you in a stronger position to weather the storm, and rapidly earn back your customers' trust.

BRIAN LAPIDUS
Brian Lapidus is managing director and leader of Kroll's Identity Theft & Breach Notification group. In addition to helping business clients resolve issues resulting from a data breach, Brian's practice is engaged in consumer-level service and remediation in the wake of such an event. He expanded Kroll's individual identity theft restoration footprint in 2007 when he launched the program in Canada. His group is particularly attuned to solutions for healthcare, higher education, retail, and financial entities. With over 15 years of experience, Brian is recognized as a noted content authority, and has contributed articles and been featured in interviews in online and print publications.

Canada Overview

FRAUD

Over the past year, nearly a quarter (23%) more respondents in Canada reported being affected by fraud compared to 2015. The number of respondents in Canada (88%) impacted by fraud this year is 6 percentage points above the global average of 82%.

Perpetrators of fraud incidents in Canada were most likely to be insiders. In particular, senior and middle management were more likely to be responsible for fraud incidents in Canada than in other regions, at 17 percentage points above the reported global average of 30%. Junior employees were named as key perpetrators in 39% of fraud incidents in Canada, equal to the reported global average. They are the second most common perpetrator in the country after senior or middle management.

This theme continues when considering the types of fraud committed. Out of all countries surveyed, only participants from Canada mentioned misappropriation of company funds as one of the top five types of fraud experienced in the past 12 months. Respondents from Canada had above-average mentions for physical theft of stock or assets at 34% (5 percentage points above the reported global average of 29%), as well as data theft at 32% (8 percentage points above the reported global average of 24%).

A large majority (90%) of respondents in Canada had invested in a risk officer and risk management system (12 percentage points above the reported global average of 78%). A further 88% had invested in management controls (14 percentage points above the reported global average of 74%). Overall, more participants from Canada had invested in anti-fraud measures than the reported global average.

CYBER SECURITY

The majority (85%) of respondents in Canada suffered a cyber incident, in line with the reported global incidence average of 85%. Virus/worm attacks were a significant issue: 41% of participants from Canada reported this type of incident, 8 percentage points above the global average of 33%. Lost equipment containing sensitive data was also an issue for executives from Canada, with this incidence reported at over twice (39%) the global average of 17%.

The targets of cyber attacks were primarily customer records and companies' R&D and trade secrets. Over half the participants from Canada reported attacks on customer records (57%), physical assets/money (57%), and trade secrets (51%). The most common perpetrators of cyber incidents in Canada were permanent employees which at 20% was twice the reported global average of 10%.

In the event of a cyber incident, respondents in Canada most commonly turned to an incident response firm or an IT service vendor.

SECURITY

Surprisingly, participants from Canada were more likely to report security incidents, at 10 percentage points above the reported global average of 68%. Just under half (49%) of respondents in Canada said they had experienced a theft or loss of intellectual property. Ex-employees were mentioned as the most common perpetrators by 28% of Canadian participants.

Respondents in Canada also reported a significant degree of exposure to environmental risks (46%), which is above the reported global average of 27%.

In terms of security incidents, participants in Canada feel most vulnerable to workplace violence and environmental risks, even though workplace violence was not reported in the top three incidents experienced.

CANADA REPORT CARD

Top responses given by survey respondents.

			Global avg.
Fraud	**88** Percentage of respondents affected by fraud in the past 12 months.	▲ 23% points above 2015 ▲ 6% points above global average of 82%	
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	**34%**	29%
	Information theft, loss, or attack *(e.g., data theft)*	**32%**	24%
	Regulatory or compliance breach	**32%**	21%
	Vendor, supplier, or procurement fraud	**32%**	26%
	Misappropriation of company funds	**32%**	18%
MOST COMMON PERPETRATORS	Senior or middle management employees of our own company	**47%**	30%
	Junior employees of our own company	**39%**	39%
	Freelance/temporary employees	**36%**	27%
	Ex-employees	**36%**	27%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	**36%**	27%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Risk *(risk officer and risk management system)*	**90%**	78%
	Management *(management controls, incentives, external supervision such as audit committee)*	**88%**	74%
	Information *(IT security, technical countermeasures)*	**86%**	82%
	Assets *(physical security systems, stock inventories, tagging, asset register)*	**86%**	79%
	Partners, clients, and vendors *(due diligence)*	**85%**	77%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	**44%**	44%
Cyber Security	**85** Percentage of respondents that experienced a cyber incident in the past 12 months.	= equal to global average of 85%	
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm attack	**41%**	33%
	Lost equipment with sensitive data	**39%**	17%
	Data deletion or corruption by malware or system issue	**34%**	22%
	Data breach resulting in loss of IP/trade secrets/R&D	**34%**	19%
MOST COMMON PERPETRATORS	Permanent employees of our own company	**20%**	10%
MOST COMMON TARGET	Customer records	**57%**	51%
	Physical assets/money	**57%**	38%
	Trade secrets/R&D/IP	**51%**	40%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Incident response firm	**20%**	14%
	IT service vendor	**20%**	27%
Security	**78** Percentage of respondents that experienced a security incident in the past 12 months.	▲ 10% points above global average of 68%	
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	**49%**	38%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**46%**	27%
	Geographic and political risk *(i.e., operating in areas of conflict)*	**27%**	22%
MOST COMMON PERPETRATORS	Ex-employees	**28%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	**32%**	27%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**29%**	20%
	Terrorism, including domestic and international events	**24%**	18%

United States Overview

FRAUD

80% of respondents in the U.S. experienced fraud in the past 12 months, an increase of 5 percentage points on the previous year. This figure is 2 percentage points below the reported global average of 82%.

Intellectual property (IP) theft, piracy, or counterfeiting is a clear threat to companies in the U.S., which was reported by just over a quarter (27%) of U.S. participants, almost twice the reported global average. The U.S. was the only country where IP theft was the most common type of fraud reported. Information theft, loss, or attack was the second most mentioned type of fraud impacting companies in the U.S., followed by conflicts of interest in the management team.

The main perpetrators of fraud were reported to be insiders. Where fraud had been discovered, 36% of executives in the U.S. reported that junior employees were responsible, and 32% named senior or middle management.

Respondents in the U.S. were most likely to have adopted IT security measures, followed by financial controls and asset security as their top three ways to mitigate fraud risk.

In the U.S., the most common way fraud was detected was not through a whistle-blower, as it was for most of the other countries surveyed, but through an internal audit. Nearly half (49%) of U.S. participants said it was the most common detection mechanism.

CYBER SECURITY

Respondents in the U.S. were particularly susceptible to cyber incidents, with the majority (88%) reporting incidents in the last 12 months.

These predominantly stem from virus and worm attacks and data deletion or loss from system issues, both experienced at above-average rates by U.S. participants. To a lesser extent, one in five companies responding from the U.S. reported email-based phishing attacks, which was below levels reported globally.

The most common U.S. target, similar to other countries, was customer records, cited by 57% of participants. Trade secrets and company or employee identities were also common targets in the U.S.

Companies in the U.S. were the most likely of all countries surveyed to go straight to their IT service vendor in the event of an attack (43% of participants compared to a reported global average of 27%).

SECURITY

Security incidents in the U.S. were less prevalent than other countries surveyed, with the exception of Brazil. A majority of executives in the U.S. had experienced some kind of incident in the past year (58%), which is 10 percentage points below the reported global average of 68%. The most common security incident reported by U.S. respondents was the theft or loss of intellectual property, followed by environmental events and workplace violence.

Unusually, competitors and random individuals or organisations were cited as the most likely perpetrators of security incidents by U.S. participants. The U.S. was the only country where random perpetrators were mentioned as one of the top two culprits, and the only country other than China where competitors were mentioned in the top two.

Significantly, fewer respondents in the U.S. reported feeling vulnerable to all the major types of security risks listed than participants based in other countries.

UNITED STATES REPORT CARD

Top responses given by survey respondents.

Fraud

80 — **Percentage of respondents affected by fraud in the past 12 months.**

▲ 5% points above 2015

▼ 2% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	IP theft *(e.g. of trade secrets)*, piracy, or counterfeiting	**27%**	16%
	Information theft, loss, or attack *(e.g., data theft)*	**24%**	24%
	Management conflict of interest	**24%**	21%
MOST COMMON PERPETRATORS	Junior employees of our own company	**36%**	39%
	Senior or middle management employees of our own companys	**32%**	30%
	Ex-employees	**30%**	27%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	**21%**	26%
	Freelance/temporary employees	**17%**	27%
	Customers	**17%**	19%
MOST COMMON ANTI-FRAUD MEASURES	Information *(IT security, technical countermeasures)*	**91%**	82%
	Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	**86%**	77%
	Assets *(physical security systems, stock inventories, tagging, asset register)*	**85%**	79%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	**49%**	39%

Cyber Security

88 — **Percentage of respondents that experienced a cyber incident in the past 12 months.**

▲ 3% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	**42%**	33%
	Data deletion or loss due to system issues	**26%**	24%
	Email-based phishing attack	**21%**	26%
MOST COMMON PERPETRATORS	Ex-employees	**19%**	20%
MOST COMMON TARGET	Customer records	**57%**	51%
	Trade secrets/R&D/IP	**38%**	40%
	Company/employee identity	**38%**	36%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor	**43%**	27%

Security

58 — **Percentage of respondents that experienced a security incident in the past 12 months.**

▼ 10% points below global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	**30%**	38%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**21%**	27%
	Workplace violence	**15%**	23%
MOST COMMON PERPETRATORS	Competitors	**21%**	12%
	Random perpetrator	**21%**	10%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	**18%**	27%
	Theft or loss of IP	**12%**	19%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**9%**	20%

Foreign Investment in the US: How Best to Get Government National Security Approval

BY DANIEL J. ROSENTHAL

According to public reporting, in January 2016, Phillips's deal to sell its lighting business to Chinese buyers was blocked by the Committee on Foreign Investment in the United States (CFIUS), a multi-agency U.S. government body that evaluates inbound foreign investments that create foreign control of U.S. entities to determine whether they pose any national security risks to the United States[1]. CFIUS has the authority to take various actions that can impose significant costs on businesses. For example, it can block proposed mergers and acquisitions, order the divestment of assets acquired by foreign companies in deals that have already been closed, and direct the transacting parties to take other steps to mitigate any risks that it determines could arise in connection with the transaction.

Over the past year, CFIUS has been at the center of several large and high-profile international bids for investments in the United States. In August 2016, for example, it reportedly approved the US$43 billion bid by China National Chemical Corporation to purchase seed giant Syngenta AG. Congress has also entered the fray. Members have publicly called for legislation to extend CFIUS's mandate and expand the legal standard it uses to evaluate national security risks in ways that would potentially make it more difficult for deals to gain CFIUS approval.

These trends have increased the regulatory risk that foreign investors face in the United States. However, we feel that companies should not be dissuaded from investing in the United States and should instead embrace the CFIUS process.

DANIEL J. ROSENTHAL
Daniel ("DJ") Rosenthal is an Associate Managing Director in Kroll's Investigations and Disputes practice, based in the Washington, D.C. office. DJ's unique background of service with the White House, U.S. Department of Justice, the Intelligence Community, the U.S. judicial system, and private law practice gives him an invaluable perspective from which to assist Kroll's global clients on complex risk-related matters, including CFIUS reviews, cyber security, internal investigations, and privacy concerns.

In our experience, there are steps that investors can take to help them gain CFIUS approval. These include:

1 Be proactive. While the government's concerns are not always foreseeable to the parties, in many cases the issues are knowable. Both the acquiring company and the target entity should engage in a concerted due diligence exercise, focusing on the types of issues of greatest concern to CFIUS, such as the technical sensitivity of the products and knowledge base of the U.S. target and the backgrounds, reputations, and level of ties to foreign governments of the contemplated acquirer. Being proactive helps all parties identify any potential concerns the deal might face under CFIUS review. The parties are then better informed to decide whether to pursue the deal and, if so, whether to file with CFIUS.

2 Be transparent. With better information about the issues that CFIUS is likely to focus on during its review, the parties are empowered to be fully transparent with the committee about any identified issues that may be of interest or concern to it. Doing so will provide the parties with two concrete benefits:

- Being transparent sends a clear message to CFIUS that the genuine focus of the companies is to pursue a business venture, and that they are absolutely committed to working with CFIUS, not against it, as it undertakes a national security review of the transaction.
- Through early transparency, the parties to the transaction can be proactive in discussing with the committee ways to mitigate the issues they have identified. Far too often, negotiations with the committee become hurried as the statutory deadlines for a CFIUS decision approach. Early transparency affords the companies involved and CFIUS invaluable negotiating time to find a way forward that addresses the committee's concerns and is acceptable from a business operations perspective.

3 Be collaborative. Where CFIUS concerns relate to the exchange of sensitive information or product know-how from the U.S. target to the foreign investor, the committee may impose (1) certain protocols and protections that essentially isolate the U.S. information from the foreign entity and (2) the creation of auditable records regarding compliance with those protocols and protections.

Given the committee's lack of direct insight into the business operations of the parties, its proposed mitigation terms could be difficult to implement from efficiency and cost perspectives. Parties that anticipate CFIUS's concerns and proactively offer well-conceived and auditable mitigation options to the committee can demonstrate their singular focus on the success of the transaction and willingness to adopt measures to satisfy U.S. government national security concerns. More importantly, doing so allows the parties to set a baseline to begin discussions with the committee. It's better to work from your draft than from theirs. And CFIUS will appreciate the head start.

1 All statements of fact, opinion, or analysis expressed are the author's alone and do not necessarily reflect the official positions or views of the Department of Justice (DOJ) or any other U.S. government agency. This article has been reviewed by DOJ to prevent the disclosure of classified or otherwise sensitive information.

Middle East Overview

FRAUD

Respondents based in the Middle East reported the highest increase in fraud over the past 12 months of all regions surveyed. Over a quarter (26%) more respondents said they had experienced fraud compared to 2015. Overall the incidence of fraud in the Middle East was 6 percentage points above the global average of 82%.

Internal financial fraud was named as the most common type of fraud experienced by respondents in the Middle East. This was followed by the theft of both physical and information assets, the incidence of which were approximately in line with the global averages of 29% and 24%, respectively.

Senior or middle management were named as the most common perpetrators of fraud in the region, cited by 36% of respondents in the Middle East, followed by junior employees, cited by 34%. Third party entities were also considered to have significant roles in most fraud incidents, with joint venture partners, vendors, suppliers, and agents named by around a quarter of participants.

Respondents in the Middle East were most likely to have implemented information-related anti-fraud measures, such as IT security and technical countermeasures (80% of participants), followed by staff training (70%), the appointment of a risk officer and risk management system (68%), and staff background screening (68%).

CYBER SECURITY

The majority (90%) of Middle East participants reported a cyber incident, which was 5 percentage points above the global average of 85%.

Virus and worm infestations and data deletion due to system issues were the most common types of cyber incident. Above-average levels of lost equipment with sensitive data were reported in the region: 28% of participants compared to the global average of 17%.

The key target of a cyber attack was reported to be physical assets and money (47% of all participants). Customer records were mentioned third in the list of common targets. Similar to other regions, respondents in the Middle East were more likely to turn to their IT service vendors in the event of an incident.

SECURITY

Respondents in the Middle East were more likely to experience a security incident than in other regions. The majority (82%) of companies reported an incident, which was 14 percentage points above the global average. The most common incident was theft or loss of IP, reported by 38% of participants in the region.

When asked to name the key perpetrator of security incidents experienced in the past 12 months, 24% cited permanent employees, which was 7 percentage points above the global average of 17%.

Workplace violence was the second most likely cause of a security incident, and respondents felt most vulnerable to this type of security risk.

MIDDLE EAST REPORT CARD

Top responses given by survey respondents.

Fraud

88 — **Percentage of respondents affected by fraud in the past 12 months.**

▲ 26% points above 2015

▲ 6% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Internal financial fraud *(manipulation of company results)*	**30%**	20%
	Theft of physical assets or stock	**26%**	29%
	Information theft, loss, or attack *(e.g., data theft)*	**24%**	24%
MOST COMMON PERPETRATORS	Senior or middle management employees of our own company	**36%**	30%
	Junior employees of our own company	**34%**	39%
	Joint venture partners *(i.e., a partner who provides manufacturing or other business function, or a franchisee)*	**30%**	23%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	**27%**	27%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	**23%**	26%
MOST COMMON ANTI-FRAUD MEASURES	Information *(IT security, technical countermeasures)*	**80%**	82%
	Staff *(training, whistle-blower hotline)*	**70%**	76%
	Staff *(background screening)*	**68%**	74%
	Risk *(risk officer and risk management system)*	**68%**	78%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	**50%**	44%

Cyber Security

90 — **Percentage of respondents that experienced a cyber incident in the past 12 months.**

▲ 5% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	**30%**	33%
	Data deletion or loss due to system issues	**30%**	24%
	Lost equipment with sensitive data	**28%**	17%
	Email-based phishing attack	**28%**	26%
MOST COMMON PERPETRATORS	Accidental placement of sensitive data that was indexed by a search engine *(e.g., Google)*	**22%**	10%
MOST COMMON TARGET	Physical assets/money	**47%**	38%
	Trade secrets/R&D/IP	**42%**	40%
	Customer records	**38%**	51%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor	**24%**	27%

Security

82 — **Percentage of respondents that experienced a security incident in the past 12 months.**

▲ 14% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	**38%**	38%
	Workplace violence	**32%**	23%
	Geographic and political risk *(i.e., operating in areas of conflict)*	**32%**	22%
MOST COMMON PERPETRATORS	Permanent employees of our own company	**24%**	17%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	**28%**	27%
	Environmental risk *(including damage caused by natural disasters such as floods)*	**24%**	20%
	Theft or loss of IP	**22%**	19%

Italy Overview

FRAUD

Despite a 3 percentage point increase in exposure since 2015, the incidence of fraud reported by respondents in Italy was below the global average at 77%.

The three most reported instances involved the theft of physical assets (34%) or of information (26%), along with regulatory and compliance breaches (26%).

The reported perpetrators of fraud in Italy were varied. Junior employees were considered key culprits by half of the executives in Italy surveyed, but interestingly, customers were also frequently mentioned in just over a fifth of incidents (22%).

The most common anti-fraud measures implemented by respondents in Italy were to secure physical assets (83%), engage the board of directors in cyber security policies and procedures (72%), conduct due diligence on partners and vendors (70%) and set up better IP monitoring (68%).

CYBER SECURITY

Respondents reported fewer cyber incidents in Italy than the global average of 85%, although the incidence is still high at 79%.

The most common challenge for respondents in Italy suffering a cyber incident was data deletion by a malicious insider, followed by email-based phishing attacks and a virus or worm attack. Survey participants from Italy reported the highest incidence of data deletion by malicious insiders out of all regions covered, at 30%.

Another variance in the data from Italy shows that money or physical assets were the most likely target of a cyber attack – customer records were more frequently targeted in other jurisdictions. Respondents in Italy said in the event of an attack, their first call would be to a webhosting provider. Similar to other jurisdictions, the most common perpetrators of cyber attacks were ex-employees, named by 24% of participants.

SECURITY

Executives in Italy said their company had suffered security incidents over the past 12 months, equal to the global average of 68%. The theft or loss of IP was the most common incident, cited by 43% of participants, followed by environmental incidents and workplace violence.

Respondents in Italy felt most vulnerable to workplace violence and theft or loss of IP.

ITALY REPORT CARD

Top responses given by survey respondents.

			Global avg.
Fraud	**77** Percentage of respondents affected by fraud in the past 12 months.	▲ 3% points above 2015 ▼ 5% points below global average of 82%	
MOST COMMON TYPES OF FRAUD	Theft of Physical Assets or Stock	**34%**	29%
	Information theft, loss or attack *(e.g., data theft)*	**26%**	24%
	Regulatory or compliance breach	**26%**	21%
MOST COMMON PERPETRATORS	Junior employees of our own company	**50%**	39%
	Ex-employees	**36%**	27%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	**33%**	26%
	Senior or middle management employees of our own company	**31%**	30%
	Customers	**22%**	19%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Assets *(physical security systems, stock inventories, tagging, asset register)*	**83%**	79%
	Board of director engagement in cyber security policies and procedures	**72%**	75%
	Partners, clients, and vendors *(due diligence)*	**70%**	77%
	IP *(intellectual property risk assessment and trademark monitoring program)*	**68%**	75%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	**53%**	44%
Cyber Security	**79** Percentage of respondents that experienced a cyber incident in the past 12 months.	▼ 6% points below global average of 85%	
MOST COMMON TYPES OF CYBER INCIDENT	Data deletion by malicious insider	**30%**	19%
	Email-based phishing attack	**21%**	26%
	Virus/worm infestation	**21%**	33%
MOST COMMON PERPETRATORS	Ex-employees	**24%**	20%
MOST COMMON TARGET	Physical assets/money	**38%**	38%
	Customer records	**35%**	51%
	Trade secrets/R&D/IP	**35%**	40%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Webhosting/website provider	**16%**	9%
Security	**68** Percentage of respondents that experienced a security incident in the past 12 months.	= equal to global average of 68%	
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of intellectual property	**43%**	38%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**21%**	27%
	Workplace violence	**13%**	23%
MOST COMMON PERPETRATORS	Ex-employees	**31%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	**17%**	27%
	Theft or loss of intellectual property	**13%**	19%
	Terrorism *(including domestic and international events)*	**9%**	18%

Russia Overview

FRAUD

Participants in Russia reported a 9 percentage point increase in fraud over the last 12 months at 82%, equal to the global average.

The most common types of fraud were theft of physical assets, theft of data, and vendor or procurement fraud. Theft of assets was 9 percentage points above the global average of 29%. Where fraud had been detected, junior employees were most likely to have been involved, followed by freelance and temporary employees, cited by 31% and 28% of participants in Russia, respectively.

The most common risk mitigation measure implemented by respondents in Russia was information security, followed by management controls. Again, a significant proportion of respondents in Russia (77%) had seen the need to engage boards of directors in cyber policies and procedures.

CYBER SECURITY

Cyber incidents were less prevalent in Russia compared to other countries, coming in at 3 percentage points below the global average of 85%. Most notably, virus and worm infestations were reported less frequently by executives in Russia, experienced by 18% of respondents compared to a global average of 33%. The most common incidents stemmed from phishing and malware or system issues.

Customer and employee records were the primary targets of attacks, followed by physical assets or money. Customer records were reported as a target by 56% of participants, 5 percentage points above the global average of 51%.

SECURITY

Respondents in Russia were less likely than those in other countries to report a security incident, at 9 percentage points below the global average of 68%. The most common type of incident was the theft or loss of intellectual property, equal to the global average.

Ex-employees were responsible for over a third of all incidents, double the number of permanent employees, who were the next most common perpetrators.

The gap between the perceived vulnerability to security risks compared to the actual incidence of security events was the highest in the survey. For example, 38% of respondents had experienced theft or loss of IP whereas only 8% said they felt highly vulnerable to this type of risk.

RUSSIA REPORT CARD

Top responses given by survey respondents.

				Global avg.
Fraud	82	**Percentage of respondents affected by fraud in the past 12 months.**	▲ 9% points above 2015 = equal to global average of 82%	
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock		**38%**	29%
	Information theft, loss, or attack		**33%**	24%
	Vendor, supplier, or procurement fraud		**26%**	26%
MOST COMMON PERPETRATORS	Junior employees of our own company		**31%**	39%
	Freelance/temporary employees		**28%**	27%
	Senior or middle management employees of our own company		**22%**	30%
	Ex-employees		**22%**	27%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*		**19%**	26%
	Customers		**19%**	19%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*		**19%**	27%
MOST COMMON ANTI-FRAUD MEASURES	Information *(IT security, technical countermeasures)*		**90%**	82%
	Management *(management controls, incentives, external supervision such as audit committee)*		**79%**	74%
	Board of director engagement in cyber security policies and procedures		**77%**	75%
	Risk *(risk officer and risk management system)*		**77%**	78%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company		**41%**	44%
Cyber Security	82	**Percentage of respondents that experienced a cyber incident in the past 12 months.**	▼ 3% points below global average of 85%	
MOST COMMON TYPES OF CYBER INCIDENT	Email-based phishing attack		**33%**	26%
	Data deletion or corruption by malware or system issue		**26%**	22%
	Insider theft of IP/trade secrets/R&D		**18%**	17%
	Lost equipment with sensitive data		**18%**	17%
	Denial of service attack		**18%**	14%
	Virus/worm infestation		**18%**	33%
MOST COMMON PERPETRATORS	Ex-employees		**28%**	20%
MOST COMMON TARGET	Customer records		**56%**	51%
	Employee records		**34%**	40%
	Physical assets/money		**28%**	38%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor		**31%**	27%
Security	59	**Percentage of respondents that experienced a security incident in the past 12 months.**	▼ 9% points below global average of 68%	
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP		**38%**	38%
	Geographic and political risk *(i.e., operating in areas of conflict)*		**21%**	22%
	Workplace violence		**18%**	23%
MOST COMMON PERPETRATORS	Ex-employees		**35%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence		**18%**	27%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*		**8%**	20%
	Theft or loss of IP		**8%**	19%
	Geographic and political risk		**8%**	12%

Sub-Saharan Africa Overview

FRAUD

Respondents in Sub-Saharan Africa experienced one of the highest fraud incidence levels of all regions covered in the survey: 89% had experienced at least one type of fraud in the past year, 7 percentage points above the global average and 5 percentage points higher than in 2015.

Executives in the region reported the highest incidence of internal financial fraud (31%), 11 percentage points higher than the global average of 20%. They also experienced a higher than average incidence of information theft or loss.

Junior employees were cited as the most common perpetrators of fraud, followed by freelance and temporary staff. This is the only region surveyed where regulators were reported to significantly contribute to fraudulent activity, named in over a fifth (23%) of all frauds reported.

The most frequently mentioned anti-fraud measure was to engage the board of directors with the development of cyber security policies and procedures. The next most common anti-fraud measures were information security and staff background screening, both adopted by 70% of respondents in the region. However, these mitigation strategies had been adopted by fewer respondents in Sub-Saharan Africa than in the rest of the world on average.

CYBER SECURITY

Respondents in Sub-Saharan Africa reported the third highest exposure to cyber incidents (91%). Data deletion due to system issues was reported as the top form of attack by over a third of respondents in the region.

Other forms of attack, such as virus and worm infestations and email-based phishing attacks, were in line with the global averages. The greatest anomaly was in wire transfer fraud, which was at the highest level in the survey (26%) and nearly twice the global average of 14%.

Ex-employees were most likely to be responsible for a cyber incident, reported by 22% of participants.

Customer and employee records along with trade secrets were almost equally likely to be reported as the target of cyber attacks.

In the event of an attack, only 22% of participants said they would contact their IT service vendor first, while almost as many (16%) said they would contact an incident response firm.

SECURITY

Security incidents affected more respondents in the region, at 6 percentage points above the global average of 68%. The most common incidents were theft or loss of intellectual property (IP) (43%) and workplace violence (26%).

Theft or loss of IP weighs heavily as a concern and was mentioned as a vulnerability by a greater percentage of respondents in the region (28%) than any other region or country surveyed.

Participants in the region were more likely to name ex-employees as perpetrators of security incidents than elsewhere. They were named by 28% of participants compared to the global average of 23%.

SUB-SAHARAN AFRICA REPORT CARD

Top responses given by survey respondents.

			Global avg.
Fraud	**89** Percentage of respondents affected by fraud in the past 12 months.	▲ 5% points above 2015 ▲ 7% points above global average of 82%	
MOST COMMON TYPES OF FRAUD	Internal financial fraud *(manipulation of company results)*	**31%**	20%
	Information theft, loss, or attack *(e.g., data theft)*	**30%**	24%
	Theft of physical assets or stock	**26%**	29%
MOST COMMON PERPETRATORS	Junior employees of our own company	**33%**	39%
	Freelance/temporary employees	**27%**	27%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	**25%**	27%
	Senior or middle management employees of our own company	**23%**	30%
	Regulators	**23%**	14%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Board of director engagement in cyber security policies and procedures	**76%**	75%
	Staff *(background screening)*	**70%**	74%
	Information *(IT security, technical countermeasures)*	**70%**	82%
	Partners, clients, and vendors *(due diligence)*	**70%**	77%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	**60%**	39%
Cyber Security	**91** Percentage of respondents that experienced a cyber incident in the past 12 months.	▲ 6% points above global average of 85%	
MOST COMMON TYPES OF CYBER INCIDENT	Data deletion or loss due to system issues	**35%**	24%
	Virus/worm infestation	**31%**	33%
	Wire transfer fraud	**26%**	14%
	Email-based phishing attack	**26%**	26%
MOST COMMON PERPETRATORS	Ex-employees	**22%**	20%
MOST COMMON TARGET	Customer records	**49%**	51%
	Employee records	**47%**	40%
	Trade secrets	**47%**	40%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor	**22%**	27%
Security	**74** Percentage of respondents that experienced a security incident in the past 12 months.	▲ 6% points above global average of 68%	
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	**43%**	38%
	Workplace violence	**26%**	23%
	Geographic and political risk *(i.e., operating in areas of conflict)*	**19%**	22%
MOST COMMON PERPETRATORS	Ex-employees	**28%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Theft or loss of IP	**28%**	19%
	Workplace violence	**19%**	27%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**17%**	20%

United Kingdom Overview

FRAUD

Participants in the UK reported a higher incidence of fraud than every other country except Colombia. The vast majority (90%) of participants said they had been affected by fraud in the past 12 months. This represented an increase of 16 percentage points on last year and is 8 percentage points above the current global average of 82%.

Theft of physical assets and the misappropriation of funds were the two most common types of fraud reported by respondents in the UK. Both were more widespread in the UK than in any other region surveyed. Most perpetrators again came from inside the company. Executives in the UK indicated that junior employees were the biggest threat followed by senior or middle management (41% and 32% of participants, respectively).

Respondents in the UK have implemented anti-fraud measures such as IT security, management controls, and intellectual property monitoring/tracking.

CYBER SECURITY

Executives in the UK reported the second highest rate of cyber incidents after Colombia. Nearly all companies (92%) said they had experienced an attack or information loss over the past 12 months, which is 7 percentage points above the global average of 85%.

Virus and worm infestations were the most common types of incident, as in most countries and regions. Insider theft of customer or employee data was the second most common type of cyber incident in the UK, which was unusually high at 27% of respondents. Only respondents in China experienced this kind of insider theft at a higher rate (33%).

Similar to respondents from other countries, those in the UK said customer records were the most likely target of attacks or information theft, and ex-employees were the most likely perpetrators.

SECURITY

Along with respondents in the Middle East, those in the UK experienced the highest rate of security incidents in the past year. The majority (82%) said they had been the victims of an incident, which is 14 percentage points above the global average.

Theft of intellectual property, geopolitical events, and workplace violence were all reported at levels above the global average.

Executives from the UK were more likely to feel highly vulnerable to a wider range of security risks than participants from other regions.

UNITED KINGDOM REPORT CARD

Top responses given by survey respondents.

Fraud

90 — **Percentage of respondents affected by fraud in the past 12 months.**

▲ 16% points above 2015

▲ 8% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	**41%**	29%
	Misappropriation of company funds	**37%**	18%
	Information theft, loss, or attack *(e.g., data theft)*	**24%**	24%
	Market collusion *(e.g., price fixing)*	**24%**	17%
MOST COMMON PERPETRATORS	Junior employees of our own company	**41%**	39%
	Senior or middle management employees of our own companys	**32%**	30%
	Ex-employees	**30%**	27%
	Freelance/temporary employees	**27%**	27%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	**27%**	27%
	Customers	**27%**	19%
MOST COMMON ANTI-FRAUD MEASURES	Information *(IT security, technical countermeasures)*	**84%**	82%
	Management *(management controls, incentives, external supervision such as audit committee)*	**80%**	74%
	IP *(intellectual property risk assessment and trademark monitoring program)*	**76%**	75%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	**50%**	44%

Cyber Security

92 — **Percentage of respondents that experienced a cyber incident in the past 12 months.**

▲ 7% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	**33%**	33%
	Insider theft of customer or employee data	**27%**	19%
	Data breach resulting in loss of customer or employee data	**22%**	23%
	Data deletion or loss due to system issues	**22%**	24%
MOST COMMON PERPETRATORS	Ex-employees	**29%**	20%
MOST COMMON TARGET	Customer records	**42%**	51%
	Trade secrets/R&D/IP	**42%**	40%
	Company/employee identity	**40%**	36%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor	**33%**	27%

Security

82 — **Percentage of respondents that experienced a security incident in the past 12 months.**

▲ 14% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	**51%**	38%
	Geographic and political risk *(i.e., operating in areas of conflict)*	**39%**	22%
	Workplace violence	**29%**	23%
MOST COMMON PERPETRATORS	Ex-employees	**28%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	**31%**	27%
	Theft or loss of IP	**24%**	19%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**24%**	20%
	Geographic and political risk *(i.e., operating in areas of conflict)*	**24%**	12%
	Terrorism, including domestic and international events	**24%**	18%

China Overview

FRAUD

A large proportion (86%) of respondents in China reported fraud in the last 12 months, above the global average of 82%, and representing a double-digit (13 percentage point) increase from 2015.

Respondents in China reported the widest spread of fraud types. Out of all the regions surveyed, participants in China named regulatory or compliance breaches as the primary fraud (41%), which was nearly twice the global average. This was followed by vendor, supplier, and procurement fraud, which was 11 percentage points above the global average.

Other types of fraud mentioned included the theft of physical assets or stock as well as the theft of data and information. Respondents in China also fell victim to above-average rates of corruption and bribery, market collusion, and the misappropriation of company funds.

Respondents in China identified joint venture partners as the key perpetrators of fraud (52% of cases), more than twice the global average of 23% and significantly above any other region surveyed. Overall, external perpetrators are mentioned more frequently in China compared to the global averages. For example, agents/intermediaries were identified as key perpetrators by 43% of executives in China, 16 percentage points above the global average of 27%, and vendors/suppliers were mentioned by 36% of respondents, 10 percentage points above the global average of 26%.

The internal threat is also significant. Almost half (48%) of the participants in China said junior employees were responsible for fraud, and over a third (34%) said senior or middle management were the main perpetrators.

Respondents in China have taken measures to combat fraud. Nearly all (90%) of the region's participants had invested in partner, client or vendor due diligence, followed by the protection of physical assets (86%), and board engagement in cyber policies and procedures (86%).

Similar to other regions, respondents in China reported that their company had detected fraud through internal whistle-blowers (55%). The same proportion cited external audits as a fraud detection method, which was 19 percentage points higher than the global average of 36%.

CYBER SECURITY

The number of executives in China who reported a cyber incident was 1 percentage point above the global average of 85%. Two of the most common incidents were significantly above the global incidence average: email-based phishing attacks (15 percentage points above the global average of 26%) and data deletion from malware or system issues (17 percentage points above the global average of 22%).

The majority of participants in China (82%) noted customer records as the most common target of a cyber attack. This was significantly higher than the global average of 51%. Other popular targets were trade secrets and R&D/intellectual property at 59%, and employee records and identities, both at 41%.

The most common perpetrators were freelance and temporary employees. Upon discovering an attack, the first call for 34% of respondents was to an IT service vendor.

SECURITY

Environmental risks were the most frequently reported security incidents by respondents from China, at nearly 20 percentage points above the global incidence average of 27%.

In addition, geopolitical events were reported by a quarter of participants, as well as theft or loss of intellectual property which was reported by 41% of participants.

Respondents in China were unique in reporting competitors as being the most frequent perpetrators of security incidents at 21%, almost twice the global average of 12%.

CHINA REPORT CARD

Top responses given by survey respondents.

Fraud

86 — **Percentage of respondents affected by fraud in the past 12 months.**

▲ 13% points above 2015

▲ 4% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Regulatory or compliance breach	**41%**	21%
	Vendor, supplier, or procurement fraud	**37%**	26%
	Theft of physical assets or stock	**25%**	29%
	Information theft, loss, or attack *(e.g., data theft)*	**25%**	24%
	Corruption and bribery	**25%**	15%
	Market collusion *(e.g., price fixing)*	**25%**	17%
	Misappropriation of company funds	**25%**	18%
MOST COMMON PERPETRATORS	Joint venture partners *(i.e., a partner who provides manufacturing or other business function, or a franchisee)*	**52%**	23%
	Junior employees of our own company	**48%**	39%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	**43%**	27%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	**36%**	26%
	Senior or middle management employees of our own company	**34%**	30%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Partners, clients, and vendors *(due diligence)*	**90%**	77%
	Assets *(physical security systems, stock inventories, tagging, asset register)*	**86%**	79%
	Board of director engagement in cyber security policies and procedures	**86%**	75%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	**55%**	44%
	Through an external audit	**55%**	36%

Cyber Security

86 — **Percentage of respondents that experienced a cyber incident in the past 12 months.**

▲ 1% point above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Email-based phishing attack	**41%**	26%
	Virus/worm infestation	**39%**	33%
	Data deletion or corruption by malware or system issue	**39%**	22%
MOST COMMON PERPETRATORS	Freelance/temporary employees	**25%**	14%
MOST COMMON TARGET	Customer records	**82%**	51%
	Trade secrets/R&D/IP	**59%**	40%
	Employee records	**41%**	40%
	Company/employee identity	**41%**	36%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor	**34%**	27%

Security

75 — **Percentage of respondents that experienced a security incident in the past 12 months.**

▲ 7% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**45%**	27%
	Theft or loss of IP	**41%**	38%
	Geographic and political risk *(i.e., operating in areas of conflict)*	**25%**	22%
MOST COMMON PERPETRATORS	Competitors	**21%**	12%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	**33%**	27%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**31%**	20%
	Terrorism, including domestic and international events	**31%**	18%

China: Developing a Strategy to Combat Fraud

BY VIOLET HO

China stood out in Kroll's 2016 Global Fraud and Risk survey, but not in a good way. A quarter of survey respondents indicated that they were dissuaded from operating in China due to concerns over fraud and corruption. This result is consistent with what we see on the frontline of fighting fraud in China.

Over the past decade, fraud in China has become increasingly complex and challenging. While its fraud trends share some common traits with other developing countries, fraud in China also has some unique characteristics. For example, fraud is often committed by senior executives, resulting in losses that are potentially more significant. It also often involves cross-departmental and multiple-party collusions, rendering traditional internal control measures ineffective. To complicate the problem, the rapid expansion and quick staff turnover of many organizations means that there is a lack of continuity in corporate governance and fraud detection. Fraudsters in China are also becoming more systematic and enterprising, posing significant threats to their victims.

While some survey respondents suggested that they were prepared to walk away from China because of their fear of fraud, this may not be the easiest (or necessarily the smartest) move.

China has firmly established itself as the second-largest economy in the world. As such, it is becoming increasingly difficult for global organizations to avoid doing business there altogether. It is also the dominant trading partner of many countries, and Chinese consumers represent attractive revenue streams that are not easily ignored.

Managing the risk of fraud in China is never easy, but it is achievable with a clear and consistent strategy. While no single solution will work in isolation, in our experience, there are a number of fraud mitigation measures that can be adopted by organizations of any size, in any industry. Companies must be vigilant and dynamic in their approach. It is essential to treat the fight against fraud as a long-term game, and not to look for shortcuts or overnight miracles.

VIOLET HO
Violet Ho is a Senior Managing Director and Co-Head of Kroll's Investigations and Disputes practice in Greater China. With over 19 years of professional experience in investigations, and an in-depth understanding of China's business environment, Violet has successfully advised on numerous highly complex investigative projects in China and beyond.

1 Get the most out of your whistle-blowing system: Fraud is most commonly perpetrated by company insiders – and is most commonly discovered by company insiders. Whistle-blower complaints and senior management oversight are the most effective channels for detecting fraud in China. Many companies now have whistle-blower hotlines or reporting systems, but are not necessarily making the best use of them.

For example, Kroll worked with a multinational company to modify and domesticate its whistle-blowing system. To ensure that sufficient and relevant information is extracted from each whistle-blower and presented in a manner that can be easily accessed and analyzed, we designed questions and fields for whistle-blowers to complete during the anonymous reporting process. We also advised the client to implement a protocol to document the nature of the specific allegations in each report, including the department and seniority of the personnel implicated, the types of fraud alleged, and the duration of the alleged scheme.

Over a period of 2–3 years, a clear and auditable trail was maintained. More importantly, the accumulated data was reviewed and analyzed, which revealed internal control vulnerabilities and fraud risks in particular functions. Subsequent investigations were much more effective as a result.

2 Focus on the human factor: Regardless of the type and scale, all fraud is committed by people. In my experience, many companies do not do enough to ensure that they are hiring individuals with proven track records and strong integrity. During an investigation, we often discover that wrong-doers have committed fraud against their employers before. This could have been flagged through employee background checks. Robust employee due diligence carried out in conjunction with third-party vendor due diligence often reveal signs of potential conflicts of interest and kickback arrangements.

3 Ensure independence of investigations: Given the high prevalence of fraud in China, it may not be practical or feasible for a company to investigate all allegations. It is therefore important not to give employees the perception that investigations were initiated to further someone's personal agenda. Using professional advisers can enhance senior management's credibility and ensure confidentiality and independence. External advisers can also deter fraudsters who hope to influence the investigations by playing office politics.

4 Build a strong compliance culture with tone from the top and clear accountability: One of the best tools for preventing, detecting, and responding to fraud is to build and maintain a corporate culture with zero tolerance for fraud and corruption. This takes time, and support from the C-Suite is crucial. When setting key performance indicators for employees, financial goals should not be the only objectives considered. Senior executives should also be responsible for setting the tone and embedding a robust compliance culture in their teams.

India Overview

FRAUD

Respondents in India reported a 12 percentage point reduction in the incidence of fraud over the last 12 months. The percentage of respondents affected by fraud was 68%, equal to that of Brazil, with both countries tied for having the lowest prevalence in the survey. The incidence of fraud in India was reported at 14 percentage points below the global average of 82%.

However, when all participants of the survey were asked whether they had been dissuaded from operating in a jurisdiction because of fraud concerns, India (19%) was the second most mentioned jurisdiction after China (25%).

This suggests that there is a gap between internal and external stakeholders in the perception of fraud in India.

Executives in India named junior employees inside the company (61%) as the primary perpetrators of fraud incidents. The next most common group to be named was agents and intermediaries working for the company. Executives identified both sets of perpetrators at 22 percentage points above the global averages of 39% and 27%, respectively.

Respondents in India are implementing anti-fraud measures. Over 85% of participants are combating fraud through better financial controls, due diligence on partners, clients, and vendors, information security systems, and staff controls.

Fraud was most likely to be detected by a whistle-blower system, named by 66% of participants.

CYBER SECURITY

Coming in at 12 percentage points below the global average, 73% of participants in India reported that they had experienced a cyber incident in the past 12 months. This relatively low number may well reflect that not all segments of Indian businesses appreciate cyber risk. This could be because not many sectors in India, apart from the financial services industry, are as digitized as they are in more developed countries, which reduces their exposure to cyber security risk. Another reason could be that respondents that face cyber-security-related events are often not required to disclose data breaches, and hence the sensitivity to this cyber-security-related risk is still evolving.

The most common types of cyber incidents threatening companies in India were cited as data deletion from malware or system issues (28%), and malicious insiders (27%).

Interestingly, however, executives in India did not identify a group of individuals as perpetrators, but most commonly said that the cause of incidents was most likely to be accidental placement of sensitive data on a search engine (mentioned by 25% of participants, 15 percentage points above the global average of 10%).

SECURITY

Security incidents were more prevalent in India at 4 percentage points above the global average of 68%, which is consistent with Kroll's experience on the ground in India. The damage from natural disasters was 13 percentage points above the global average of 27%. Compared to other major developed markets, the theft of intellectual property came slightly under the global average (35% versus 38%, respectively).

The most common perpetrators of security incidents were cited as permanent employees of the company. While participants said they felt most vulnerable to workplace violence (52%), followed by other forms of violence such as international or domestic terrorism (45%), environmental risks ranked third (37%) despite being cited as the most common cause of a security incident.

INDIA REPORT CARD

Top responses given by survey respondents.

Fraud

68 — **Percentage of respondents affected by fraud in the past 12 months.**

▼ 12% points below 2015

▼ 14% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	**28%**	29%
	Management conflict of interest	**27%**	21%
	Corruption and bribery	**27%**	15%
	Vendor, supplier, or procurement fraud	**27%**	26%
	Market collusion *(e.g., price fixing)*	**27%**	17%
	Internal financial fraud *(manipulation of company results)*	**25%**	20%
MOST COMMON PERPETRATORS	Junior employees of our own company	**61%**	39%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	**49%**	27%
	Freelance/temporary employees	**41%**	27%
	Senior or middle management employees of our own company	**37%**	30%
	Joint venture partners *(i.e., a partner who provides manufacturing or other business function, or a franchisee)*	**37%**	23%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	**87%**	77%
	Partners, clients, and vendors *(due diligence)*	**87%**	77%
	Information *(IT security, technical countermeasures)*	**85%**	82%
	Staff *(background screening)*	**85%**	74%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	**66%**	44%

Cyber Security

73 — **Percentage of respondents that experienced a cyber incident in the past 12 months.**

▼ 12% points below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Data deletion or corruption by malware or system issue	**28%**	22%
	Data deletion by malicious insider	**27%**	19%
	Virus/worm infestation	**23%**	33%
	Denial of service attack	**23%**	14%
MOST COMMON PERPETRATORS	Accidental placement of sensitive data that was indexed by a search engine *(e.g., Google)*	**25%**	10%
MOST COMMON TARGET	Employee records	**59%**	40%
	Trade secrets/R&D/IP	**48%**	40%
	Customer records	**45%**	51%
	Physical assets/money	**45%**	38%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor	**34%**	27%

Security

72 — **Percentage of respondents that experienced a security incident in the past 12 months.**

▲ 4% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Environmental risk *(including damage caused by natural disasters such as hurricanes,tornadoes, floods, earthquakes, etc.)*	**40%**	27%
	Workplace violence	**37%**	23%
	Theft or loss of IP	**35%**	38%
	Geographic and political risk *(i.e., operating in areas of conflict)*	**35%**	22%
MOST COMMON PERPETRATORS	Permanent employees of our own company	**26%**	17%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	**52%**	27%
	Terrorism, including domestic and international events	**45%**	18%
	Environmental risk *(including damage caused by natural disasters such as hurricanes,tornadoes, floods, earthquakes, etc.)*	**37%**	20%

India: Riding the Contradictions

BY RESHMI KHURANA

In Kroll's 2016 Global Fraud and Risk survey, India was second on the list of jurisdictions that respondents were dissuaded from operating in, after China. Nearly a fifth (19%) of respondents said India was enough of a fraud risk to stop them from operating there. An equal proportion of respondents said that security risk deters them from operating in India.

The statistics reveal the contradiction in the Indian economy. On the one hand, India is an attractive destination for foreign investors. As one of the fastest-growing major emerging markets, it is politically more stable than in previous cycles and the BJP-led government is undertaking overdue economic reforms to attract foreign direct investment. On the other hand, as our survey indicates, investors are deterred due to fraud, corruption, and security concerns.

The India market is too large to ignore for many investors, and strategic investors often choose to operate there via joint ventures with local partners who control the operations of the local companies. Foreign investors believe such local partners are better able to manage India's operating environment – which involves a close nexus between business, government, and bureaucracy, thus creating suspicions of improper dealings.

While local businesses can see behind the scenes, foreign investors struggle to do so, which creates an opportunity for fraudulent activity. For example, local management may engage in related-party transactions to generate cash by inflating vendor invoices or creating fake employees. Such practices can make it difficult for investors to understand whether the cash is being generated for legitimate business purposes (such as land acquisition or paying rural employees), or for paying kickbacks to government officials.

Similar to China, the levels of collusion between employees, vendors, customers, and other stakeholders to perpetrate fraud can be high in India. Fraud can arise in dealings with third parties as well as among groups of employees. When a fraud is identified, it is often not easy to terminate employees or discontinue relationships with key vendors, as this can damage employee morale and business continuity. Companies therefore need to tread carefully when responding to fraud allegations.

RESHMI KHURANA
Reshmi Khurana is a Managing Director and Head of South Asia in Kroll's Investigations and Disputes practice, based in the Mumbai office. Reshmi has more than 16 years of experience in the United States as well as in South and Southeast Asia conducting complex corruption investigations, litigation support projects, and due diligence on the management, operations, and business models of organizations. Her experience includes helping clients identify and bridge gaps in internal controls and corporate governance through people, processes, and technology.

For example, Kroll recently conducted an investigation for a major global conglomerate that had received an anonymous whistle-blower complaint alleging that its local CEO was accepting kickbacks from certain vendors. The client was understandably concerned about how the investigation would impact the morale of the local organization, and its ability to continue serving customers while the investigation was underway. Kroll helped the client investigate the allegations discreetly by reviewing electronic evidence, conducting subtle on-the-ground enquiries, and analyzing specific vendor transaction data in order to minimize disruption.

The investigation revealed that the local management culture, accounting processes, and corporate governance had arguably led to the creation of an environment that was ripe for fraud. We found that senior management was aware of the gaps in corporate governance as well as the fraud that resulted. Kroll helped the client understand the full scope of the problem, which led to the removal of the CEO and other employees.

Security issues are also making their way to the top of the agenda: nearly a fifth of respondents said they would be dissuaded from investing in India because of security risks.

It is, however, possible to manage these risks. To avoid fraud, we advise both new and experienced investors to:

1 **Assess:** A qualitative assessment of the operating environment and any potential partners—which includes their reputation, political connections, ethical standards, and business practices—is as important as reviewing growth numbers, financial records, and legal documents.

2 **Understand:** Foreign investors need to understand the full dynamics of India's business and political environment to ensure they make wise investments.

3 **Prepare well:** Investors should not be swayed by the competitive pressures of the investment environment in India, where too many investors often pursue the same opportunities. They should take their time so they are prepared to make a well-informed investment.

4 **Never compromise:** Investors should select advisors on a "no-compromise basis" to ensure they are truly independent, and that the integrity of any due diligence process is maintained.

Brazil Overview

FRAUD

Brazil was one of three countries surveyed whose incidence of fraud came under the global average of 82%. The other two were India and Italy. Just over two-thirds (68%) of participants in Brazil experienced fraud in the past 12 months, 14 percentage points below the global average.

Theft is a big issue for companies in Brazil, with nearly a quarter (24%) of participants reporting instances of theft of physical assets. In addition, over a fifth (21%) of participants reported information theft and vendor, supplier, or procurement fraud. However, in keeping with the lower levels of fraud reported in Brazil, the incidence of these frauds is below the reported global average.

A large majority (85%) had invested in management-focused anti-fraud methods, resulting in high adoption rates of physical asset registers (88%) and information security measures (88%).

The most common fraud detection method for Brazilian companies was through an external audit, cited by 43% of participants.

A significant proportion (43%) of participants pointed to ex-employees as the main perpetrators of fraud. Freelance/temporary staff and junior staff were cited as contributing to fraud incidents by approximately a quarter (26%) and a fifth (22%) of participants, respectively.

CYBER SECURITY

Respondents in Brazil experienced fewer cyber security incidents than other regions at 9 percentage points below the reported global average of 85%. However, with over three-quarters of participants (76%) indicating they had experienced a cyber incident in the last 12 months, a majority of respondent companies from Brazil are still vulnerable.

Data from Brazil shows participants were targeted by attacks from viruses and worms and breaches that resulted in the loss of customer and employee data.

Virus and worm attacks were 8 percentage points above the global average (33%), with 41% of participants saying they had been a victim of this method of attack. Customer records were the main targets for attackers, followed by employee records, and company and employees identities.

At 38%, the rate of ex-employees instigating cyber attacks was nearly twice the reported global average of 20%.

SECURITY

Just over half (53%) of the surveyed participants in Brazil said they had experienced a security incident. This was significantly (15 percentage points) below the reported global average of 68%. The most common type of incident reported was the theft and loss of intellectual property followed by environmental and geopolitical events.

BRAZIL REPORT CARD

Top responses given by survey respondents.

			Global avg.
Fraud	**68** Percentage of respondents affected by fraud in the past 12 months.	▼ 9% points below 2015 ▼ 14% points below global average of 82%	
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	**24%**	29%
	Information theft, loss or attack *(e.g., data theft)*	**21%**	24%
	Vendor, supplier or procurement fraud	**21%**	26%
MOST COMMON PERPETRATORS	Ex-employees	**43%**	27%
	Freelance/temporary employees	**26%**	27%
	Junior employees of our own company	**22%**	39%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	**17%**	26%
	Agents and/or intermediaries *(i.e., a 3rd party working on behalf of your company)*	**17%**	27%
	Joint venture partners *(i.e., a partner who provides manufacturing or other business function, or a franchisee)*	**17%**	23%
	Customers	**17%**	19%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Assets *(physical security systems, stock inventories, tagging, asset register)*	**88%**	79%
	Information *(IT security, technical countermeasures)*	**88%**	82%
	Management *(management controls, incentives, external supervision such as audit committee)*	**85%**	74%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	**43%**	36%
Cyber Security	**76** Percentage of respondents that experienced a cyber incident in the past 12 months.	▼ 9% points below global average of 85%	
MOST COMMON TYPES OF CYBER INCIDENT	Virus/ worm infestation	**41%**	33%
	Data breach resulting in loss of customer or employee data	**29%**	23%
	Data deletion or loss due to system issues	**21%**	24%
MOST COMMON PERPETRATORS	Ex-employees	**38%**	20%
MOST COMMON TARGET	Customer records	**46%**	51%
	Employee records	**42%**	40%
	Company/employee identity	**42%**	36%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Webhosting/website provider	**23%**	9%
Security	**53** Percentage of respondents that experienced a security incident in the past 12 months.	▼ 15% points below global average of 68%	
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	**32%**	38%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**18%**	27%
	Geographic and political risk *(i.e., operating in areas of conflict)*	**12%**	22%
MOST COMMON PERPETRATORS	Ex-employees	**39%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Theft or loss of IP	**21%**	19%
	Workplace violence	**18%**	27%
	Geographic and political risk *(i.e., operating in areas of conflict)*	**15%**	12%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**15%**	20%

Colombia Overview

FRAUD

Fraud was reported by almost all (95%) of the participants in Colombia, the highest proportion in the survey and a 12 percentage point increase compared to 2015.

Participants reported that the most common type of fraud was the result of conflicts of interest in management teams, followed by vendor and procurement fraud and then the theft of physical assets. The most common perpetrators were ex-employees, freelance/temporary employees, and vendors/suppliers, with each group being reported by just over a third of participants from Colombia (35%).

Responses from participants in Colombia indicated that there are sizable steps being taken to implement anti-fraud measures, with participants detailing their efforts around financial controls, physical asset management strategies and staff background screening.

Half of the participants in Colombia reported fraud was most often detected through internal audits.

CYBER SECURITY

More participants in Colombia reported cyber incidents (95%) than in any other region at 10 percentage points above the global average of 85%. Over half of participants from Colombia said they had experienced attacks due to virus and worm infestations (52%), followed by email-based phishing attacks (38%). Data deletion or losses were reported by 29% of executives in Colombia, 5 percentage points above the global average.

The main targets of cyber attacks in Colombia included customer records, physical assets, and employee records, which were roughly in line with the global averages. Also echoing experiences from other regions were the reported perpetrators: ex-employees were identified as the primary culprits of cyber incidents by a quarter of participants in Colombia.

SECURITY

Participants in Colombia indicated that the prevalence of security incidents was slightly below the reported global average at 62%. Workplace violence was the most common security incident. Again, freelancers and temporary staff were in the spotlight as the perpetrators named by 38% of participants in Colombia.

COLOMBIA REPORT CARD

Top responses given by survey respondents.

			Global avg.
Fraud	**95** Percentage of respondents affected by fraud in the past 12 months.	▲ 12% points above 2015 ▲ 13% points above global average of 82%	
MOST COMMON TYPES OF FRAUD	Management conflict of interest	**43%**	21%
	Vendor, supplier, or procurement fraud	**43%**	26%
	Theft of physical assets or stock	**38%**	29%
MOST COMMON PERPETRATORS	Ex-employees	**35%**	27%
	Freelance/temporary employees	**35%**	27%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	**35%**	26%
	Senior or middle management employees of our own company	**20%**	30%
	Junior employees of our own company	**20%**	39%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	**95%**	77%
	Assets *(physical security systems, stock inventories, tagging, asset register)*	**95%**	79%
	Staff *(background screening)*	**95%**	74%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	**50%**	39%
Cyber Security	**95** Percentage of respondents that experienced a cyber incident in the past 12 months.	▲ 10% points above global average of 85%	
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	**52%**	33%
	Email-based phishing attack	**38%**	26%
	Data deletion or loss due to system issues	**29%**	24%
MOST COMMON PERPETRATORS	Ex-employees	**25%**	20%
MOST COMMON TARGET	Customer records	**50%**	51%
	Physical assets/money	**45%**	38%
	Employee records	**40%**	40%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Incident response firm	**15%**	14%
	Insurance portal	**15%**	5%
	Webhosting/website provider	**15%**	9%
Security	**62** Percentage of respondents that experienced a security incident in the past 12 months.	▼ 6% points below global average of 68%	
MOST COMMON TYPES OF SECURITY INCIDENTS	Workplace violence	**24%**	23%
	Theft or loss of intellectual IP	**24%**	38%
	Terrorism, including domestic and international events	**19%**	15%
MOST COMMON PERPETRATORS	Freelance/temporary employees	**38%**	16%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Terrorism, including domestic and international events	**19%**	18%
	Workplace violence	**19%**	27%
	Environmental risk *(including damage caused by natural disasters such as hurricanes,tornadoes, floods, earthquakes, etc.)*	**14%**	20%

Mexico Overview

FRAUD

The majority (82%) of respondents in Mexico reported incidents of fraud over the past 12 months, an increase of 2 percentage points on 2015.

The striking detail to take away from the survey of executives in Mexico is the frequency of vendor and supplier fraud, which at 52% was the highest of all countries surveyed and double the reported global average of 26%.

Currently, the two mechanisms which are most commonly used by respondents in Mexico to combat fraud are partner, vendor or supplier due diligence and, financial controls, both by 82% of respondents.

Fraud is most commonly detected through internal audits, named by 44% of participants in Mexico.

CYBER SECURITY

Respondents in Mexico experienced a slightly below-average occurrence of cyber incidents, at 82%. The main methods of attack were through viruses and worms, email-based phishing attacks, and data deletion through malware or system issues.

The majority of attacks originated from competitors. Participants in Mexico were three times more likely than the global average to report competitors as primary perpetrators of cyber incidents.

Those respondents in Mexico who had experienced an attack were most likely to turn first to federal law enforcement agencies.

SECURITY

Participants in Mexico reported the lowest rate of security incidents in the survey. Less than half the participants (48%) said they had experienced an incident, which is 20 percentage points below the reported global average of 68%. The most common incident reported was environmental events (27%), with the next most common incidents being the loss of intellectual property and geopolitical events.

Participants in Mexico felt vulnerable to workplace violence and terrorism although they did not report events related to either of these security risks in their top three incidents.

MEXICO REPORT CARD

Top responses given by survey respondents.

			Global avg.
Fraud	**82** Percentage of respondents affected by fraud in the past 12 months.	▲ 2% points above 2015 = equal to global average of 82%	
MOST COMMON TYPES OF FRAUD	Vendor, supplier, or procurement fraud	**52%**	26%
	Theft of physical assets or stock	**30%**	29%
	Corruption and bribery	**18%**	15%
MOST COMMON PERPETRATORS	Ex-employees	**33%**	27%
	Junior employees of our own company	**30%**	39%
	Freelance/temporary employees	**30%**	27%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	**30%**	26%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	**26%**	27%
MOST COMMON ANTI-FRAUD MEASURES	Partners, clients, and vendors *(due diligence)*	**82%**	77%
	Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	**82%**	77%
	Risk *(risk officer and risk management system)*	**81%**	78%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	**44%**	39%
Cyber Security	**82** Percentage of respondents that experienced a cyber incident in the past 12 months.	▼ 3% points below global average of 85%	
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	**39%**	33%
	Email-based phishing attack	**33%**	26%
	Data deletion or corruption by malware or system issue	**33%**	22%
MOST COMMON PERPETRATORS	Competitors	**22%**	6%
MOST COMMON TARGET	Company/employee identity	**52%**	36%
	Customer records	**48%**	51%
	Physical assets/money	**37%**	38%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Federal law enforcement	**30%**	8%
Security	**48** Percentage of respondents that experienced a security incident in the past 12 months.	▼ 20% points below global average of 68%	
MOST COMMON TYPES OF SECURITY INCIDENTS	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**27%**	27%
	Theft or loss of IP	**24%**	38%
	Geographic and political risk *(i.e., operating in areas of conflict)*	**21%**	22%
MOST COMMON PERPETRATORS	Freelance/temporary employees	**31%**	16%
	Ex-employees	**31%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	**24%**	27%
	Terrorism, including domestic and international events	**21%**	18%
	Theft or loss of IP	**18%**	19%

Construction, Engineering, and Infrastructure Overview

FRAUD

This year's survey shows the construction, engineering, and infrastructure industry as a success story. While 70% of respondents in the industry still reported being affected by fraud, this number was significantly under the global average and by far the lowest rate of any industry. The next lowest was the technology, media, and telecoms (TMT) sector, where 79% of respondents reported fraud.

Construction, engineering, and infrastructure was also the only industry which saw a decrease in fraud from 2015 to 2016, with the percentage of respondents reporting an incident falling by 5 percentage points over the period.

Consistent with other industries, the most common perpetrators of fraud were junior employees, with participants reporting that they were a key perpetrator in 45% of instances. Ex-employees were responsible in a third of all cases.

Reflecting the threat from employees, the most widely adopted anti-fraud measures related to staff. These covered training, whistle-blower hotlines, and background screening for new recruits. Internal audits were the most common method of detection of fraud for these respondents.

CYBER SECURITY

When it came to cyber attacks, more than three-quarters of participants reported that their company had experienced an instance in the last 12 months. While below the global average, the instance of a cyber attack was still prevalent, with customer records the main target through virus or worm infestations, email-based phishing attacks, and data deletion or loss due to system issues.

SECURITY

More than half (63%) of respondents in the construction, engineering, and infrastructure industry had experienced a security risk in the past 12 months. Instances of environmental and geopolitical risk were higher than the global averages; however, theft and loss of intellectual property was less of a risk for these respondents than most, despite being reported as an area of vulnerability.

CONSTRUCTION, ENGINEERING, AND INFRASTRUCTURE

Top responses given by survey respondents.

Fraud

70 **Percentage of respondents affected by fraud in the past 12 months.**

▼ 5% points below 2015

▼ 12% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Vendor, supplier, or procurement fraud	**28%**	26%
	Internal financial fraud *(manipulation of company results)*	**21%**	20%
	Corruption and bribery	**19%**	15%
	Misappropriation of company funds	**19%**	18%
	Theft of physical assets or stock	**19%**	29%
MOST COMMON PERPETRATORS	Junior employees	**45%**	39%
	Ex-employees	**33%**	27%
	Senior or middle management employees	**30%**	30%
	Freelance/temporary employees	**30%**	27%
	Vendors/suppliers	**30%**	26%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Staff *(training, whistle-blower hotline),*	**81%**	76%
	Staff *(background screening)*	**79%**	74%
	Partners, clients, and vendors *(due diligence)*	**79%**	77%
	Information *(IT security, technical countermeasures)*	**79%**	82%
	Risk *(risk officer and risk management system)*	**79%**	78%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	**38%**	39%

Cyber Security

77 **Percentage of respondents that experienced a cyber incident in the past 12 months.**

▼ 8% points below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	**35%**	33%
	Email-based phishing attack	**30%**	26%
	Data deletion or loss due to system issues	**30%**	24%
MOST COMMON PERPETRATORS	Ex-Employees	**20%**	20%
MOST COMMON TARGET	Customer records	**59%**	51%
	Employee records	**45%**	40%
	Physical assets/money	**43%**	38%

Security

63 **Percentage of respondents that experienced a security incident in the past 12 months.**

▼ 5% points below global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Environmental risk	**33%**	27%
	Theft or loss of IP	**32%**	38%
	Geographic and political risk	**23%**	22%
	Workplace violence	**23%**	23%
MOST COMMON PERPETRATORS	Ex-Employees	**25%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Theft or loss of intellectual property	**18%**	19%
	Environmental risk	**18%**	20%
	Workplace violence	**12%**	27%

Consumer Goods Overview

FRAUD

A majority (82%) of respondents in the consumer goods industry reported instances of fraud in the past 12 months, on par with the global average. This represented a 10 percentage point rise on the previous year. Instances of information theft, loss, or attack were most common, accounting for almost a third (32%) of fraud experienced.

Agents and intermediaries were the most frequent perpetrators of fraud for consumer goods industry respondents, responsible in 43% of cases. It was the only industry group where agents and intermediaries topped the list of common perpetrators.

The adoption of anti-fraud measures was relatively low in the consumer goods industry. Information and asset security measures were the most commonly adopted, but both came in below the global average. Furthermore, the adoption of information security measures was the lowest of any industry sector except professional services.

CYBER SECURITY

Email-based phishing attack was the most common type of cyber incident suffered in the past year (28%) followed closely by data breach resulting in loss of customer or employee data (27%) and virus/worm infestation (27%). Customer records were the target in nearly two-thirds (62%) of all attacks, which was more often than for any other industry except manufacturing.

SECURITY

Theft or loss of intellectual property and environmental risks were the most common security risks experienced. Terrorism was third on the list, but with a fifth of all consumer goods industry executives surveyed reporting having been affected, it was higher than the global average.

CONSUMER GOODS

Top responses given by survey respondents.

Fraud

82 — **Percentage of respondents affected by fraud in the past 12 months.**

▲ 10% points above 2015

= Equal to global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Information theft, loss, or attack *(e.g., data theft)*	**32%**	24%
	Theft of physical assets or stock	**28%**	29%
	Vendor, supplier, or procurement fraud	**28%**	26%
MOST COMMON PERPETRATORS	Agents and/or intermediaries	**43%**	27%
	Junior employees	**37%**	39%
	Vendors/suppliers	**35%**	26%
	Joint venture partners	**31%**	23%
	Senior or middle management employees	**24%**	30%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Information *(IT security, technical countermeasures)*	**77%**	82%
	Assets *(physical security systems, stock inventories, tagging, asset register)*	**77%**	79%
	Board of director engagement in cyber security policies and procedures	**73%**	75%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	**53%**	44%

Cyber Security

83 — **Percentage of respondents that experienced a cyber incident in the past 12 months.**

▼ 2% points below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Email-based phishing attack	**28%**	26%
	Data breach resulting in loss of customer or employee data	**27%**	23%
	Virus/worm infestation	**27%**	33%
MOST COMMON PERPETRATORS	Ex-employees	**28%**	20%
MOST COMMON TARGET	Customer records	**62%**	51%
	Trade secrets/R&D/IP	**54%**	40%
	Company/employee identity	**30%**	36%

Security

75 — **Percentage of respondents that experienced a security incident in the past 12 months.**

▲ 7% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	**27%**	38%
	Environmental risk	**27%**	27%
	Terrorism	**20%**	15%
	Geographic and political risk	**20%**	22%
MOST COMMON PERPETRATORS	Ex-employees	**31%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Theft or loss of IP	**22%**	19%
	Workplace violence	**20%**	27%
	Environmental risk	**18%**	20%

Financial Services Overview

FRAUD

The financial services industry as a whole experienced a massive 19 percentage point increase in fraud, with 89% of all respondents in the industry reporting at least one type in the past year. The most common types of fraud experienced were theft of physical assets and stock (experienced by 39% of respondents) and vendor, supplier, or procurement fraud (32% of respondents). The percentage of financial services executives surveyed that experienced intellectual property (IP) theft, piracy, and counterfeiting was 27%, almost double the global average.

Respondents in the financial services industry were more likely to have adopted anti-fraud measures than the global average, with risk officers and risk management systems unsurprisingly topping the list. These respondents were also significantly more likely to have implemented IP risk management measures than all industries except healthcare.

While most fraud was detected by whistle-blowers in other industry sectors, financial services fraud was more likely to be discovered through an external audit.

CYBER SECURITY

Respondents in the financial services industry also reported a higher than average incidence of cyber attack, with data deletion or loss due to system issues the most common. The targets of attacks were most often customer records, followed by trade secrets, R&D, and IP.

SECURITY

While surveyed financial services executives experienced higher rates of fraud and cyber attack than most industries, they were the least likely to have had a security incident. Just under three-fifths (57%) had suffered a security incident, a rate 11 percentage points below the global average. Theft or loss of IP was indicated by participants to be the most common security incident, but participants in the financial services industry were most likely to say they felt highly vulnerable to terrorism.

FINANCIAL SERVICES REPORT CARD

Top responses given by survey respondents.

Fraud

89 — **Percentage of respondents affected by fraud in the past 12 months.**

▲ 19% points above 2015

▲ 7% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	**39%**	29%
	Vendor, supplier, or procurement fraud	**32%**	26%
	IP theft *(e.g., of trade secrets, piracy, or counterfeiting)*	**27%**	16%
MOST COMMON PERPETRATORS	Junior employees	**38%**	39%
	Ex-employees	**34%**	27%
	Senior or middle management employees	**32%**	30%
	Vendors/suppliers	**24%**	26%
	Freelance/temporary employees	**22%**	27%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Risk *(risk officer and risk management system)*	**88%**	78%
	Information *(IT security, technical countermeasures)*	**84%**	82%
	IP *(IP risk assessment and trademark monitoring program)*	**84%**	75%
MOST COMMON MEANS OF DISCOVERY	Through an external audit	**40%**	36%

Cyber Security

89 — **Percentage of respondents that experienced a cyber incident in the past 12 months.**

▲ 4% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Data deletion or loss due to system issues	**30%**	24%
	Email-based phishing attack	**27%**	26%
	Virus/worm infestation	**27%**	33%
MOST COMMON PERPETRATORS	Ex-employees	**28%**	20%
MOST COMMON TARGET	Customer records	**42%**	51%
	Trade secrets/R&D/IP	**38%**	40%
	Company/employee identity	**38%**	36%

Security

57 — **Percentage of respondents that experienced a security incident in the past 12 months.**

▼ 11% points below global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	**34%**	38%
	Geographic and political risk	**20%**	22%
	Workplace violence	**16%**	23%
MOST COMMON PERPETRATORS	Ex-employees	**31%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Terrorism	**21%**	18%
	Workplace violence	**20%**	27%
	Theft or loss of IP	**18%**	19%

Healthcare, Pharmaceuticals, and Biotechnology Overview

FRAUD

Respondents in the healthcare, pharmaceuticals, and biotechnology industry reported slightly fewer instances of fraud than the global average. However, with four in five respondents reporting being affected by fraud in the last 12 months, it is still a substantial issue for the industry.

Consistent with most other industries, junior employees are cited as the most common perpetrators of fraud, while agents and intermediaries have a risk of involvement similar to that of consumer goods (43%) and transportation, leisure and tourism (35%) industries.

Healthcare industry respondents were the most likely to have implemented anti-fraud measures, with over 90% having adopted financial, management, information, and risk (risk officer and risk management system) measures. Whistle-blowers feature significantly when it comes to fraud detection in this industry, drawing attention to 63% of all identified incidents in the past year.

CYBER SECURITY

Close to nine out of ten (86%) participants indicated that their company had experienced a cyber attack in the past 12 months. Consistent with other industries, these most commonly took the form of virus or worm infestations, email-based phishing attack, data breaches resulting in the loss of customer or employee data, or data deletion or corruption by malware or system issue. Attackers primarily targeted customer and employee records or identity information.

SECURITY

Close to two-thirds (65%) of healthcare industry respondents had been effected by a security risk in the past 12 months, with the most common being environmental risk, 8 percentage points higher than the global average. Geographic and political risks were also reported to be higher than average, yet the threat of workplace violence remained the area where most participants felt their companies were highly vulnerable.

Interestingly, the most common perpetrators of security risks for these industries are freelance and temporary employees, while in most industries, ex-employees were reported to be the most common perpetrators of security risks.

HEALTHCARE, PHARMACEUTICALS, AND BIOTECHNOLOGY

Top responses given by survey respondents.

Fraud

80 — **Percentage of respondents affected by fraud in the past 12 months.**

▲ 11% points above 2015

▼ 2% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Vendor, supplier, or procurement fraud	37%	26%
	Theft of physical assets or stock	31%	29%
	Misappropriation of company funds	27%	18%
MOST COMMON PERPETRATORS	Junior employees	44%	39%
	Agents and/or intermediaries	37%	27%
	Senior or middle management employees	34%	30%
	Ex-employees	29%	27%
	Joint venture partners	27%	23%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	94%	77%
	Information *(IT security, technical countermeasures)*	92%	82%
	Management *(management controls, incentives, external supervision such as audit committee)*	92%	74%
	Risk *(risk officer and risk management system)*	92%	78%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	63%	44%

Cyber Security

86 — **Percentage of respondents that experienced a cyber incident in the past 12 months.**

▲ 1% point above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	45%	33%
	Email-based phishing attack	35%	26%
	Data breach resulting in loss of customer or employee data	29%	23%
	Data deletion or corruption by malware or system issue	29%	22%
MOST COMMON PERPETRATORS	Ex-employees	20%	20%
MOST COMMON TARGET	Customer records	48%	51%
	Employee records	48%	40%
	Company/employee identity	45%	36%

Security

65 — **Percentage of respondents that experienced a security incident in the past 12 months.**

▼ 3% points below global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Environmental risk	35%	27%
	Theft or loss of intellectual property	31%	38%
	Geographic and political risk	27%	22%
MOST COMMON PERPETRATORS	Freelance/temporary employees	15%	16%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	35%	27%
	Terrorism	25%	18%
	Theft or loss of IP	20%	19%
	Environmental risk	20%	20%

Manufacturing Overview

FRAUD

Fraud is an almost universal problem for manufacturing companies. They suffered the highest rates of fraud in 2015 and again in 2016, with an increase of 7 percentage points in the latest survey. This now means that nearly 9 out of every 10 respondents in the manufacturing industry experienced at least one kind of fraud in the past year.

These respondents were particularly susceptible to information loss, theft, or attack; along with respondents in the technology, media, and telecoms sector, they were second only to respondents in the consumer goods sector for experiencing this type of fraud. Manufacturing industry respondents were more likely than those in any other industry to have suffered a regulatory or compliance breach.

When it came to preventing and detecting fraud, manufacturing industry respondents were the most likely to already have management anti-fraud measures in place. And while most fraud was detected by a whistle-blower across other industries, for respondents in the manufacturing industry just over half of fraud detected was uncovered by an internal audit.

CYBER SECURITY

Manufacturing companies have also been hit hard by cyber attacks and information loss, theft, or attack. Almost all respondents in the manufacturing industry (91%) have suffered some incident in the past year. While virus or worm infestations were the most common, as they were across most industries, manufacturing industry participants experienced a particularly high rate of data breach resulting in loss of IP, R&D, or trade secrets.

Trade secrets, R&D, or IP were also specifically named as the target by just over half (52%) of all respondents, with customer records being the most targeted (reported by 63% of all respondents).

Unusually, an agent or intemediary was the most likely perpetrator of a cyber incident, responsible in nearly a quarter (23%) of all cases. Ex-employees were the most likely perpetrators of cyber incidents in every other industry except technology, media, and telecoms.

SECURITY

Security incidents are also widespread in this industry, with over four-fifths (81% of respondents) reporting at least one type of security incident in the past year. This was the highest rate across all industries. The most common type of security incident suffered was physical theft of intellectual property (IP).

It was the only industry where competitors were the most likely perpetrators, responsible in almost a quarter (24%) of all security incidents.

While the main threat to manufacturing companies has been to their information and IP, more respondents say they feel highly vulnerable to environmental risks or workplace violence than theft or loss of IP.

MANUFACTURING

Top responses given by survey respondents.

Fraud

89 Percentage of respondents affected by fraud in the past 12 months.

▲ 7% points above higher than 2015

▲ 7% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Information theft, loss, or attack *(e.g., data theft)*	**30%**	24%
	Regulatory or compliance breach	**30%**	21%
	IP theft *(e.g., of trade secrets, piracy or counterfeiting)*	**26%**	16%
MOST COMMON PERPETRATORS	Junior employees	**39%**	39%
	Freelance/temporary employees	**37%**	27%
	Senior or middle management employees	**33%**	30%
	Ex-employees	**33%**	27%
	Vendors/suppliers	**33%**	26%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Management *(management controls, incentives, external supervision such as audit committee)*	**88%**	74%
	Information *(IT security, technical countermeasures)*	**86%**	82%
	Staff *(training, whistle-blower hotline)*	**79%**	74%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	**51%**	39%

Cyber Security

91 Percentage of respondents that experienced a cyber incident in the past 12 months.

▲ 6% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	**39%**	33%
	Data breach resulting in loss of IP/trade secrets/R&D	**35%**	19%
	Email-based phishing attack	**35%**	26%
MOST COMMON PERPETRATORS	Agents and/or intermediaries	**23%**	13%
MOST COMMON TARGET	Customer records	**63%**	51%
	Trade secrets/R&D/IP	**52%**	40%
	Employee records	**44%**	40%

Security

81 Percentage of respondents that experienced a security incident in the past 12 months.

▲ 13% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	**56%**	38%
	Environmental risk	**28%**	27%
	Workplace violence	**26%**	23%
MOST COMMON PERPETRATORS	Competitors	**24%**	12%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Environmental risk	**28%**	20%
	Workplace violence	**21%**	27%
	Theft or loss of IP	**21%**	19%

Fraud Mitigation in Global Manufacturing

BY BRIAN WEIHS, NICOLE LAMB-HALE AND BRIAN SPERLING

The risk of fraud increases dramatically when firms offshore, outsource, or otherwise migrate their manufacturing to emerging markets. Fraud mitigation requires a robust set of tools and strategies including due diligence investigations, comprehensive auditing and monitoring of partners and subsidiaries, and the development of company-wide anti-fraud measures.

Due to the remarkable growth of the middle class in many emerging markets, manufacturing companies must have a presence in those markets to remain competitive. The appeal of lower production costs, the benefits of regional centers of manufacturing expertise, and proximity to customers' global supply chains leaves the industry with little choice but to expand. Unfortunately, such expansion has made the manufacturing sector the most vulnerable to fraud, as highlighted in this year's Kroll Global Fraud and Risk Report survey, which showed that 91% of respondents from the sector had experienced fraud in the past 12 months, the highest incidence of all sectors surveyed.

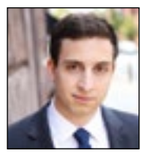
A critical fraud risk in the sector is the loss of intellectual property. For example, in one of Kroll's high-profile cases, a clothing manufacturer learned that authentic versions of its products, not counterfeit goods, were being sold through unauthorized supply channels at far below the market rate. The traditional methods of fraud identification and verification, such as factory walkthroughs and other assessments, proved inadequate to identify the source of these goods.

Kroll conducted an investigation, which found that the Asian vendor was mishandling factory overproduction and the production of lower-quality goods or "seconds." Rather than being disposed of properly, excess supplies and seconds were diverted by managers and sold on the gray market.

In another case, the jerseys of a major sports league were being counterfeited in China. The quality of the counterfeit jerseys was indistinguishable from the actual product; the jerseys were even printed with barcodes corresponding to U.S. retailers. Therefore the sports league was unable to determine if jerseys were excess production or counterfeit goods. Kroll's investigation helped them identify and move towards shutting down the sellers, while the manufacturer deployed proprietary anti-fraud technology to help deter future counterfeiters.

BRIAN WEIHS
Brian Weihs is a Managing Director with Kroll's Investigations and Disputes practice and head of the Mexico office. With over 20 years of experience advising clients across multiple industries on complex matters, Brian is an expert in corporate investigations, corporate governance and compliance, crisis management, and reputational issues, and has led risk management projects and investigations throughout Latin America.

NICOLE LAMB-HALE
Nicole Y. Lamb-Hale is a Managing Director in Kroll's Investigations and Disputes practice, based in the Washington, D.C. office. Nicole has over twenty years of executive-level experience and a unique viewpoint on global commercial and compliance matters from her extensive service in both the public and private sectors. In addition to serving as an Assistant Secretary and Deputy General Counsel at the U.S. Department of Commerce, Nicole has built a distinguished career as a strategic advisor and practicing attorney with top-tier international U.S. advisory and law firms.



BRIAN SPERLING
Brian Sperling is an Associate with Kroll's Investigations and Disputes practice in Philadelphia. With a background in international political economy and information technology, Brian has experience in due diligence and corporate investigations, asset traces, and litigation support.

Operations in far-flung markets challenge a manufacturer's ability to ensure adequate integration into its global strategy and safeguards. Kroll's investigations have uncovered numerous examples of local partners or management taking advantage of the distance to systematically siphon production, customers, and profits into parallel operations for their own benefit.

In two recent cases in a Latin American country, Kroll investigations found that the local management activities of a supplier to the automotive industry and a consumer goods packaging company were so shielded from global management oversight that they were working almost entirely for the benefit of their own networks, while creating significant material and reputational liabilities for the respective global companies. Only through a comprehensive understanding of how this occurred were the global companies able to recover control of their local operations and avoid continued losses and liabilities.

How can manufacturers take advantage of the opportunities in new markets while mitigating their exposure to fraud?

1 Before establishing relationships with partners and third-party vendors in country, conduct due diligence on, among other things, their personal and business reputations, regulatory history, and business practices. These findings (and the relevant parties) should be monitored on an established schedule.

2 When considering a manufacturing joint venture or acquisition, it is not enough to understand the partner or target: the strengths of (and threats to) its whole logistics chain and its relationships must also be understood. Mapping what is key to the business and what should be changed from the outset will help determine the success of the venture.

3 When assessing or managing the risks in a manufacturer's value chain, look beyond fraud and corruption to other compliance issues—for example, labor practices (child labor, modern slavery, substandard work conditions) and community and environmental issues. Also, examine the business' own operations as well as those of its suppliers.

4 After the deal is signed, ensure that global best practices and oversight structures are integrated into the newly acquired operation, and that the local partner or personnel understands the role that these practices and structures play in the global company's strategy.

5 Conduct robust and frequent audits of overseas operations to assess regulatory compliance. Areas of inquiry should include, but not be limited to, compliance with anti-corruption and anti-money laundering regulations, and any applicable sanctions.

6 Identify vulnerabilities in the protection of intellectual property and introduce appropriate measures to secure assets before a loss is suffered.

These strategies will help maximize the opportunities for manufacturers in overseas markets and significantly mitigate fraud as an enterprise risk.

Natural Resources Overview

FRAUD

Consistent with most other industries, respondents from the natural resources sector saw an increase in instances of fraud this year. Four in five respondents now report having being affected by fraud.

It was the only industry in which money laundering was one of the top three most common risks suffered. Money laundering was the equal most common fraud experienced by respondents from the natural resources industry in 2016, alongside vendor, supplier, and procurement fraud.

While in almost every other industry, junior employees were the most likely perpetrators of fraud, for respondents in the natural resources industry, the greatest risk was from freelance and temporary employees. The instance of fraud committed by regulators was also twice that of the global average.

According to respondents in the natural resources industry, half of all instances of fraud uncovered were detected by whistle-blowers.

CYBER SECURITY

Respondents from the natural resources sector experienced an above-average incidence of cyber attacks, with almost nine out of 10 (86%) reporting an incident in the past 12 months. Consistent with other industries, cyber attacks most commonly took the form of a virus or worm infestation. Three in ten respondents from the natural resources industry experienced lost equipment with sensitive data, which was almost twice the rate of other industries. Attacks most frequently targeted customer and employee records, as well as physical assets and money.

SECURITY

The most common security incident reported by respondents from the natural resources industry in the past 12 months was the theft or loss of intellectual property. Permanent employees were the most likely perpetrator of security incidents.

NATURAL RESOURCES

Top responses given by survey respondents.

Fraud

80 — Percentage of respondents affected by fraud in the past 12 months.

▲ 3% points above 2015

▼ 2% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Vendor, supplier, or procurement fraud	30%	26%
	Money laundering	30%	15%
	Management conflict of interest	28%	21%
MOST COMMON PERPETRATORS	Freelance/temporary employees	35%	27%
	Junior employees	30%	39%
	Ex-employees	30%	27%
	Joint venture partners	30%	23%
	Senior or middle management employees	28%	30%
	Regulators	28%	14%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Information *(IT security, technical countermeasures)*	80%	82%
	IP *(IP risk assessment and trademark monitoring program)*	80%	75%
	Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	78%	77%
	Partners, clients, and vendors *(due diligence)*	78%	77%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	50%	44%

Cyber Security

86 — Percentage of respondents that experienced a cyber incident in the past 12 months.

▲ 1% point above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	36%	33%
	Lost equipment with sensitive data	30%	17%
	Data breach resulting in loss of customer or employee data	24%	23%
	Data breach resulting in loss of IP/trade secrets/R&D	24%	17%
	Data deletion by malicious insider	24%	19%
MOST COMMON PERPETRATORS	Ex-employees	19%	20%
MOST COMMON TARGET	Employee records	58%	40%
	Customer records	53%	51%
	Physical assets/money	47%	38%

Security

70 — Percentage of respondents that experienced a security incident in the past 12 months.

▲ 2% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	40%	38%
	Environmental risk	38%	27%
	Workplace violence	36%	23%
MOST COMMON PERPETRATORS	Permanent employees of our own company	26%	17%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	36%	27%
	Environmental risk	26%	20%
	Theft or loss of intellectual property	24%	19%

Professional Services Overview

FRAUD

A significant majority (84%) of respondents from professional services firms detected instances of fraud in the past 12 months. Alongside respondents from manufacturing companies, this industry saw the greatest increase over the past year, up 12 percentage points since 2015. Junior employees were most likely to be responsible for fraud, while senior and middle-management employees were involved in fewer cases than in other industries.

In detecting and preventing fraud, the majority of respondents from professional services firms (82%) have partner, client, and vendor due diligence processes in place, and a similar number (80%) indicated the existence of a risk management system and risk officer.

Like in most other industry sectors, whistle-blowers uncovered the majority of fraud cases in the past year, but management also played an important role. Over a third (37%) of fraud was detected by management, compared with 32% across all industries.

CYBER SECURITY

Not surprisingly, cyber security remains a major concern for the professional services industry, with more than four in five (84%) participants reporting that their company had experienced a cyber incident, in line with the global average. The type, frequency, targets, and perpetrators of cyber incidents in the professional services industry were very similar to those experienced across other industry sectors. However, the instance of denial of service attacks was higher, and trade secrets, R&D, or IP were less likely to be the target of an attack than in other industries.

SECURITY

Security risks were less prevalent among professional service firms, with a reported incidence in the past year 5 percentage points below the global average. Of those that occurred, ex-employees were the most common perpetrators, and theft of intellectual property (IP) the most likely type of security breach.

One in five (20%) participants also indicated that they had suffered an incident of workplace violence, and when asked what security risks their company was most vulnerable to, over a quarter (27%) were concerned with this potential physical threat.

On the other hand, over a third (35%) had suffered theft or loss of IP, while only one in ten said they felt highly vulnerable to this type of threat.

PROFESSIONAL SERVICES

Top responses given by survey respondents.

Fraud

84 — Percentage of respondents affected by fraud in the past 12 months.

▲ 12% points above 2015

▲ 2% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Management conflict of interest	29%	21%
	Theft of physical assets or stock	29%	29%
	Information theft, loss, or attack *(background screening)*	20%	24%
MOST COMMON PERPETRATORS	Junior employees	35%	39%
	Freelance/temporary employees	28%	27%
	Ex-employees	26%	27%
	Senior or middle management employees	23%	30%
	Customers	21%	19%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Partners, clients, and vendors *(due diligence)*	82%	77%
	Risk *(risk officer and risk management system)*	80%	78%
	Assets *(physical security systems, stock inventories, tagging, asset register)*	78%	79%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	42%	44%

Cyber Security

84 — Percentage of respondents that experienced a cyber incident in the past 12 months.

▼ 1% point below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	35%	33%
	Denial of service attack	20%	14%
	Data deletion or corruption by malware or system issue	20%	22%
MOST COMMON PERPETRATORS	Ex-Employees	23%	20%
MOST COMMON TARGET	Customer records	53%	51%
	Trade secrets/R&D/IP	30%	40%
	Company/employee identity	28%	36%
	Physical assets/money	28%	38%

Security

63 — Percentage of respondents that experienced a security incident in the past 12 months.

▼ 5% points below global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	35%	38%
	Environmental risk	22%	27%
	Workplace violence	20%	23%
MOST COMMON PERPETRATORS	Ex-Employees	38%	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	27%	27%
	Terrorism	14%	18%
	Theft or loss of IP	10%	19%
	Environmental risk	10%	20%

Retail, Wholesale, and Distribution Overview

FRAUD

Respondents from retail, wholesale, and distribution companies reported a slight (4 percentage points) increase in fraud over the last 12 months, raising overall levels to 83%. Theft of physical assets or stock was the most common type of fraud, while misappropriation of company funds was significantly more likely than in other industries. It was the only sector where misappropriation of company funds was in the top two most common types of fraud.

Consistent with other industry sectors, junior employees were most frequently responsible for fraud. Customers also made it onto the list of the five most likely perpetrators of fraud, playing a part in over a quarter (26%) of all cases.

Respondents from retail, wholesale, and distribution companies reported above-average adoption of financial, asset, and information controls. They were the most likely of any industry group to have implemented asset security measures.

CYBER SECURITY

This industry's figures for cyber attacks were slightly above the global average, and respondents experienced a wide range of different types of cyber attacks. Email phishing attacks and insider theft of customer or employee data were the most commonly reported types of cyber incident, and customer records were the most common target.

Many different perpetrators were involved in cyber incidents, making managing cyber risks in this industry particularly complex. Ex-employees, freelance and temporary staff, and joint venture partners were all implicated equally (13%). Unique to retail, accidental placement of sensitive data that was then indexed by a search engine was among the most common causes behind a cyber incident.

SECURITY

Retail industry respondents reported the second highest rate of security risks, after manufacturing. Nearly four-fifths (79%) of respondents said they had suffered from some kind of security incident in the past year. The terrorist threat is more acute in this industry than others. It was the second most common type of security risk experienced, and an area where almost a third (31%) felt highly vulnerable.

RETAIL, WHOLESALE, AND DISTRIBUTION

Top responses given by survey respondents.

Fraud

83 — Percentage of respondents affected by fraud in the past 12 months.

▲ 4% points above 2015

▲ 1% point above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	33%	29%
	Misappropriation of company funds	25%	18%
	Information theft, loss, or attack *(e.g., data theft),*	17%	24%
	Vendor, supplier, or procurement fraud	17%	26%
MOST COMMON PERPETRATORS	Junior employees	37%	39%
	Senior or middle management employees	33%	30%
	Vendors/suppliers	33%	26%
	Agents and/or intermediaries	26%	27%
	Joint venture partners	26%	23%
	Customers	26%	19%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Assets *(physical security systems, stock inventories, tagging, asset register)*	85%	79%
	Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	83%	77%
	Information *(IT security, technical countermeasures)*	83%	82%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	42%	44%

Cyber Security

87 — Percentage of respondents that experienced a cyber incident in the past 12 months.

▲ 2% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Email-based phishing attack	25%	26%
	Insider theft of customer or employee data	21%	19%
	Data breach resulting in loss of customer or employee data	19%	23%
	Data breach resulting in loss of IP/trade secrets/R&D	19%	17%
	Denial of service attack	19%	14%
MOST COMMON PERPETRATORS	Freelance/temporary employees	13%	14%
	Ex-employees	13%	20%
	Joint venture partners	13%	6%
	Accidental placement of sensitive data that was indexed by a search engine *(e.g., Google)*	13%	10%
MOST COMMON TARGET	Customer records	44%	51%
	Employee records	40%	40%
	Physical assets/money	36%	38%

Security

79 — Percentage of respondents that experienced a security incident in the past 12 months.

▲ 11% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	38%	38%
	Terrorism	19%	15%
	Geographic and political risk	19%	22%
MOST COMMON PERPETRATORS	Freelance/temporary employees	22%	16%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Terrorism	31%	18%
	Workplace violence	29%	27%
	Geographic and political risk	19%	12%

Technology, Media, and Telecoms Overview

FRAUD

Respondents in the technology, media, and telecoms (TMT) industry were the second least likely industry group to have experienced fraud in the past year. It was one of only two industries – the other was construction engineering, and infrastructure – which did not see a rise in fraud over the previous year.

However, this still meant that almost four-fifths (79%) had suffered at least one type of fraud in the period.

Theft of physical assets or stock was the most common type of fraud (experienced by 35% of respondents). This was followed by information theft, loss, or attack, suffered by 30% of TMT companies. This was 6 percentage points higher than the rate experienced by respondents across all industries. A quarter had experienced a management conflict of interest, which was also higher than the average for all industries.

Compared to other industries, TMT respondents experienced, on average, notably fewer incidents of vendor, supplier, or procurement fraud (8 percentage points less).

TMT companies were more likely than others to have already adopted anti-fraud measures to protect physical assets.

CYBER SECURITY

Contrary to the global trend, these respondents were slightly less likely to say they had experienced a cyber incident than fraud. Interestingly, given the nature of their businesses, the rate of cyber attack or information loss, theft, or attack was significantly lower than the global industry average (8 percentage points below).

Perhaps because of the higher proportion of freelance employees in the technology industry in particular, TMT was the only industry group where freelance and temporary employees were the most likely perpetrators of cyber incidents.

SECURITY

The TMT industry had the third highest rate of security incidents over the past year, after manufacturing and retail industry respondents. Nearly three-quarters (72%) had experienced a security incident, with almost half having suffered from theft or loss of intellectual property.

Freelance and temporary employees were also the most likely perpetrators of security incidents, responsible for over a quarter (27%) of all incidents suffered by TMT respondents in the past year.

TECHNOLOGY, MEDIA, AND TELECOMS

Top responses given by survey respondents.

Fraud

79 — **Percentage of respondents affected by fraud in the past 12 months.**

= equal to 2015

▼ 3% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	35%	29%
	Information theft, loss, or attack	30%	24%
	Management conflict of interest	25%	21%
MOST COMMON PERPETRATORS	Junior employees	42%	39%
	Senior or middle management employees	36%	30%
	Ex-employees	27%	27%
	Freelance/temporary employees	22%	27%
	Vendors/suppliers	22%	26%
	Regulators	22%	14%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Assets *(physical security systems, stock inventories, tagging, asset register)*	82%	79%
	Financial *(financial controls, internal/external audit, anti-money laundering policies)*	79%	77%
	Partners, clients, and vendors *(due diligence)*	79%	77%
	Risk *(risk officer and risk management system)*	79%	78%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	40%	39%

Cyber Security

77 — **Percentage of respondents that experienced a cyber incident in the past 12 months.**

▼ 8% points below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	37%	33%
	Email-based phishing attack	32%	26%
	Data deletion or loss due to system issues	23%	24%
MOST COMMON PERPETRATORS	Freelance/temporary employees	23%	14%
MOST COMMON TARGET	Physical assets/money	48%	38%
	Trade secrets/R&D/IP	43%	40%
	Company/employee identity	43%	36%

Security

72 — **Percentage of respondents that experienced a security incident in the past 12 months.**

▲ 4% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	46%	38%
	Environmental risk	33%	27%
	Geographic and political risk	26%	22%
MOST COMMON PERPETRATORS	Freelance/temporary employees	27%	16%
RESPONDENTS COMPANIES ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	28%	27%
	Terrorism	21%	18%
	Environmental risk	18%	20%

Transportation, Leisure, and Tourism Overview

FRAUD

At 85%, the transportation, leisure, and tourism industry respondents experienced a 10 percentage point increase in fraudulent activity over the last 12 months, raising the overall level to 3 percentage points above the global average.

Similar to other industries, junior employees were the most common perpetrators (a responsible party in 39% of all fraud cases), closely followed by agents and intermediaries (35% of cases).

There was widespread adoption of all the listed anti-fraud measures by respondents in this sector, second only to those in the healthcare industry. More than 80% had implemented each of the top four measures listed in the report card.

CYBER SECURITY

This industry had the equal third highest rate (87%) of cyber incidents, which were most commonly virus and worm infestations. Transportation industry respondents also suffered the alteration or change of customer data at almost twice the global average.

SECURITY

Over two-thirds (70%) of industry respondents have reported a security incident over the last 12 months, with theft of intellectual property (IP) a particular issue for the industry. At 30%, workplace violence is reported at 7 percentage points above global average levels, with the main perpetrators of incidents equally likely to be permanent employees or ex-employees.

TRANSPORTATION, LEISURE, AND TOURISM

Top responses given by survey respondents.

Fraud

85 — Percentage of respondents affected by fraud in the past 12 months.

▲ 10% points above 2015

▲ 3% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	33%	29%
	Vendor, supplier, or procurement fraud	30%	26%
	Regulatory or compliance breach	26%	21%
MOST COMMON PERPETRATORS	Junior employees	39%	39%
	Agents and/or intermediaries	35%	27%
	Freelance/temporary employees	30%	27%
	Senior or middle management employees	26%	30%
	Joint venture partners	22%	23%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Information *(IT security, technical countermeasures)*	89%	82%
	Assets *(physical security systems, stock inventories, tagging, asset register)*	87%	79%
	Board of director engagement in cyber security policies and proceduress	85%	75%
	Staff *(background screening)*	85%	74%
	Risk *(risk officer and risk management system)*	78%	78%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	46%	44%

Cyber Security

87 — Percentage of respondents that experienced a cyber incident in the past 12 months.

▲ 2% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	37%	33%
	Alteration or change of customer data	31%	16%
	Data deletion or loss due to system issues	30%	24%
MOST COMMON PERPETRATORS	Ex-employees	19%	20%
MOST COMMON TARGET	Customer records	51%	51%
	Physical assets/money	51%	38%
	Employee records	45%	40%
	Trade secrets/R&D/IP	45%	40%

Security

70 — Percentage of respondents that experienced a security incident in the past 12 months.

▲ 2% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	43%	38%
	Workplace violence	30%	23%
	Environmental risk	26%	27%
MOST COMMON PERPETRATORS	Permanent employees of our own company	24%	17%
	Ex-employees	24%	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	41%	27%
	Environmental risk	35%	20%
	Theft or loss of IP	31%	19%

A Closing Note

I hope you have found our report to be both informative and useful. Viewing the landscape through the lens of your peers in business and measuring it against your own day at the office can be reassuring or it can be a call to action, but we hope always enlightening.

When my co-chairman Tommy Helsby (the author of this report's Introduction) and I began our work at Kroll more than 30 years ago, we investigated corrupt employees and other wrongdoers who stole money, trade secrets, company products, and company property. Some bribed government officials for contracts – or accepted bribes from vendors for their company's business; some counterfeited products. Those who stole on a major scale – the "carnivores" we called them – tried to hide their ill-gotten gains behind a fog of anonymous companies.

Well, the crimes haven't changed but some of the tools have. What a corrupt employee or criminal stole with a forged check or from a file in a drawer now is often heisted electronically. Companies are under relentless attacks from hackers and phishers.

The challenges businesses face today have also grown more complex due to globalization and connectivity. Much of business crime is opportunistic. And our findings show that some of the most opportunistic perpetrators are employees and insiders, past and present.

So, how can your company make itself an unattractive target for business crime? Based on our experience, as well as what the survey respondents told us, risk management programs that address the issue from multiple vantage points — including prevention, detection, and response — can better thwart fraudsters and mitigate the harm they do.

My colleagues who contributed articles to this report have provided best practices and real-world examples of how companies can reap significant benefits when they integrate and invest resources in these critical areas. But we know everyone's situation is unique. As we have done for 45 years, Kroll stands ready to help your company investigate fraud of any kind, and mitigate risk.

DANIEL KARSON
Co-Chairman, Investigations and Disputes, Kroll

Contact Kroll

For information about any of Kroll's services, please contact a representative in one of our offices below or visit www.kroll.com

CORPORATE HEADQUARTERS
600 Third Avenue, New York, NY 10016

Global Representatives

NORTH AMERICA

Bill Nugent
Philadelphia
T +1 215.568.8090
bnugent@kroll.com

EUROPE, MIDDLE EAST & AFRICA

Tom Everett-Heath
London
T +44 20 7029.5067
teverettheath@kroll.com

ASIA

Tadashi Kageyama
Singapore
T +65 6645.4959
tkageyama@kroll.com

LATIN AMERICA

Recaredo Romero
Bogotá
T +57 1 742.5556
rromero@kroll.com

Local Offices

NORTH AMERICA

Dan Karson
New York
T +1 212.833.3266
dkarson@kroll.com

Daniel Linskey
Boston
T +1 617. 210.7471
daniel.linskey@kroll.com

Peter Turecek
Chicago
T +1 312.765.8753
pturecek@kroll.com

Erik Rasmussen
Los Angeles
T +1 213.443.1128
erik.rasmussen@kroll.com

Mark Ehlers
Philadelphia
T +1 215.568.8305
mehlers@kroll.com

Betsy Blumenthal
San Francisco
T +1 415.743.4825
bblument@kroll.com

Peter McFarlane
Toronto
T +1 416.813.4401
pmcfarlane@kroll.com

EUROPE, MIDDLE EAST & AFRICA

Neil Kirton
London
T +44 20 7029.5000
nkirton@kroll.com

Tom Everett-Heath
Dubai
T +971 4 4496700
teverettheath@kroll.com

Marcelo Correia
Madrid
T +34 91 274.79.74
marcelo.correia@kroll.com

Marianna Vintiadis
Milan
T +39 02 86998088
mvintiadis@kroll.com

Alex Volcic
Moscow
T +7 495 9692898
avolcic@kroll.com

Béchir Mana
Paris
T +33 1 42678146
bmana@kroll.com

ASIA

Violet Ho
Hong Kong/Beijing/Shanghai
T +86 10 5964.7600
vho@kroll.com

Reshmi Khurana
Mumbai
T +91 22 6724.0504
rkhurana@kroll.com

Richard Dailly
Singapore
T +65 6645.4521
rdailly@kroll.com

Omer Erginsoy
Singapore
T +65 6645.4530
oerginsoy@kroll.com

Naoko Murasaki
Tokyo
T +81 3 3509.7103
nmurasaki@kroll.com

LATIN AMERICA

James Faulkner
Miami
T +1 305.789.7130
jfaulkner@kroll.com

Recaredo Romero
Bogotá
T +57 1 742.5556
rromero@kroll.com

Brian Weihs
Mexico City
T +52 55 5279.7250
bweihs@kroll.com

Juan Cruz Amirante
Buenos Aires
T +54 11 4706.6000
jcamirante@kroll.com

Glen Harloff
São Paulo
T +55 11 3897.0892
gharloff@kroll.com

kroll.com