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.

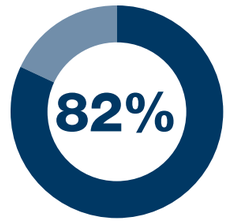
The findings of this year's survey paint a picture of a global business environment fraught with high and mounting risks and repercussions; increasing complexity in the types of risk, perpetrators, and means of attack; and adoption of risk mitigation policies and procedures to help build corporate resilience.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

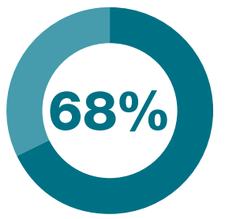
CYBER SECURITY

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

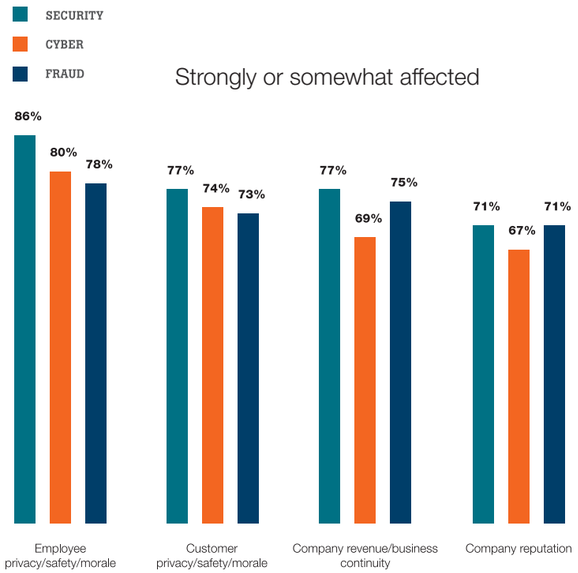
The survey indicates that the experience of a fraud, cyber, or security incident has widespread repercussions for a company's employees and customers as well as its revenue and reputation.

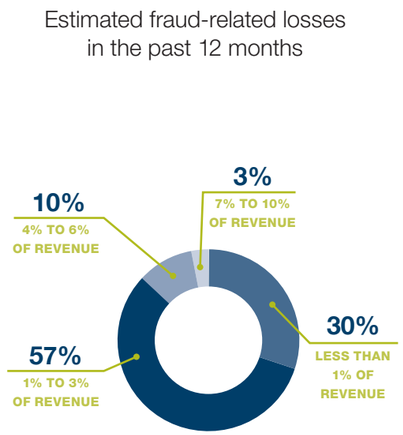
- The most common repercussion noted was the impact on employees: 86% of respondents who reported experiencing a security incident said that employee privacy/safety/morale was strongly or somewhat affected. This level of employee impact was reported by 80% of respondents who cited a cyber incident and 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 40 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 60 and 64 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 82, there are steps manufacturing companies, and others working in different sectors, can take to reduce the risk of operating in emerging markets.

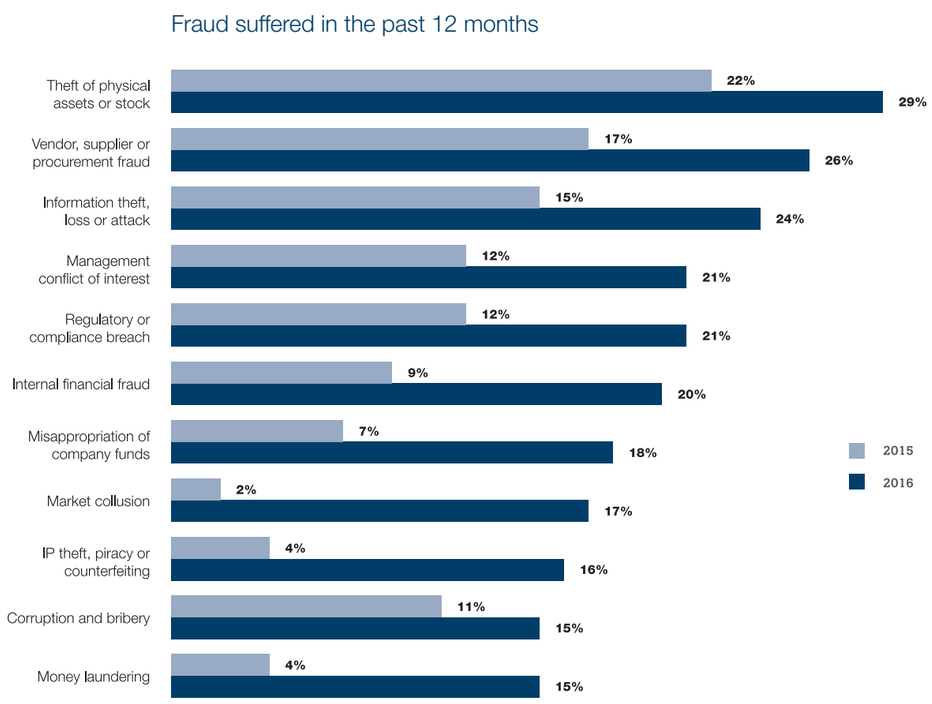
2 The complexity of the threat

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

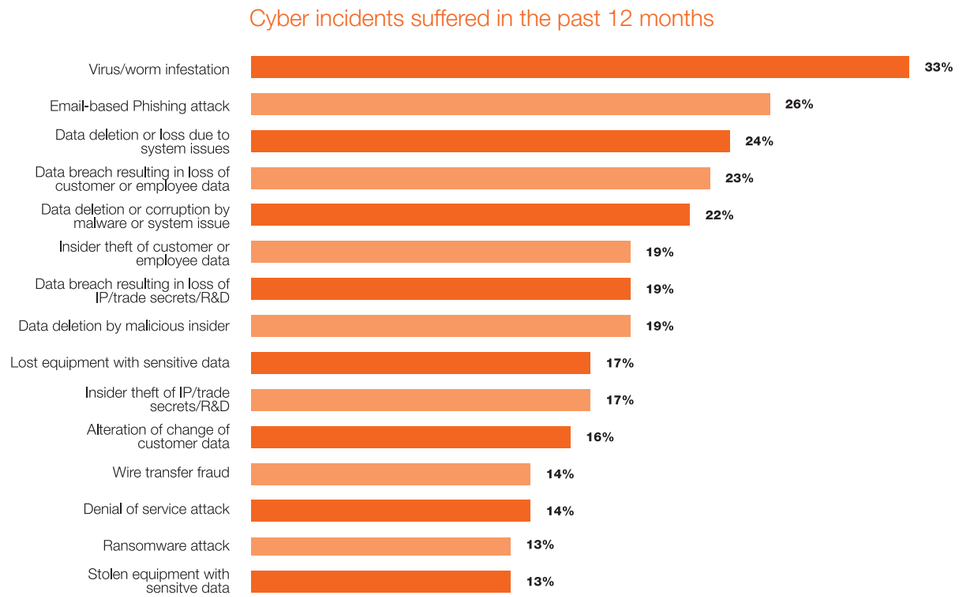
In the past year, respondents reported experiencing more of every type of fraud than was cited in the 2015 survey. Moreover, the stated incidence of every type has now reached double-digit levels.



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.

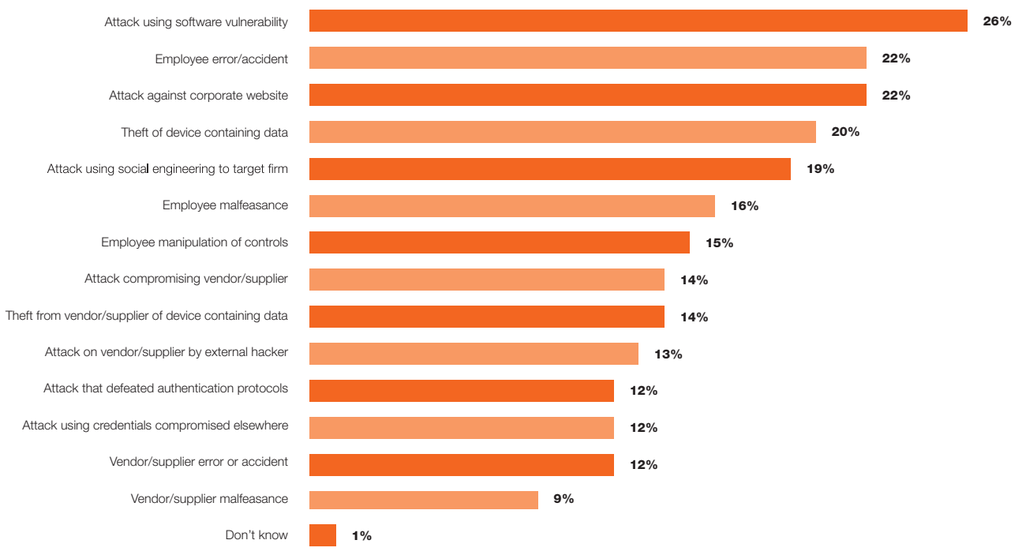
- **Data breach:** Nearly a quarter (23%) of respondents said data breaches resulted in loss of customer or employee data, while 19% cited loss of IP/trade secrets/R&D from a data breach.
- **Data deletion:** 24% of surveyed executives indicated they had experienced data deletion incidents due to system 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.

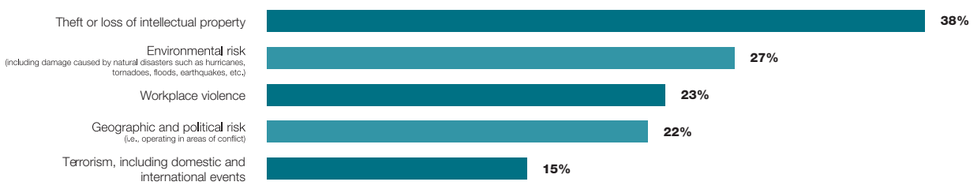
If your company has suffered from cyber attack or information loss, theft, or attack in the past 12 months, which best describes how this took place?
(Participants were asked to select up to three responses.)



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 36 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

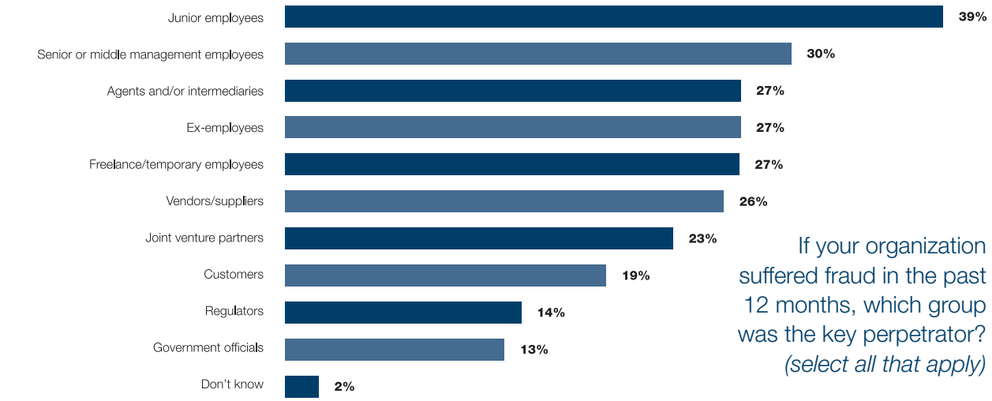
In total, 56% of executives surveyed said insiders were the key perpetrators of security incidents, citing ex-employees (23%), permanent employees (17%), and temporary/freelance employees (16%).

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

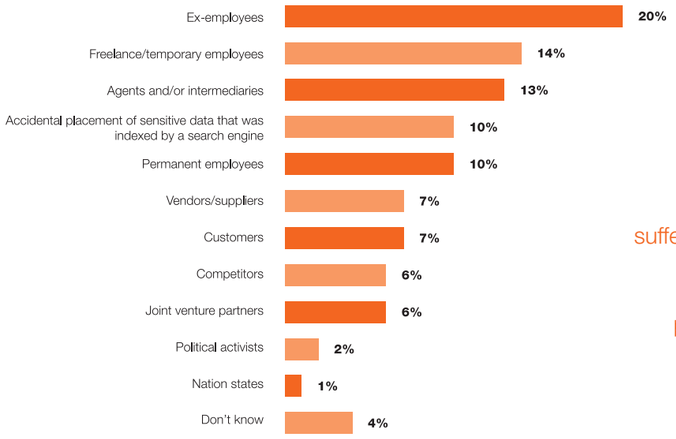
The survey showed a consistently high percent of respondents who disclosed that ex-employees were key perpetrators of fraud (27%), cyber incidents (20%), and security incidents (23%). Kroll experts Marianna Vintiadis and Tadashi Kageyama take on this topic in their article on page 26, in which they discuss some ways companies can carefully manage employee exits.

Perpetrators of fraud



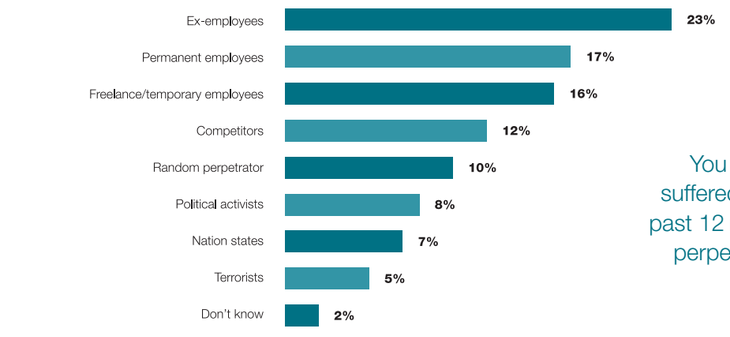
If your organization suffered fraud in the past 12 months, which group was the key perpetrator? *(select all that apply)*

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)*

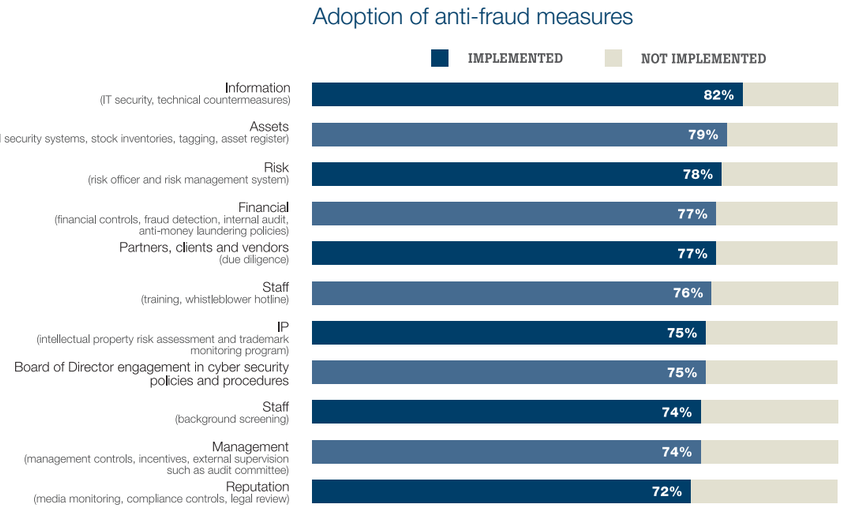
3 The road to resilience

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

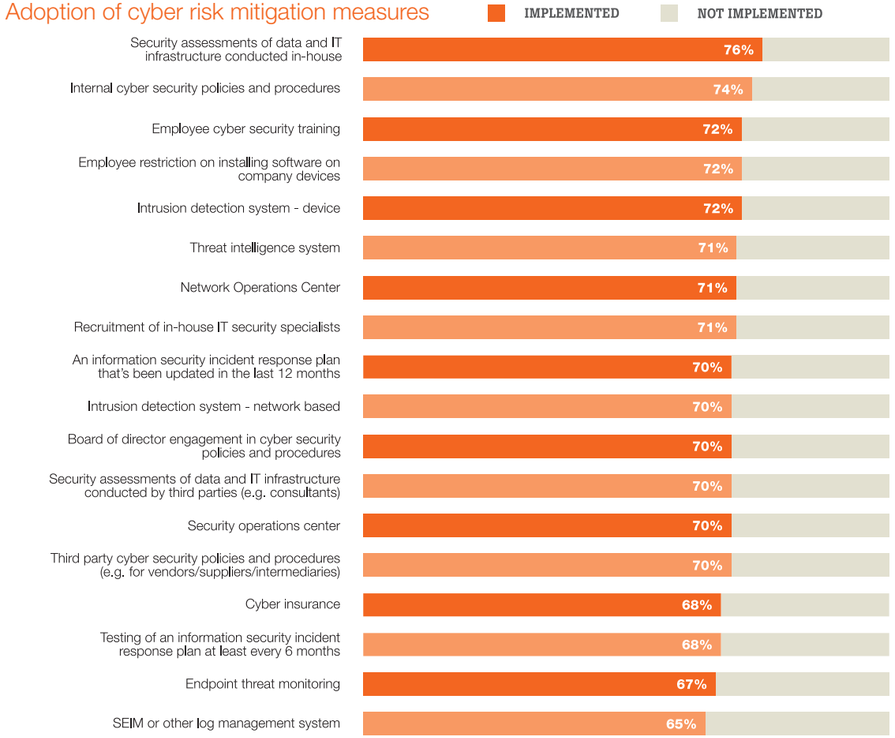
FRAUD RISK MITIGATION MEASURES



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 32.

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.

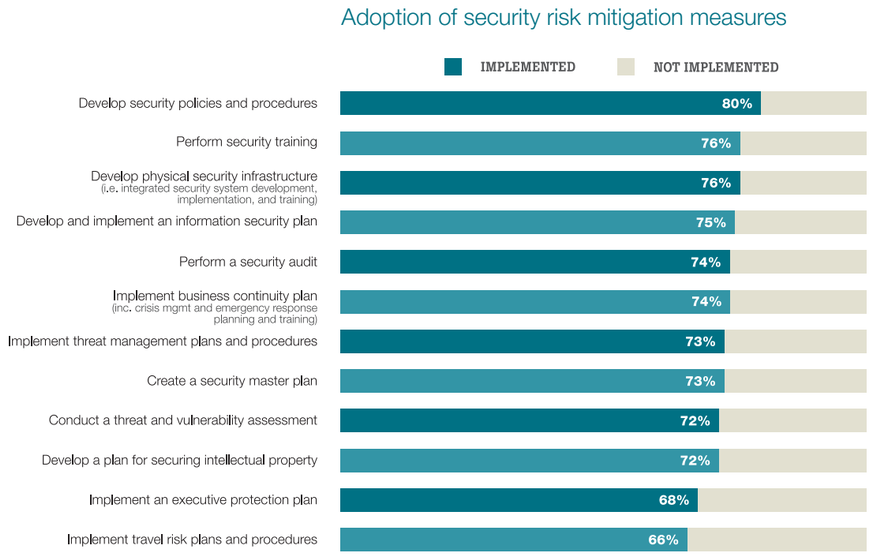
As discussed previously, 44% of cyber incidents were perpetrated by insiders (permanent staff, temporary/freelancers, ex-employees), and this reality is reflected in the adoption of internal training and policies: 72% have introduced employee cyber security training and an equal percentage have employee 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 and Michael Quinn, address the importance of a robust, tested incident response plan in their article on page 38.

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 30, 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 24 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.