Kroll

Global Fraud & Risk Report

Forging New Paths in Times of Uncertainty

10TH ANNUAL EDITION - 2017/18

FORRESTER®

Kroll commissioned research conducted by Forrester Consulting.

ABOUT THE RESEARCH METHODOLOGY

For the 2017/2018 Global Fraud & Risk Report (the "Report"), Kroll commissioned Forrester Consulting to conduct an online worldwide survey of 540 senior executives who hold positions across multiple industries and geographies. The survey was fielded through June and August 2017.

This study builds on last year's analysis of fraud, cyber, and security risks. This year, a number of modifications to survey questions were implemented, primarily in the cyber section, to reflect changes in how cyber threats manifest themselves and the responses these threats elicit from industry professionals. The Report highlights any variations to the survey questions that impact the analysis of data.

As with prior studies, respondents represented a variety of industry sectors, including (1) Construction, Engineering, and Infrastructure; (2) Consumer Goods; (3) Financial Services; (4) Healthcare, Pharmaceuticals, and Biotechnology; (5) Manufacturing; (6) Natural Resources; (7) Professional Services; (8) Retail, Wholesale, and Distribution; (9) Technology, Media, and Telecoms; as well as (10) Transportation, Leisure, and Tourism.

Respondents held senior positions within their companies, with 69% of respondents representing a C-suite, chief counsel, or board member level of seniority. 84% of companies surveyed had annual revenues of $500 million or more.

Respondents represented all major global geographies, including 20% from Europe, 20% from Asia-Pacific, 20% from North America, 19% from Latin America,11% from the Middle East, and 10% from Sub-Saharan Africa.

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

Foreword

Forty-five years ago, Kroll pioneered the business investigation industry. Since that time, Kroll has acquired a unique perspective on risk — encountering a variety of situations ranging from threats that persist for decades to new and emerging dangers that can quietly sabotage organizations and/or strike with alarming speed and without warning. Over this entire time period, there is one constant: Risk, in its many forms, is an ever-present threat to the people, assets, and reputation of an enterprise.

This 10th edition of the Kroll Global Fraud & Risk Report continues our long-standing commitment to sharing the knowledge and insight that is unique to Kroll and its time-tested expertise. Our ultimate goal is to facilitate the adoption of best practices as well as the development of pragmatic solutions to these complex risks, all within a framework informed by regional and global realities.

I invite you to read how organizations around the world and across business sectors are navigating the current risk landscape. I believe you will also find the additional commentary from several of our Kroll practitioners who work on the front lines — delivering investigative, compliance, cyber, breach notification, and security solutions — to be particularly instructive and useful.

One of the Report's findings with the greatest implication for organizations is that many risks can no longer be neatly categorized and labeled as fraud-, cyber-, or security-related. Instead, due to the convergence of a global economy, growing digital connections, and ever-constant human behavioral factors, organizations must adopt a holistic approach to enterprise risk management and develop integrated risk mitigation strategies to address this new threat environment.

Kroll has the ability to bring together multidisciplinary teams of experts and to combine these teams with data analytics, language skills, and technology solutions – anywhere, anytime – to assist clients in understanding and navigating this new world of RISK. We stand ready to provide clients with the knowledge and intelligence edge that will help them to anticipate, detect, mitigate, and respond to risk, both today and into the future.

David R. Fontaine
Chief Executive Officer
Kroll

Table of Contents

Research Summary

Introduction

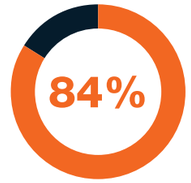
Welcome to the 10th edition of the Kroll Global Fraud & Risk Report. This year's Report addresses the diverse range of fraud-, cyber-, and security-related challenges that organizations are facing around the world and across a variety of industry sectors. In this Report, executives offer an insider's perspective on the nature of incidents their organizations have experienced over the last 12 months, along with insights into the perpetrators and methods employed. These executives also share specific steps they are taking to anticipate, detect, mitigate, and respond to an expanding and increasingly complex set of risks that bring with them material consequences, including potentially adverse financial and reputational impacts.

Heightened Incidence and Substantial Repercussions

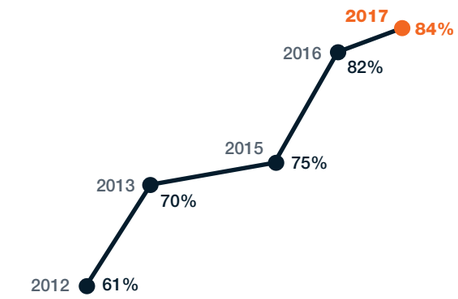
All-time High Incidence

FRAUD

The incidence of fraud continued to climb this year. Overall, 84% of surveyed executives report their company fell victim to at least one instance of fraud in the past 12 months, up from 82% in 2016. This represents a continuous, year-on-year rise since 2012, when the reported incidence was 61%.



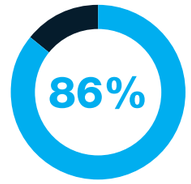
▲ **2%** above 2016



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

CYBER

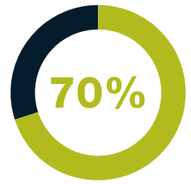
Having already reported a "new normal" incidence level of 85% in 2016, this year 86% of surveyed executives said that their company experienced a cyber incident or information/data theft, loss, or attack in the last 12 months. In some countries and industries, however, the number verges on nearly 100%.



▲ **1%** above 2016

SECURITY

70% of respondents reported the occurrence of at least one security incident at their company during the last year, up from the reported 68% incidence level in 2016.



▲ **2%** above 2016

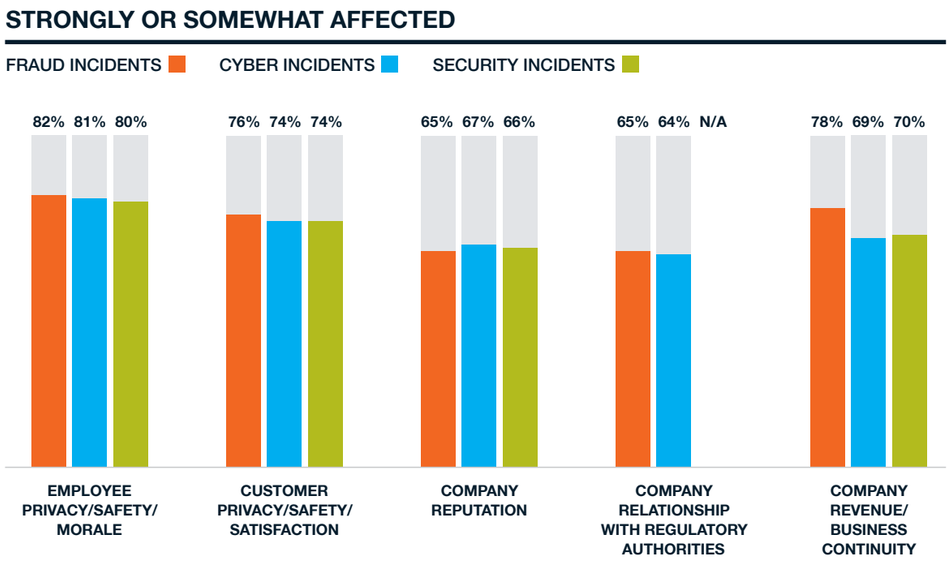
Widespread Substantial Repercussions

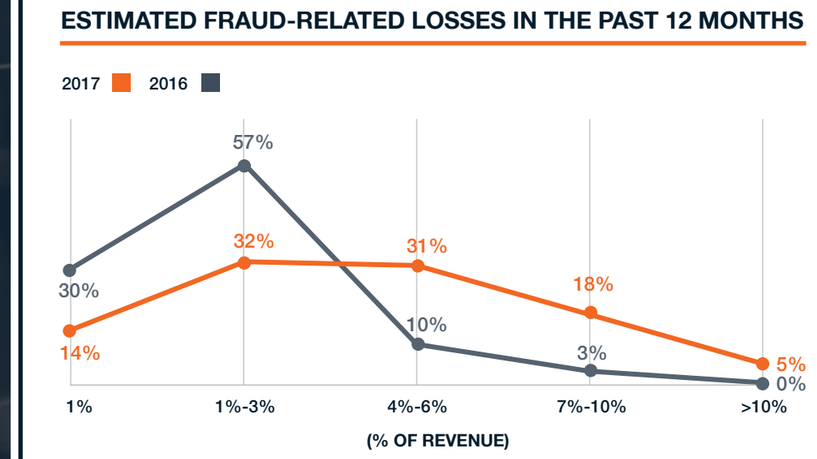
In addition to reporting extremely high incidence levels, survey respondents indicated that the repercussions were both costly and wide-ranging – negatively impacting employees, customers, reputation, relationships with regulators, and revenue.

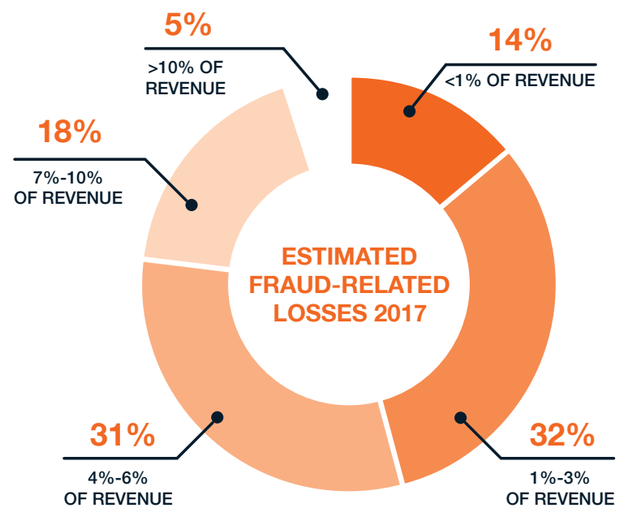
- Not surprisingly, the most extensive repercussion noted was the impact on **employees:** employee privacy/safety/morale was strongly or somewhat negatively affected according to 82% of surveyed executives whose company suffered a fraud incident, 81% of those experiencing a cyber incident, and 80% of executives whose company endured a security incident.
- Roughly three-quarters of respondents stated that their **customers** were strongly or somewhat negatively impacted by all three risk sectors: fraud (76%), cyber (74%), and security (74%).
- Nearly two-thirds of executives indicated that they took a hit to their company's **reputation:** 65%, 67%, and 66% for a fraud, cyber, or security incident, respectively.
- In a global landscape undergoing shifting regulation and regulatory enforcement, 65% of respondents who cited a fraud incident said it strongly or somewhat negatively impacted their company's relationship with **regulatory authorities.**
- 78% of executives whose companies were victims of fraud stated that their company's **revenue/business continuity** was strongly or somewhat negatively affected. Similarly, 70% of respondents who suffered a security incident and 69% of those who experienced a cyber incident reported an adverse impact on their revenue/business continuity.

Stolen money and assets are often hidden across multiple, complex jurisdictions, where it is traditionally hard to locate and recover them. **In their article on page 26,** Glen Harloff, Dan Karson, and Alex Volcic explain how organizations that seek expert help are often able to recoup a significant portion of such losses, even in jurisdictions where it is difficult to obtain recoveries.

To what extent have the following been negatively affected by [fraud/cyber/security] incidents at your company?







Indeed, survey respondents claimed significant economic damage from fraud. In this year's survey, nearly half of respondents (46%) reported losses of 3% or less of company revenues. Notably, 23% of respondents reported losses of 7% or more of revenues; last year, only 3% of respondents reported this scale of loss. Of the respondents who reported losses of 7% or more, 69% were in two industries: Retail, Wholesale, and Distribution (35%) and Construction, Engineering, and Infrastructure (34%).

In their article on page 28, Tarun Bhatia, Reshmi Khurana, Oliver Stern, and Brian Weihs examine the risks associated with infrastructure investments in emerging markets across Sub-Saharan Africa, Latin America, and South Asia, and potential strategies for mitigating these risks.

Confidential Information Under Increasing Threats

In a digitized world – characterized by massive increases in data creation, collection, and reliance for all manner of business – information has become increasingly valuable and vulnerable. Criminals are continually finding new ways to monetize confidential information, including personal data. Employees often have access to highly sensitive information that can be accidentally or intentionally publicized, stolen, or deleted. Furthermore, for some companies, intellectual property and trade secrets are their most valuable assets, and they now find these treasures susceptible to new and growing threats.

TYPES OF FRAUD

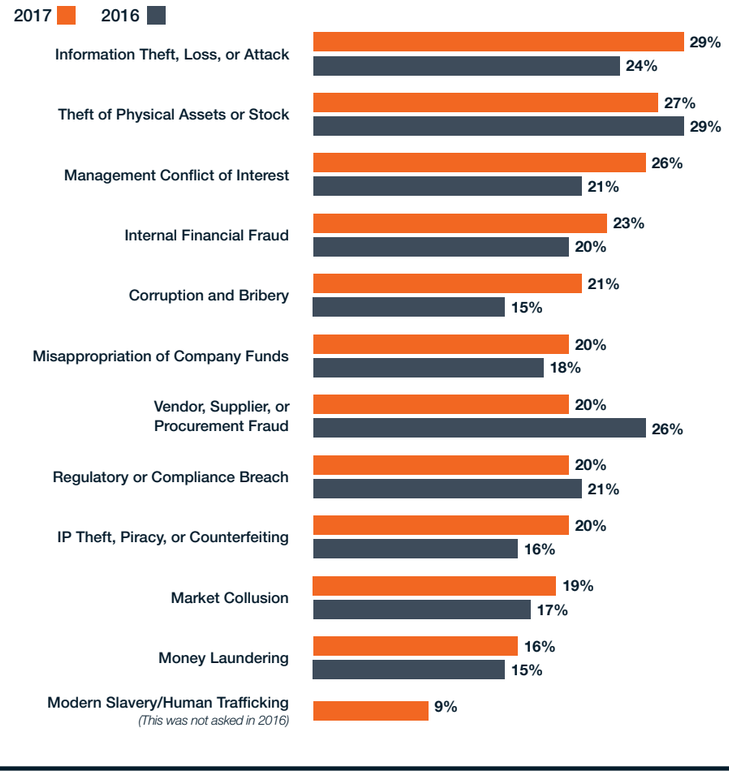
For the first time in 10 years of reporting, information theft, loss, or attack was the most prevalent type of fraud experienced in the last year, cited by 29% of respondents, up 5 percentage points from 24% of respondents in the 2016 survey. This in turn was up 7 percentage points from 22% of respondents in the 2015 survey.

Theft of physical assets or stock, long the most common type of fraud, was the second most frequently cited incident, suffered by 27% of respondents.

The greatest year-over-year increase in incidence was corruption and bribery, reported by 21% of surveyed executives, and up 6 percentage points from 15% in the last survey. With the incidence of bribery and corruption almost doubling over the last two years, the risk for organizations has heightened considerably.

In their article on page 23, Richard Dailly, Arturo del Castillo, and Paul Nash explore how governments around the world are stepping up to tackle bribery and corruption.

TYPES OF FRAUD SUFFERED IN THE PAST 12 MONTHS



TYPES OF CYBER INCIDENTS

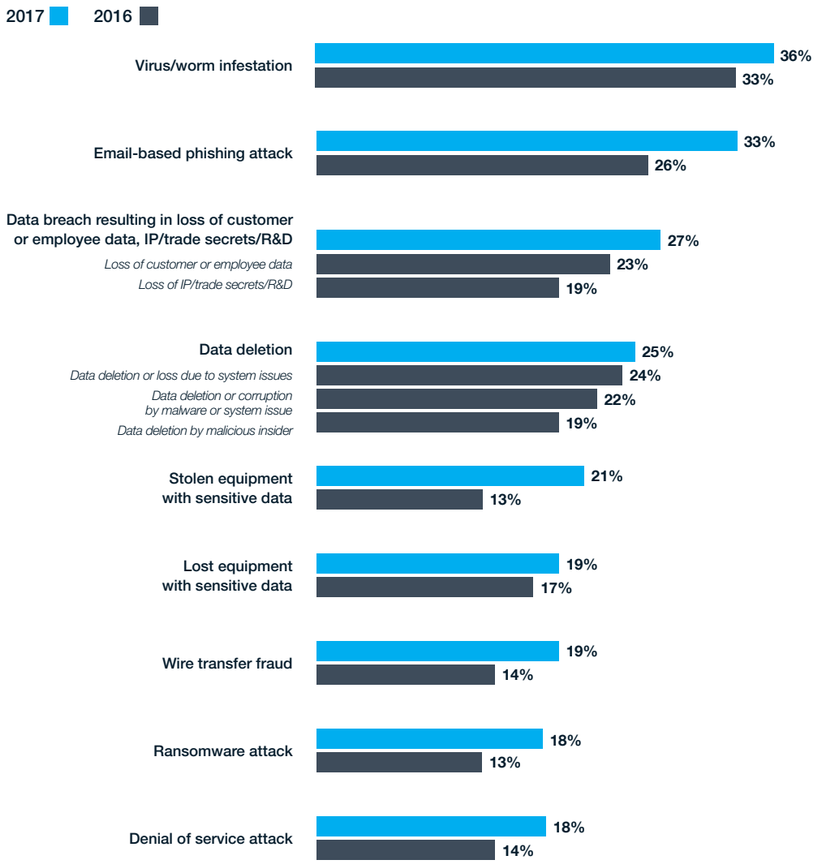
In the past year, respondents reported falling victim to more of every type of cyber incident than executives cited in the 2016 survey.

In the year when major viruses such as WannaCry and Petya spread around the world, nearly four in 10 (36%) surveyed executives said they had been hit by a virus or worm attack, an increase of 3 percentage points year on year, and the most frequent type of cyber incident named in this year's Report.

Whereas a quarter (26%) of respondents in last year's survey reported suffering from an email-based phishing attack, this year, fully a third (33%) experienced this type of cyber incident. Additionally, data breach and data deletion impacted 27% and 25% of this year's respondents, respectively.

Not all cyber threats were confined to the digital realm, however. Of the executives surveyed, 21% said equipment with sensitive data was stolen, while 19% said equipment was "lost", highlighting the convergence between physical and digital threats.

TYPES OF CYBER INCIDENTS SUFFERED IN THE PAST 12 MONTHS

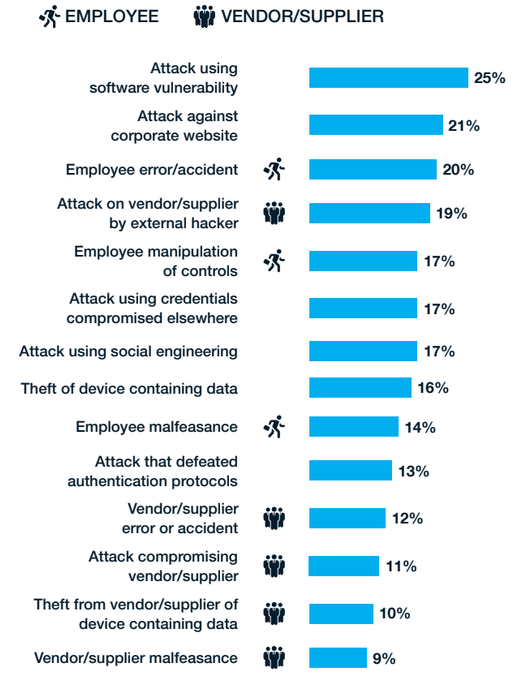


HOW CYBER INCIDENTS HAPPEN

When asked about a specific cyber incident their company had experienced, respondents often mentioned more than one attack vector, underscoring the complexity of the cyber-sphere. Furthermore, cyber incidents may result from malfeasance by bad actors – both outsiders and insiders – or error/accident caused by third parties and/or employees.

- Software vulnerability was the most common attack vector, named by a quarter (25%) of executives surveyed, followed by attack against corporate website, cited by 21% of respondents.
- Employee error or accident played a significant role, as indicated by one out of five respondents (20%), while employee manipulation of controls was cited by 17% and employee malfeasance by 14%.
  In their article on page 30, Alan Brill, Jonathan Fairtlough, Kenya Mann Faulkner, and John Friedlander show how organizations can make employees their greatest asset when it comes to information security by assessing how employees really work and then using that knowledge to put in place the right rules, tools, and compliance mechanisms.
- Third parties represent a vulnerability as well; notably 19% of those suffering a cyber incident were impacted via an attack on a vendor/supplier by an external hacker.

You stated your company has suffered from a cyber incident in the past 12 months. Which best describes how this took place? *(Select up to three)*



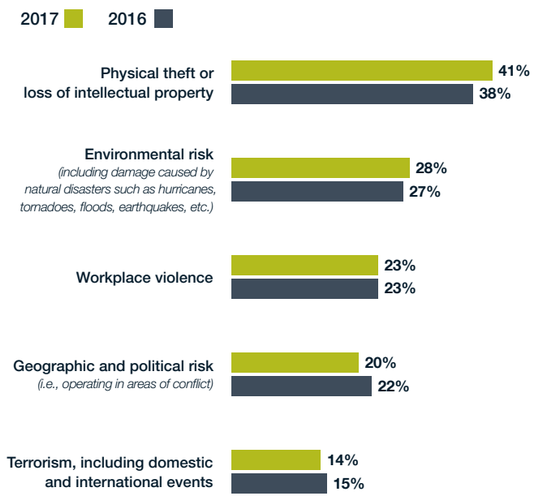
TYPES OF SECURITY INCIDENTS

The last year brought high-profile cases of intellectual property (IP) infringement, ranging from counterfeit goods to trademark violation and theft of proprietary information or artistic works. These incidents often result from coordinated cyber and physical intrusions. In this year's survey, physical theft or loss of IP remained by far the most prevalent type of security event; indeed, among those executives who stated they experienced a security event this year, a notably high 41% claimed their company fell victim to this type of incident. Respondents in the Manufacturing sector experienced the highest level of physical theft or loss of IP, at 45%.

Environmental risks also took their toll, reported by 28% of respondents this year. These risks were most prevalent within the Natural Resources sector (42%), followed by Healthcare, Pharmaceuticals, and Biotechnology (35%), and Construction, Engineering, and Infrastructure (30%).

Nearly a quarter (23%) of those experiencing a security incident cited workplace violence, the same level as last year.

TYPES OF SECURITY INCIDENTS SUFFERED IN THE PAST 12 MONTHS



Culprits Inside and Outside

Perpetrators

Insiders and ex-employees continue to pose the greatest threat to companies around the world, according to this year's survey. Whether it's a premeditated solo attack, a well-crafted collaboration with other internal and/or external parties, or simply an unfortunate accident with no malice intended, it's important to recognize the need for training, policies, and procedures to mitigate internal human risks.

Respondents revealed that fraud, cyber, and security incidents are often inside jobs, i.e., perpetrated by one or more of the following groups: senior or middle management, junior employees, ex-employees, freelance/temporary employees. Specifically:

- Of those respondents who reported a fraud incident, 81% cited one or more insider groups as perpetrators.
- Among those who experienced a security incident, 71% of respondents named one or more of these insider groups.
- And for those who suffered a cyber incident, fewer – but still a majority (58%) – identified one or more insider groups as perpetrators.

The insider risk notwithstanding, external parties also pose a significant threat. They were named in the top three responses across all three risk categories: fraud, cyber, and security.

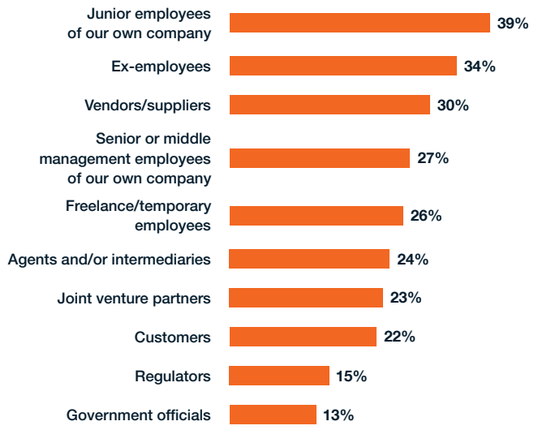
PERPETRATORS OF FRAUD INCIDENTS

Respondents reported that insiders continue to be the most common perpetrators of fraud, naming junior employees (39%), ex-employees (34%), senior/middle management (27%), and freelance/temporary employees (26%). Agents and/or intermediaries, arguably quasi-employees, were also cited by 24% of respondents.

While insiders were identified as the main perpetrators of fraud, respondents also stated that insiders were the most likely to discover it. Nearly half (47%) of respondents said that fraud was discovered by whistleblowers, 44% said it was detected through an internal audit, and 35% credited management with uncovering fraud.

Third parties are also frequently named as culprits of fraud; nearly a third (30%) of surveyed executives cited vendors/suppliers as key perpetrators and nearly a quarter (23%) named joint venture partners. **In their article on page 32,** Kevin Braine, Julian Grijns, Tad Kageyama, and Cem Ozturk discuss the multitude of insidious risks that can arise in supply chains and how organizations can better identify and mitigate these risks in a proactive way.

You stated your organization suffered at least one fraud incident in the past 12 months. Which of the following describes the key perpetrator(s) of these incidents? *(Select all that apply)*



PERPETRATORS OF CYBER INCIDENTS

Respondents who had experienced a cyber incident in the last 12 months said external parties were in many instances among the key perpetrators, citing random cyber criminals (34%), competitors (23%), and vendors/suppliers (18%). Indeed, random cyber criminal was the single most commonly named perpetrator of cyber incidents in this year's survey. Perhaps this is not surprising given that virus/worm attacks and email-based phishing attacks were the top two types of cyber incident suffered. Both are often opportunistic crimes where attackers play the odds and are abetted by the fact that raids can be easily deployed from any location and in high volume.

As noted previously, insiders are also key perpetrators, sometimes unwittingly through errors and sometimes through malfeasance. Ex-employees were named as key perpetrators by 28% of surveyed executives, whereas senior/middle management, freelance/temporary, and junior employees were cited by 19%, 18%, and 16%, respectively.

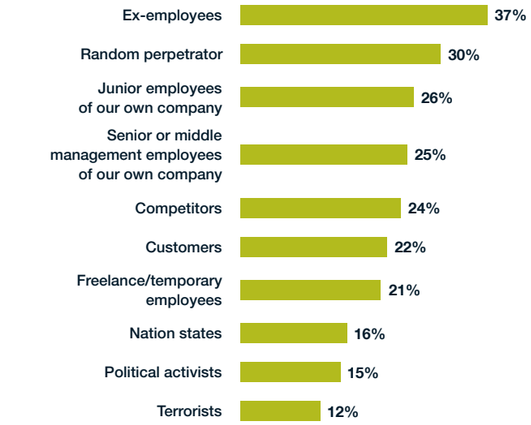
You stated your organization suffered at least one cyber incident in the past 12 months. Which of the following describes the key perpetrator(s) of these incidents? *(Select all that apply)*

PERPETRATORS OF SECURITY INCIDENTS

Ex-employees were the most commonly named perpetrators of security incidents, named by 37% of respondents. This was most evident in the Healthcare, Pharmaceuticals, and Biotechnology sector, at 54%. Among respondents from all sectors, roughly a quarter reported junior employees (26%) and senior/middle management (25%) as key perpetrators.

In looking at the role played by external perpetrators, nearly a third (30%) of respondents reported random perpetrators as the main culprits, with the Transportation, Leisure, and Tourism sector citing the highest proportion of all sectors surveyed (38%). The next most commonly identified perpetrator overall was a competitor (24%), although respondents in the Retail, Wholesale, and Distribution sector reported suffering the most from this threat (33%). Rounding out the overall top three of named perpetrators were customers (22%); given the nature of their business, it was perhaps not surprising to learn respondents from Consumer Goods and Transportation, Leisure, and Tourism each reported higher levels of customer-related incidents (31%). While nation states, political activists, and terrorists were only reported by 16%, 15%, and 12% of respondents, respectively, it's important to note these are all double-digit responses.

You stated your organization suffered at least one security incident in the past 12 months. Which of the following describes the key perpetrator(s) of these incidents? *(Select all that apply)*



Vulnerability and the Drive to Mitigate Risks

This survey shows mounting concerns about companies' vulnerability to fraud, cyber, and security risks. It is particularly striking that despite having taken some actions to mitigate risk, the share of respondents perceiving themselves as highly or somewhat vulnerable to threats has increased broadly. The emergence of the random perpetrator as a significant source of risk may be contributing to feelings of uncertainty, along with concerns over other "random" dangers such as environmental or geopolitical risk and, of course, worries about insiders and other typical sources of risk "learning new tricks". This suggests that as companies are becoming acutely aware that threats to their organization can arise at any time and from any place, they lack confidence in their current mitigation approaches; they must look to new methods and resources if they are to effectively anticipate, detect, and respond to risks.

Perceived Vulnerability on the Rise

With threats clearly increasing, it is not unexpected to see that the executives surveyed report a heightened sense of vulnerability across the board. It is notable, however, that information-related risks top the concerns in all sectors – fraud, cyber, and security.

FRAUD

Just as the most commonly reported type of fraud experienced in the last year was information theft, loss, or attack, it was also the most commonly named area of concern. A majority of respondents (57%) said they believe they are highly or somewhat vulnerable to information theft, and 56% identified the same level of concern around IP theft, piracy, or counterfeiting. Theft of physical assets, historically top of the list of concerns, was still high (cited by 55% of executives), but has now been overtaken by concerns about the vulnerability of information.

How vulnerable do you believe your company is to each of the following types of fraud today? *(Highly and somewhat vulnerable shown)*

	2017	2015*	Point (+/-)
Information theft, loss, or attack *(e.g., data theft)*	57%	51%	+6
IP theft (e.g., of trade secrets), piracy, or counterfeiting	56%	37%	+19
Theft of physical assets or stock	55%	62%	-7
Management conflict of interest	52%	36%	+16
Internal financial fraud	52%	43%	+9
Vendor, supplier, or procurement fraud	51%	49%	+2
Market collusion *(e.g., price fixing)*	50%	26%	+24
Corruption and bribery	50%	40%	+10
Regulatory or compliance breach	49%	40%	+9
Misappropriation of company funds	48%	40%	+8
Money laundering	43%	34%	+9
Modern slavery/human trafficking	40%	n/a	n/a

*This question was asked in 2015, but not in 2016.

CYBER

With cyber incidents at an all-time high and perpetrators seeming to develop new methods of attack virtually every day, we see a corresponding rise in perceived vulnerability among respondents. For each type of cyber incident, half or more of all executives surveyed admitted that they believe their company is highly or somewhat vulnerable.

How vulnerable do you believe your company is to each of the following types of cyber incidents today? *(Highly and somewhat vulnerable shown)*

	2017	2016	Point (+/-)
Virus/worm infestation	62%	54%	+8
Data deletion	58%	51%	+7
Email-based phishing attack	57%	52%	+5
Alteration or change of data	56%	47%	+9
Data breach	55%	53%	+2
Ransomware attack	55%	44%	+11
Stolen equipment with sensitive data	55%	52%	+3
Lost equipment with sensitive data	53%	49%	+4
Denial of service attack	52%	47%	+5
Wire transfer fraud *(email account takeover/impersonation)*	50%	43%	+7

The Healthcare, Pharmaceuticals, and Biotechnology industry is especially on edge, as survey respondents reported losses of personally identifiable information ("PII"), protected health information ("PHI"), employee records, and intellectual property at rates at least 15 percentage points higher than the market at large. **In their article on page 36,** Devon Ackerman and Brian Lapidus discuss how training, technology, and tone from the top can prove beneficial in helping healthcare organizations better protect the highly sensitive data they hold.

SECURITY

Similarly, the proportion of respondents who admitted to feeling vulnerable to physical security threats grew over the last year. Physical theft or loss of IP topped the list again this year, with 63% stating their company is highly/somewhat vulnerable to this information-related threat. Respondents in the Healthcare, Pharmaceuticals, and Biotechnology sector felt by far the most vulnerable to this threat, with 79% feeling highly/somewhat vulnerable, a clear 12 percentage points higher than the Professional Services sector, which was second on the list at 67%.

The data also show a significant increase in the proportion of respondents feeling vulnerable to environmental risk (up 7 percentage points), geographic and political risk (up 9 percentage points), and terrorism (up 8 percentage points).

How vulnerable do you believe your company is to each of the following types of security incidents today? *(Highly and somewhat vulnerable shown)*

	2017	2016	Point (+/-)
Physical theft or loss of intellectual property	63%	57%	+6
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	56%	49%	+7
Geographic and political risk *(i.e., operating in areas of conflict)*	53%	44%	+9
Workplace violence	50%	49%	+1
Terrorism, including domestic and international events	49%	41%	+8

The Imperative to Mitigate Risks

In a world growing ever more interconnected, companies must contend with both sides of the risk coin, i.e., not only can risk originate from any number of sources, the repercussions from incidents can make themselves felt in myriad ways. High-probability consequences such as operational disruption, financial losses, reputational damage, and regulatory investigations all make it imperative for companies to commit to establishing and supporting sustainable processes that will afford them effective protection now and into the future.

The value of proactive risk mitigation is evident for firms trying to manage today's shifting regulatory landscape. **In their article on page 38,** Violet Ho, Nicole Lamb-Hale, and Naoko Murasaki discuss four steps that investors can take to proactively navigate and manage U.S. regulatory and investment risk, particularly in the context of Asian investments that could potentially draw the attention of the U.S. Committee on Foreign Investment in the United States.

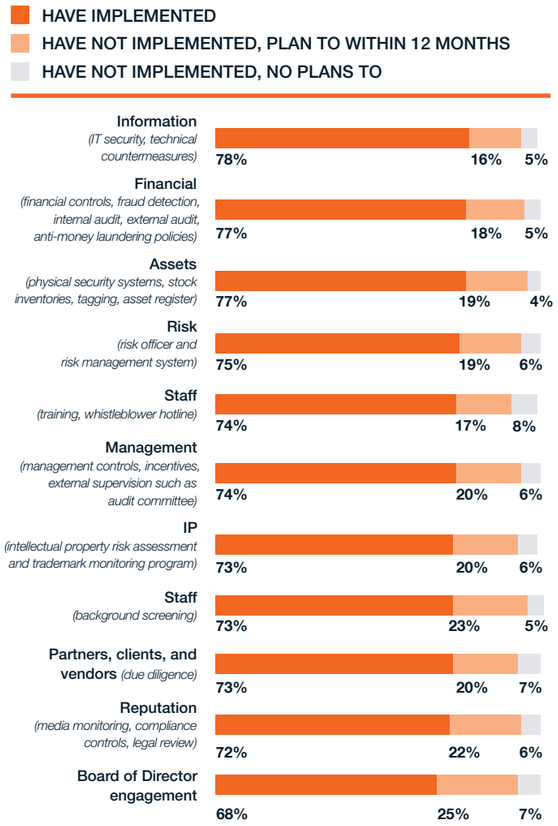
FRAUD

Nearly all anti-fraud measures mentioned in the survey were widely adopted by over 70% of respondents. Board engagement was the only measure which came in lower, at 68%, a surprisingly low percentage in the face of increasing regulations, regulatory enforcement, high incidence, and extremely wide and costly repercussions. However, 25% of respondents said they planned to implement board of director engagement in the next 12 months. The most widely adopted anti-fraud measure is information controls, e.g., IT security, at 78%. Financial controls and protection/inventory of physical assets were next on the list, both at 77%.

Given the preponderance of the insider threat, it is notable that less than three-quarters of respondents say their companies have implemented staff training/ whistleblower hotline (74%) and staff background screening (73%).

On the bright side, many respondents indicate their companies have plans to implement various measures in the coming year. If their companies do indeed act on their plans, then over 90% of executives surveyed will have all of these mitigating measures in place – at least to some degree.

Which of the following statements best reflects the current state of your company's adoption of anti-fraud measures?



CYBER

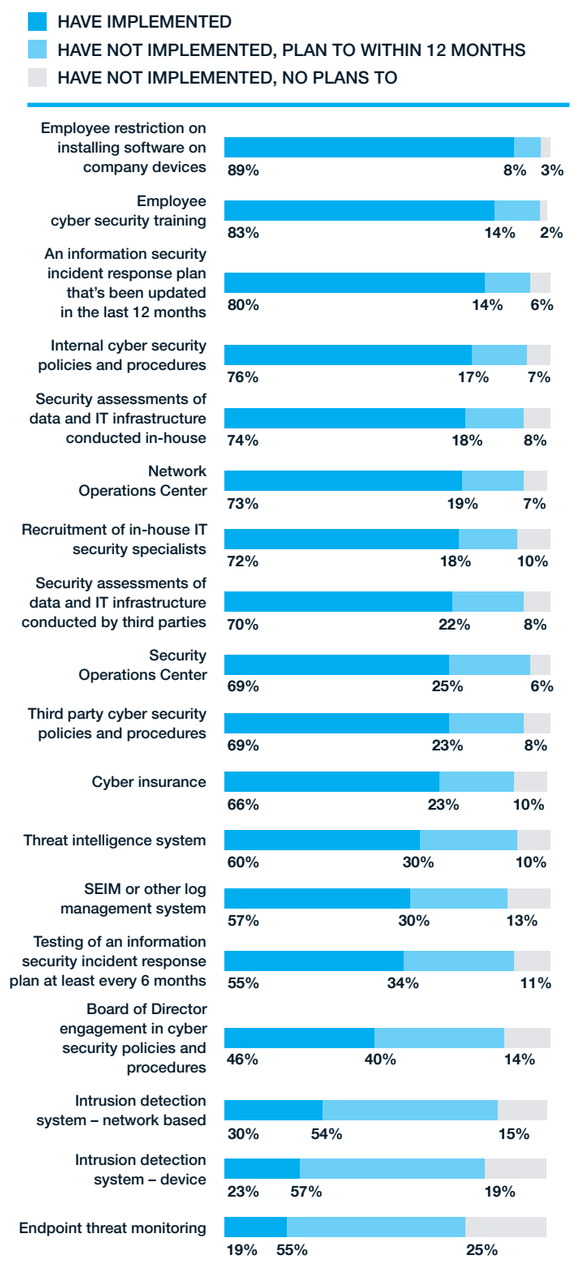
Given that insiders are key perpetrators of cyber incidents, it is encouraging to see that most respondents have already begun implementing employee-focused mitigation actions. The most implemented actions are employee restrictions on installing software (89%) and employee cyber security training (83%). Incident response plans (IRPs) also lead the list, with 80% of respondents indicating their company already has an IRP in place.

As noted previously, surveyed executives perceive themselves to be highly vulnerable to cyber intrusions, and accordingly, the top three actions they expect their company to implement in the next 12 months are intrusion detection systems that are device-based (57%), endpoint threat monitoring (55%), and intrusion detection systems that are networked based (54%).

Cyber security is rapidly becoming a board governance mandate as the likelihood of an incident grows along with increasing regulatory pressures and costly reputational risks associated with data privacy. While only 46% of respondents currently involve the board of directors in cyber security policies and procedures, another 40% plan to do so in the next 12 months.

In their article on page 40, Andrew Beckett, Paul Jackson, and Jason Smolanoff offer seven discussion points than can form an effective starting point for boards to establish an active role in cyber security risk mitigation efforts.

Which of the following statements best reflects the current state of your company's adoption of cyber risk-mitigation measures?

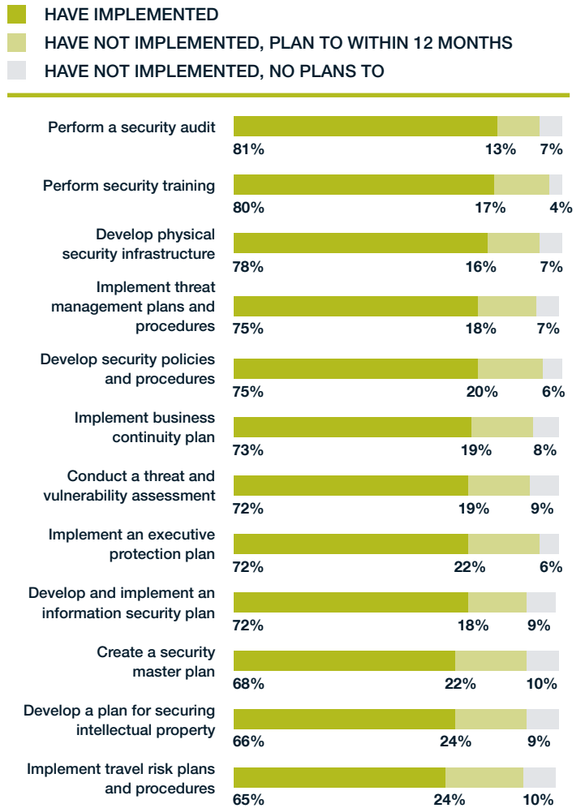


SECURITY

A large proportion of respondents have adopted security risk mitigation measures, with security audits at the top of the table (81%), followed by security training (80%), and development of a physical security infrastructure (78%).

Given the high incidence and feelings of vulnerability around theft/loss of IP, it's surprising to see that developing a plan for securing intellectual property is at the bottom of the list at 66%, almost in line with implementing travel risk plans and procedures (65%). However, reassuringly, almost a quarter (24%) of respondents plan to implement these measures in the next 12 months.

Which of the following statements best reflects the current state of your company's adoption of security risk-mitigation measures?



Conclusion

The 10th Kroll Global Fraud & Risk Report highlights yet another increase in fraud, cyber, and security incidents experienced by companies around the world. As executives strive to cope with new challenges, stay ahead of ever-evolving threats, and adapt appropriately, it has become a constant battle that requires rigorous planning and implementation, as well as adequate resources.

In today's digitized and globalized markets, the value and vulnerability of information has made it among the most difficult of assets to protect. It is not surprising that respondents report a heightened sense of vulnerability across the board, and that information-related threats top the list of concerns in all risk areas – fraud, cyber, and security.

Given the costly and wide-ranging repercussions that companies suffer from incidents, the imperative has never been greater to focus efforts on effective preparedness, response, and remediation measures. However, the convergence of a global economy, complex digital connections, and perennial human factors means that many risks are no longer solely a fraud, cyber, or security problem. Rather, the findings crystallize the need for multidisciplinary approaches if organizations are to better manage their risks going forward.

Commentary

Anticipate, detect, mitigate, and respond

Are We Winning the Battle Against Bribery and Corruption?

Written by Richard Dailly, Arturo del Castillo, and Paul Nash

This year's Global Fraud & Risk Report survey found that the incidence of bribery and corruption had increased from 15% in 2016 to 21% this year, moving from 10th place to 5th place on the list of types of fraud experienced. Looking back further to the 2015 survey results, we can see that reports of bribery and corruption have almost doubled over the last two years, increasing from 11%.

Bribery and corruption seems to be on the rise, but companies are also getting better at detecting it. And, from a regulatory perspective, governments around the world are stepping up to tackle the issue.

EUROPE, THE MIDDLE EAST, AND AFRICA

Several European countries, including France, Germany, Ireland, and Slovakia, have recently introduced, or proposed to establish, new anti-bribery and corruption laws.

In the UK, the past year has seen significant progress by the Serious Fraud Office ("SFO") in successfully using the Bribery Act to investigate and prosecute multiple cases. Of particular note is the use of U.S.-styled deferred prosecution agreements ("DPAs") in several high-profile cases. One in particular that involved a major engineering firm, which had to be approved under the supervision of a judge, marked the culmination of a four-year investigation into bribery and corruption across seven jurisdictions including Indonesia, Thailand, India, Russia, and Nigeria. The corporation's UK settlement amounted to GBP 497 million, with separate agreements with the United States totaling USD 170 million and Brazil for USD 25 million.

The focus on anti-bribery and corruption prosecutions by the SFO demonstrates that both small/medium size enterprises and large corporates are under the spotlight and, in many situations, bribery by UK corporates is taking place overseas. As a result, corporates are placing renewed focus on developing robust compliance systems to assess bribery risks across their global operations, which is directly affecting investment decisions in developing markets.

Furthermore, the UK Criminal Finances Act promises to be a powerful tool in the fight against corruption. The Act, which came into effect on September 30th, 2017, establishes a new corporate offense of failure to prevent the facilitation of tax evasion, and introduces Unexplained Wealth Orders.

CASE STUDY

Kroll recently conducted a bribery and corruption investigation in Africa to support proceedings being undertaken by a country's prosecutor to assess the existence of any criminal offenses or other irregularities related to a billion-dollar procurement contract. The investigation involved reviewing thousands of documents obtained from Africa, the Middle East, and the UK. Data analytics techniques were also used to detect suspicious payments spanning several years. All of this was supplemented by on-the-ground interviews with relevant parties.

ASIA PACIFIC

In China, the sweeping anti-corruption campaign over the past five years has been the centerpiece of the Chinese government's domestic policies. The successful prosecution of more than 200,000 government officials for corruption has helped solidify the popular support of the current leadership.

Historically, there have been very few successful Foreign Corrupt Practices Act ("FCPA") enforcement actions for violations of anti-corruption provisions relating to China. Proving the act of corruption can be challenging, jurisdiction barriers often cause issues, and obtaining evidence of government officials receiving bribes is notoriously difficult. However, now that China has stepped up its own efforts to investigate corruption in both public and private sectors, some of the schemes that have been well hidden for years may be exposed.

Elsewhere in the APAC region, bribery and corruption are constantly named as two of the largest risks facing companies. On the positive side, Indonesia's Corruption Eradication Commission ("KPK") is becoming increasingly effective, recently making arrests in the well-publicized E-KTP corruption case, which had resulted in a loss to the state of over USD 140 million; Philippines' president Duterte was elected on a mandate of tackling endemic corruption; Malaysia's Anti-Corruption Academy wants to establish itself as a regional center of excellence on anti-corruption issues; the Thai military government has promised to "eradicate" corruption; and the new Vietnamese leadership has lately made a number of high-profile arrests on corruption charges.

In practice, however, some might question whether governments in the region act in a politically neutral manner. Although independent, the KPK is still seen by many as politically biased. Duterte's anti-corruption stance has morphed into something more nationalist and populist, and the systematic dismantling of government institutions is likely to fuel corruption in the longer term. The recent arrest of Vietnamese officials on corruption charges was felt by some observers to have been driven by political rivalry at the highest levels. The Malaysian agencies have been criticized in their tackling of the 1MDB scandal: Despite international pressure, Malaysia's attorney general declared in mid-2016 that there was no evidence of fraud. Thailand, despite its introduction of new anti-corruption laws in 2016, dropped from 78 to 101 in Transparency International's 2016 Corruption Perception Index, placing it equal with the Philippines and 11 places below Indonesia.

NORTH AMERICA AND LATIN AMERICA

Despite the controversies at the beginning of 2017 about the future of FCPA enforcement, it was a busy year for FCPA investigations. Since the beginning of 2017, there have been disclosures of 38 new FCPA-related investigations being conducted by the U.S. government.

One of the largest bribery investigations in recent years has been "Operation Car Wash," carried out by the Brazilian authorities in coordination with several foreign regulators. The investigation against Brazilian contractor Odebrecht and its petrochemicals subsidiary, Braskem, spotlighted a complex and sophisticated scheme of corruption, resulting in fines of USD 2.6 billion payable to authorities in Brazil, the United States, and Switzerland, and heralding a genuine change in the prosecution of bribery in Latin America.

The revelation that Odebrecht paid bribes in 11 other countries – nine in Latin America and two in Africa – has turned the case into an international story. The Odebrecht case shows that corruption is often not just a simple transaction of illegal payments. In the global economy, corruption happens through complex financial mechanisms. Odebrecht officials shipped cash across the globe – from one shell bank account to the next – en route to politicians' pockets in more than a dozen countries.

Bribery, like other crimes, occurs when an individual has (a) motivation to do it; (b) opportunity to do it; and (c) the ability to rationalize one's actions from a moral perspective. Removing any of these elements can stop the crime from taking place. In the case of bribery, the removal of one's opportunity to commit such crime is generally the easiest element to eliminate.[1] Companies should be prepared by optimizing their anti-bribery and corruption programs, putting strong defenses in place, and being ready to detect and respond to situations before they have a serious detrimental impact on their business.

[1] Lawler, D. (2012). Frequently Asked Questions in Anti-Bribery and Corruption. Wiley, 326.

RICHARD DAILLY
Managing Director,
Head of Southeast Asia
Investigations and Disputes,
Asia Pacific
rdailly@kroll.com

ARTURO DEL CASTILLO
Associate Managing Director
Investigations and Disputes,
Latin America
arturo.delcastillo@kroll.com

PAUL NASH
Associate Managing Director
Investigations and Disputes, EMEA
paul.nash@kroll.com

Tracing Concealed Assets in Fraud Investigations, Arbitration Awards, and Judgments

Written by Glen Harloff, Dan Karson, and Alex Volcic

Respondents to this year's Global Fraud & Risk Report survey cited a significant increase in fraud-related losses.

In the case of an internal fraud, once a fraud allegation has been made and investigated, the imperative usually shifts to loss recovery. Similarly, arbitration awardees, judgment creditors, and financial institutions that are chasing debtors with non-performing loans often need expert assistance to identify assets that can be frozen and recovered.

Few debtors start out intending to default on a loan. Nor do they (or can they) erase the early asset footprints they leave behind. The same can be said even for perpetrators of fraud. How then do you find the money?

UNCOVERING ASSET FOOTPRINTS

A company's game plan should start with a well-researched history of the target debtor, going back long before the date of the loan or transaction. The asset search should also include a comprehensive search of public records and information databases. Depending on the jurisdiction, these may contain evidence and important leads to assets such as real estate, business holdings, bank accounts, cars, boats and planes, and receivables, among other items.

Social media also has become a rich source of asset-related information. For example, Kroll has often found assets and evidence disclosed by debtors and their families on social media pages that were not password protected. This is not a rare occurrence. In our 24/7, need-to-communicate, tell-all world, the subjects of investigations and their families can be indiscreet and indiscriminate, broadcasting, for example, pictures of their weekend homes and luxury possessions.

Once these tracks have been laid and analyzed, the strategy may shift to external inquiries or human intelligence.

If the debtor/fraudster is still involved in an active business, that's good news. It means there should be receivables, cash flow, banking relationships, credit cards, customers, and suppliers. (When applying for a loan or line of credit, fraudsters often provide detailed net worth statements listing assets and liabilities.) Other live sources of information can be former employees, vendors ("Who was the payee bank?"), customers ("What bank negotiated your payment?"), former business counterparties, and litigation adversaries.

GLEN HARLOFF
Senior Managing Director
Investigations and Disputes, LATAM
gharloff@kroll.com

DAN KARSON
Chairman, Americas
Investigations and Disputes, North America
dkarson@kroll.com

ALEX VOLCIC
Managing Director,
Head, Russia & CIS
Investigations and Disputes, EMEA
avolcic@kroll.com

JURISDICTION MATTERS

Money and assets may be scattered across multiple, complex jurisdictions and in some where it is traditionally hard to make recoveries. Throughout all these stages it is important to focus on the path of least resistance – investigating first in jurisdictions most amenable to enforcement.

The number of countries where assets can be safely hidden is actually shrinking, but the ways in which assets can be concealed has grown. These are abetted by the proliferation of private investment vehicles and the speed of electronic transfers; the complicity of bank managers in some jurisdictions, despite anti-money laundering laws and the banks' own internal rules; the remaining countries which still profit from being asset flight havens; and for some of the highest net worth dodgers, there still are governments and heads of state who provide shelter, undoubtedly for a price.

However, creditors seeking expert help can have realistic hopes of making potentially significant loss recoveries, even in challenging jurisdictions. If the facts merit an official criminal investigation, creditors should also consider government assistance under a Mutual Legal Assistance Treaty ("MLAT"). MLATs are multinational treaties that facilitate, among other things, obtaining in one signatory country evidence of certain designated crimes committed by an individual(s) or business entity(ies) in another signatory country. The remedy is available only to governments. However, many asset search investigations are conducted in parallel with government investigations where the government has the discretion to assist a victim creditor.

The interplay between an internal review of books and records and external inquiries was very important in a recent Kroll case:

A Russian bank had experienced a fraud on its trading floor which led to losses of over USD 300 million. Kroll conducted an onsite investigation comprising a financial review of the Bloomberg trading system and forensic interviews, supported by computer forensics and public record research. This phase of work confirmed that the bank had suffered a fraud and supported legal proceedings in London to freeze assets and obtain disclosure. In the second phase of work, Kroll collaborated with the client and its legal advisors to implement a civil and criminal investigation strategy to obtain further disclosure and to trace the proceeds of the fraud.

Using MLAT proceedings, Kroll supported the bank in obtaining information regarding the flow of funds through the international banking system and was able to successfully pierce the corporate veil. Kroll conducted public record research and local human source inquiries to identify assets in countries across Europe and Asia, including Bulgaria, Ukraine, Georgia, Azerbaijan, and Tajikistan, as well as the Middle East, and North and South America.

Kroll provided expert witness reports in support of a civil fraud claim in the UK and to recover assets in several jurisdictions. Our cyber team secured, processed, and reviewed more than 100 terabytes of electronic documentation and produced trial bundles for court proceedings. We worked with the client to report to the financial regulator and to assist the regulator's investigation. The civil judgment, issued in the UK and in favor of the bank, has resulted in the recovery of a significant proportion of the fraud proceeds. In criminal proceedings, two of the key defendants have been found guilty and are facing substantial custodial sentences.

Norwich Pharmacal Orders available in the UK and former UK jurisdictions and/or Discovery Orders, as often referred to elsewhere, are civil tools similar to MLAT, which may provide investigators with information such as banking records or the identity of directors, officers, and shareholders of offshore companies. A Norwich Pharmacal Order was instrumental in assisting Kroll in a multijurisdictional case:

Working for a Middle East client, Kroll identified the diversion of USD 5 million from the company's bank account. Although no suspects were identified, investigators were able to trace the funds to a financial institution in the Caribbean region. Kroll prepared an affidavit describing the circumstances of the investigation, and with the assistance of local Caribbean counsel, Kroll obtained a Norwich Pharmacal Order against the bank to disclose details of the bank account, including Know Your Client ("KYC") information. The order identified the beneficial owners of the bank account and also over USD 4 million of the funds still sitting in the account. With further assistance from counsel, the funds were immediately frozen and eventually returned to the client.

Few situations are more frustrating than winning a money judgment or award and chasing a debtor or crook who conceals assets and lives large. But an organized investigative strategy and the use of available tools can break down walls. The target may run, but increasingly, it is far more difficult to hide.

Infrastructure Investment in Emerging Markets – Mitigating the Risks

Written by Tarun Bhatia, Reshmi Khurana, Oliver Stern, and Brian Weihs

To meet growing regional demand for energy, transport, and communication networks, investors are financing capital-intensive infrastructure projects in Sub-Saharan Africa, South Asia, and Latin America. Infrastructure projects attract investors on the back of potential returns that can outstrip yields in mature markets. But with opportunity comes risk, particularly in the construction, engineering, and infrastructure sector, which in our survey saw the largest year-over-year increases in fraud incidents (up 13 percentage points to 83%) and cyber incidents (up 16 percentage points to 93%). Security incidents in this sector also increased to 67% (up 4 percentage points).

In this article, we draw on the expertise and experience of our teams across a range of emerging markets and explore the steps that investors can take to identify and mitigate risks.

DELIVERING INFRASTRUCTURE PROJECTS IN SUB-SAHARAN AFRICA

Successful infrastructure investment requires the integration of projects into the host jurisdiction's existing network of transport, power generation, and distribution grids. This is not just an engineering challenge. It requires institutional capacity and a functioning legal and regulatory framework to accommodate large-scale, long-term investments.

Many Sub-Saharan Africa jurisdictions lack the planning capacity and resources to link existing infrastructure to new projects. For example, power generation projects fail unless the producer can access a grid to sell energy through a commercially viable feed-in tariff. Pre-investment intelligence-gathering can help clients understand the regulatory environment and the implementation capacity of key government agencies in order to better assess the feasibility of a project.

Many new projects in this region tend to be politically significant and thus potentially vulnerable to non-transparent interference or influence. Politicians promote infrastructure projects to increase their profile and gain popularity within their constituency. Unrealistic expectations about what the project can deliver can also undermine the investment's commercial viability. For example, if investors in rail freight projects are expected to provide passenger transport to meet political and socio-economic priorities, the economics of an investment can be distorted.

While investors should be aware of such red flags, they cannot often directly influence them. As a starting point, investors need to understand the motivation and incentives of the project within the context of the country's political economy.

INFRASTRUCTURE INVESTMENT REMAINS A CHALLENGE IN SOUTH ASIA

Investors in infrastructure projects in South Asia face a similar set of challenges. For example, over the last three years, private sector infrastructure investment in India has slowed down due to a combination of stretched corporate balance sheets and rising non-performing assets for banks. The pace at which project-related decisions are being approved by various government departments (for example, approvals related to availability of land or environmental clearances) also remains slow.

Investment activity still remains high in certain pockets in South Asia, especially infrastructure. One such example is the renewable energy sector in India, which has seen significant interest from both domestic and international investors. While growth in renewable energy remains a key goal for the government of India, the aggressive push on the agenda (175 GW by 2022) has also resulted in a sharp decline in uptake prices, mainly for solar energy, due to the entry of many players, most of whom have limited or no experience in the sector. This puts immense pressure on local developers to deliver projects at low cost, which in turn affects the quality of material used and the sustainability of such projects. At the same time, companies still need to work with local governments and other stakeholders to ensure they obtain necessary approvals in a timely fashion, which means that the risk of corruption remains. With a sharp decline in tariffs for new projects, the power purchase agreements of existing projects – which have significantly higher costs per megawatts compared to prices being proposed for new projects – also become susceptible to public backlash and administrative scrutiny.

Investors often struggle to understand whether the costs and performance of a project reflect its true health. Given the relatively close nexus between companies, politicians, and bureaucracy in India, businesses often get pushed into practices which are potentially inappropriate and that can directly impact financial reporting. The wide gap between what is reported in the books versus the actual performance of the project casts doubt on the overall integrity of the quality and financials of a project. Other South Asian markets like Bangladesh and Sri Lanka are also exposed to similar issues.

While these challenges pose a risk, the significance of the opportunity often outweighs the cost of the risk. By developing a deep understanding of all the dynamics in the local market, investors can advance with greater confidence and make investments in line with their expectations regarding returns with fewer surprises.

ISSUES IN INFRASTRUCTURE INVESTMENT IN LATIN AMERICA

In Latin America, recent revelations of large-scale corruption have had a significant impact on infrastructure projects, debilitating sponsor governments and freezing projects mid-construction. The issue was recently highlighted with the investigation and prosecution in Brazil of the region's largest builder, which has admitted to having paid over $3 billion in bribes in 28 countries – including in particular Peru, Colombia, Venezuela, and Mexico – at the highest levels of government.

Energy, transportation, and communications projects in several of the region's largest countries, including Brazil, Mexico, and Argentina, also suffer from challenges with the acquisition of land rights. Land reforms in several Latin American countries in the last century have resulted in a legacy of communal land rights and long-standing conflicts over land possession. This creates difficulty and uncertainty in the negotiation of access or possession, and incentivizes shortcuts by pressured developers. For example, efforts to develop a new airport for Mexico City were stymied for decades by conflicts over land rights acquisition. Arm´s-length investors need to understand the risks and how land access or possession rights are acquired. Pre-investment investigation of relationships with land owners and communities, including forensic investigation, can help investors understand and quantify risks associated with the land rights acquisition processes.

As voters in the largest Latin American countries have started to move away from left-leaning and populist governments, new interest has been growing in private-public partnership ("PPP") investments in the transport and public services sectors. However, larger PPP investments still face scrutiny by incoming administrations, often resulting in reassessment and even cancellation of significant projects whose economic benefits are not overwhelmingly clear. Recently, the development of a combined-cycle electrical plant involved private sector builders and public sector sponsors. After a careful investigation, Kroll's research and analysis provided one of the private investors reassurance as to the integrity of the plant development's negotiation process, enabling the investor to proceed with the investment.

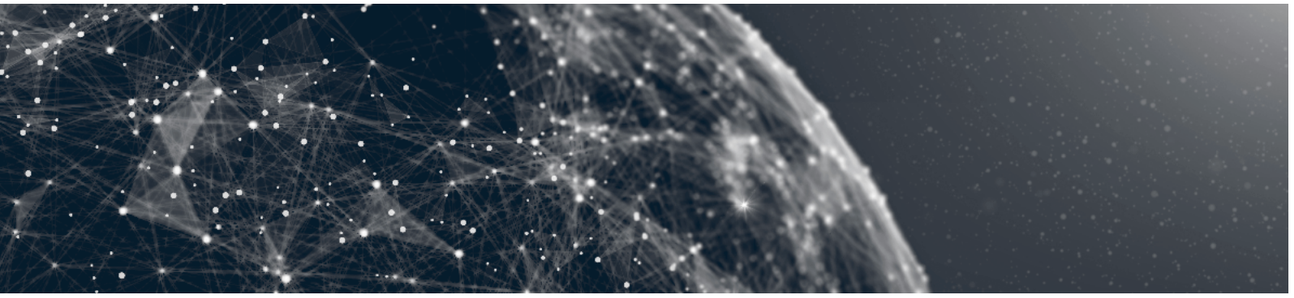
Infrastructure investors in emerging markets need to deal with a complex set of challenges to successfully finance, develop, and operate projects. With sufficient pre-transactional preparation and with access to intelligence throughout the project cycle, investors can make confident decisions on their investment strategies.

TARUN BHATIA
Managing Director,
Investigations and Disputes,
APAC
tarun.bhatia@kroll.com

RESHMI KHURANA
Managing Director,
Head of South Asia,
Investigations and Disputes
rkhurana@kroll.com

OLIVER STERN
Associate Managing Director,
Investigations and Disputes,
EMEA
oliver.stern@kroll.com

BRIAN WEIHS
Managing Director,
Mexico Office Head,
Investigations and Disputes,
bweihs@kroll.com



When It Comes to Information Security, Employees Can Be Your Most Important Asset and Your Greatest Threat

Written by Alan Brill, Jonathan Fairtlough, Kenya Mann Faulkner, and John Friedlander

The script for a large-scale information security failure has become predictable. Employee/trusted vendor makes an error in configuration or design, or fails to follow good security practices. Hacker/thief takes advantage of error. Media/regulator/litigant causes company and CEO to publicly pay for the failure.

In response to this repeating corporate nightmare, companies have stepped up their ability to try and police preventable errors. 76% of companies surveyed by Kroll have cyber security policies and procedures, and 74% (76% last year) have already implemented employee training and whistleblower programs. A mentality of user distrust is becoming the norm in IT Security departments. We've heard more than one IT manager refer to employees as "the enemy," noting that "computers don't commit crimes, people do!"

Yet, the number of data breaches has not slowed down.

MAKE SECURITY PART OF THE WORK PROCESS TO PROMOTE SUSTAINABILITY.

Does the continued occurrence of data breaches mean that security-related training, policies, and protocols do not work? No – it means that these elements are not enough when implemented in a standalone way. The key to leveraging their benefits more fully is to make information security part of employee workflows.

An approach that Kroll has found to be effective is to determine an overall risk rating (ORR) for processes that touch key data. Start with a security review that focuses on how employees work and think. This is not an audit. Indeed, 80% of all respondents to Kroll's survey are already engaging in security audits. An audit reviews existing controls at one point in time.

This approach begins by understanding what must be secured: What do you have worth protecting? Who needs to access it and from where? Why does the current process pose a risk? What is the probability of the risk, and what is the impact to the business if the risk is realized? What is the cost of mitigating the risk?

Consider this scenario. ABC Company relies on an outside sales team for revenue. Salespeople need access to customer data. Each salesperson uses a company-provided laptop daily for email, calendar, document drafting, and social media. Over time, that laptop is full of old data, poorly updated, rarely backed up, and often used for personal as well as work activity. When it gets lost, stolen, or hacked, a breach occurs.

New scenario: Each salesperson has a tablet with paid cellular access. The customer data and forms are stored in a document management system in the cloud, and never on the tablet. The tablet has mobile device management software that blocks all browsing. If lost, the device is encrypted and can be remotely wiped. No local storage, no vampire data or data hoarding. No "drive-by" infection. Security improves because it is now part of the workflow.

MAKE CLEAR SECURITY RULES, TRAIN ON THEM, AND ENFORCE THE RULES CONSISTENTLY, WITH REAL CONSEQUENCES FOR NONCOMPLIANCE.

Workflow-integrated security risk management is a great start. The security rules must be clear. They must be followed by all staff. Everyone is trained and tested on these rules. There must be consequences for noncompliance.

Organizations must also look at information risks within the context of a total security posture. Having a physical control policy is critical. After all, data can be just as easily stolen from a desktop as from a cloud storage device.

Criminals know it's far easier to trick an employee into making a mistake by using social engineering. Criminals take advantage of goodwill in human nature. Consider the lost key drop. An employee finds a ring of keys on company property with no nametag, but it does have a USB memory device. The employee plugs the USB flash drive into his or her computer, hoping to find information that will help reunite the keys with their owner. The employee unwittingly has installed malware that could devastate the company.

The protection against this is simple – train people, then test their training. A good security training plan is more than just a lecture – it is a running test. Spoof emails and see who responds. Have an outsider try to walk in carrying a pizza.

Management must follow the same rules. Nothing undermines a security protocol more than senior managers who fail to wear a badge, or who use their own equipment and/or have special access rights.

Management also needs to support people when they follow the protocols. Let's say a CFO really does call an accountant and order an immediate funds transfer, but the accountant refuses to violate the protocol. If the employee is punished, people will be afraid to follow the rules in the future.

GIVE PEOPLE THE TOOLS TO FOLLOW THE RULES.

Some simple tools can have a big impact. A locked drawer in which to place sensitive information at lunchtime or at the end of the day. A privacy shield to prevent unauthorized viewing of a laptop screen used on an airplane. A dedicated number to call when a question arises. Support security!

By assessing how your employees really work and then using that knowledge to put in place the right rules, tools, and compliance mechanisms, you can make your people a part of your security solutions – both cyber and physical – and by doing so, they can become your greatest security asset.

ALAN BRILL
Senior Managing Director,
Cyber Security and Investigations
abrill@kroll.com

JONATHAN FAIRTLOUGH
Managing Director
Cyber Security and Investigations
jfairtlough@kroll.com

KENYA MANN FAULKNER
Managing Director
Investigations and Disputes
kenya.faulkner@kroll.com

JOHN FRIEDLANDER
Senior Director
Security Risk Management
jfriedlander@kroll.com

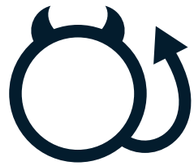
The Hidden Threats in Your Supply Chain

Written by Kevin Braine, Julian Grijns, Tad Kageyama, and Cem Ozturk

While natural disasters or civil disorder are viewed as the most disruptive and costly supply chain risks, fraud or breaches of environmental or human rights laws are far more common – and often more damaging – than geopolitical black swan events. In fact, they are becoming a much greater concern for international corporations, as evidenced in Kroll's 2017/18 Global Fraud & Risk Report, which shows these insidious supply chain risks are on the rise.

Because supply chain and procurement functions are typically quietly embedded in any given international corporation's key processes, they are a potential source of fraud and reputation risk. This is reflected in responses from the companies queried in our survey, where more than 30% indicated that vendors and suppliers were the key perpetrators of fraud incidents. This is up four percentage points from last year's survey.

This article briefly outlines some of the most common supply chain risks that Kroll has seen in our engagements and offers strategies that organizations can use to identify and mitigate risks in a proactive way.



UNETHICAL BUSINESS PRACTICES

In the last year, investigative media exposed numerous instances of forced and child labor, land-rights issues, and poor working conditions in the supply chains of prominent international brands. This often resulted in protracted internal investigations and fundamental damage to brands. For example, a chemicals company supplying the cosmetics and car manufacturing industries was named in the media as using suppliers of mica who source this mineral from illegal mines in India using child labor. Half a dozen of the world's leading car manufacturers were then attacked by pressure groups for not doing enough to prevent this. In another case, a leading Australian newspaper group was the target of a number of NGOs over their Korean supplier's history of gross environmental destruction in remote West Papua, Indonesia.

DEALINGS WITH SANCTIONED ENTITIES AND ORGANIZED CRIME

Relationships and business activities deep in the supply chain can expose organizations to a host of risks, including links with organized crime and dealings with sanctioned individuals or entities. For example, recent in-house Kroll analysis found significant numbers of vessels used in worldwide commerce are beneficially owned or controlled by politically exposed persons, with others controlled by state-owned enterprises, potentially putting organizations at risk for dealing with sanctioned entities.

One recent case is also instructive: A whistleblower from the Singapore regional headquarters of a Japanese conglomerate informed management that an Indian vendor and one of its employees were colluding to fabricate work orders for non-existent repairs. The fraud represented significant annual losses, and subsequently led to the discovery of further vendor issues in Southeast Asia and beyond, including possible links to organized crime.

CORRUPTION AND BRIBERY

Corruption and bribery are pervasive not only in emerging economies or third world countries, but also in more developed jurisdictions as well. Kroll recently assisted a client, the subject of an FCPA investigation, with a detailed forensic audit of the company's books and records to examine payments to commercial agents and government representatives in 33 countries, while also carrying out extensive on-site document and accounting analysis in Libya, Angola, Brazil, and Russia.

PRODUCT CONTAMINATION

Small contract violations can turn into big problems that can damage a company's bottom line and brand. Take, for example, the case where an apparel company's factory in Asia stops destroying blemished product and/or overruns. Instead, a factory owner, manager, or employee allows this product to enter unlicensed markets and sales channels around the world, damaging the brand owner's margins and reputation. In another case, UK and European retailers discovered that some of their suppliers fraudulently allowed horse meat to enter their supply chain and to contaminate various beef products; they were forced into large product recalls and urgent and costly reviews.

TRADE SECRET AND INTELLECTUAL PROPERTY LEAKS

Brand owners that fail to properly evaluate the physical, IT systems, applications, and overall information security in use by their vendors face the risk of losing product and process technologies, as well as other trade secrets. In fact, contracted manufacturers themselves can become competitors. This was the case when a manufacturer of highly engineered and patented rubber bushings established a second business by producing an unlabeled version of the same product.

SUPPLY CHAIN RISKS ARE AMPLIFIED WHEN COMPLEXITY AND COMPLACENCY CONVERGE

While these incidents may seem unusually complex, and therefore difficult for the respective companies to have detected, they are anything but unusual in today's global risk environment. This in fact is the new norm in supply chain risk, and it demonstrates the increasing demands placed on global businesses to understand precisely who they are working with and what their activities are, no matter how distant a supplier may seem from day-to-day operations. Yet despite these risks and challenges, more than a quarter of global respondents said they have not adopted anti-fraud measures such as due diligence on partners, clients, and vendors.

Many cases involve third-party suppliers based in emerging markets, particularly South and Southeast Asia – and for good reason. Supply chain visibility in these regions is extremely challenging. Weak rule of law, unreliable corporate information, regular use of insulating proxy companies between controversial entities and global suppliers, and the profusion of third-country subcontractors ostensibly domiciled in relatively lower-risk countries such as Hong Kong, the UAE, and Singapore all contribute to this opacity.

Even long-term vendors or contract manufacturers present their own sets of risks. Management may often become too trusting or in some cases complacent about closely monitoring such relationships. At the other end of the spectrum, supply chain onboarding processes and audits at most corporations are typically insufficient to detect such issues, especially in multi-regional supply chains and for those operating in multiple emerging market environments.

LESSONS LEARNED TRANSLATE INTO PROACTIVE RISK MITIGATION STRATEGIES

Lessons learned from recent incidents highlight the fact that many corporations share the same vulnerabilities when it comes to identifying unethical or fraudulent third parties. They also provide a road map for building more effective compliance programs.

- Establish risk-based compliance programs. One-size-fits-all compliance can waste resources and often miss critical red flags of problematic behavior.
- Seek independent verification of vendor integrity. Over-reliance on self-certification does not offer real assurance as to a vendor's integrity. After all, a third party may sign your supplier code of conduct, but do they really comply?
- Monitor historical relationships. Over time, the risk profile and compliance of a third party can change significantly and this should trigger additional scrutiny.
- Enforce audit rights or ask hard questions. This is especially critical when the relationship with a supplier starts to sour.
- Centralize compliance processes. Many larger organizations have not centralized their processes and therefore struggle to properly identify their third parties. This makes applying a consistent approach to detect and monitor potential supply chain fraud extremely tricky and can have some distressing consequences. For example, all too often, we have seen a business unit continue to do business with a third party while the rest of the group may have decided to stop the relationship after issues were identified.

Once an organization has a firm grip on its supplier universe, protecting itself from fraud and reputational risk becomes a less daunting task. A common sense, risk-based approach should ensure that an appropriate level of due diligence is conducted on higher risk suppliers and a simple escalation process needs to be in place to ensure that potential breaches are investigated and dealt with in a proactive manner.

KEVIN BRAINE
Managing Director,
Head of EMEA, Compliance
kevin.braine@kroll.com

JULIAN GRIJNS
Managing Director,
Investigations and Disputes,
North America
jgrijns@kroll.com

TAD KAGEYAMA
Regional Managing Director,
Head of Asia Operations,
Investigations and Disputes, APAC
tkageyama@kroll.com

CEM OZTURK
Managing Director,
Investigations and Disputes, APAC
cozturk@kroll.com

Training, Technology, and Tone from the Top: Remedies for Stemming Data Loss in Healthcare

Written by Devon Ackerman and Brian Lapidus

Findings from this year's Global Fraud & Risk Report underscore the severity of risks facing the global healthcare industry. Healthcare industry survey respondents who experienced at least one cyber incident in the past 12 months reported losses of personally identifiable information ("PII"), protected health information ("PHI"), employee records, and intellectual property at rates at least 15 percentage points higher than the market at large.

It is no secret healthcare entities regularly collect and store vast amounts of personally identifiable information belonging to patients, consumers, and employees, including Social Security number, date of birth, credit card information, medical insurance, and driver's license number. Each of these data points is highly valued by cyber criminals and often tied to even more sensitive patient information, such as medical diagnoses and health history.

Given the nature of the health industry, the need for open sharing of data to provide proper care intensifies the risk. Healthcare providers, administrators, and staff must all be able to access, edit, and transfer voluminous amounts of data. This provides ample opportunity for accidental exposure or malicious theft of the data by insiders. In addition, there has been an uptick in recent years of incidents reported to the U.S. Department of Health and Human Services caused by external hackers.

In this environment, security efforts can seem daunting. A review of representative Kroll casework gives a better picture of what can happen and how to respond.

In an example of **accidental exposure**, an employee downloaded 10,000 patient records onto an unencrypted USB drive to do some analysis; he was under a deadline and simply wanted to be able to work remotely. Unfortunately, the USB drive disappeared. We recommended tighter infrastructure controls (turn off ports so that employees cannot connect external devices to the network) and employee training (proper and secure data handling that follows company protocol).

Kroll was involved in an investigation of an individual (a **malicious insider**) who learned that their position was likely to be eliminated and decided to use their broad network access to download hundreds of gigabytes of patient, employee, donor, and financial data to a removable hard drive to leverage for "insurance." The employee had made insinuating remarks when let go, such that staff began questioning what might have occurred. Kroll was brought in for forensic analysis and, over the course of the next week, identified the data taken, including volume and timing, and used that information to help the client get ahead of the pending data breach-related issues surrounding the theft.

In a case of **social engineering/phishing**, an organization's human resources department was targeted during tax season by a phishing scheme. An email appeared to be coming from an internal executive requesting W-2 information on employees. Personnel complied with this very legitimate-looking order from leadership, including a follow-up to transfer funds via wire. The end result was a compromise of employee data as well as a loss of thousands of dollars. Training became an absolutely essential part of proactive measures to mitigate this kind of threat; this included sharing frequent alerts with employees regarding scams making the rounds. Tighter protocols for disclosure of PII or transfer of funds, even when involving the C-suite, were also implemented.

Kroll has also helped clients respond and remediate **ransomware** matters, where clients have found their data was inaccessible, and unreadable except for one message: their data was encrypted and a ransom with bitcoin was required to receive a decryption key. Ultimately, an organization will want to rely on backups of data stored on separate systems to rebound, which means a strenuous backup schedule, in addition to employee training, as ransomware is often deployed via a phishing attack. Security patches are essential, because ransomware attacks exploit known vulnerabilities most of the time. Most organizations are unaware that they should treat a ransomware incident like a data breach. Because it is difficult to know what was accessed, viewed, or exfiltrated, you don't want the clock to start ticking on a potential breach without essential advance preparation.

Leaders who set the tone from the top about the importance of information security can make a big impact with employees. This was particularly evident when Kroll recently entered into a new client relationship with a hospital system. Its privacy officer spoke with great reverence about their "duty to maintain the sanctity of the patients' data." By emphasizing how data privacy and security ultimately enhances the care of constituents, the privacy officer significantly raised awareness of the patient data privacy issue, which in turn helped the staff make it an integral part of their daily activities.

The healthcare entity that starts from the position of treating their data with the same level of care as their patients will find it easier to train a vigilant eye toward the unique data compromise threats the industry faces.

DEVON ACKERMAN
Associate Managing Director
Cyber Security and Investigations
devon.ackerman@kroll.com

BRIAN LAPIDUS
Managing Director,
Practice Leader,
Identity Theft and Breach Notification
blapidus@kroll.com

Asian Investment in the US – Navigating the Convergence of Increased Regulatory and Commercial Risk with Investment Opportunities

Written by Violet Ho, Nicole Lamb-Hale, and Naoko Murasaki

2017 was an unusual year in U.S.-Asia trade and investment. Asian companies seeking to invest in the U.S. market faced a rare level of uncertainty while continuing to favor the United States as a prime investment location.

Since the transition to a new presidential administration in the United States, the so-called "pivot" to Asia appears to have been reversed as showcased by the withdrawal of the United States from the Trans-Pacific Partnership ("TPP") in 2017. The U.S. withdrawal from TPP has challenged trade relations with much of Asia, including with Japan, who made significant market access accommodations to the United States in TPP negotiations and now faces talk of U.S. action to reduce the negative trade balance between the two countries. The trade relationship with South Korea is also challenged by recent indications that the trade agreement between South Korea and the United States ("Korus") may be in jeopardy because the negative trade balance with South Korea continues under Korus. Added to this uncertainty is the suggestion of import restrictions and increased tariffs which may reduce the value of investments in the United States by Asian multinational companies who manage their costs by leveraging global supply chains.

Turbulence on the U.S. trade policy front comes at the same time that uncertainty is growing on the regulatory front. This includes a push for more aggressive use of national security tools, such as the Committee on Foreign Investment in the United States ("CFIUS"), a federal, inter-agency committee charged with the national security review of transactions in which a foreign entity acquires control of a U.S. entity. Combined, all these factors are creating regulatory and commercial risks for Asian companies seeking to make investments in the United States. CFIUS risks have increased due to, among other things, proposed legislation expanding CFIUS' jurisdiction. A potential expansion of CFIUS jurisdiction may be particularly worrisome for Asian investors when considered in the context of the most recent CFIUS Annual Report to Congress[1]. Even under CFIUS' current and more limited jurisdiction, acquisitions by investors from China and Japan were in the top four of all covered transactions reviewed by CFIUS during the period discussed by the report.

Moreover, with respect to Chinese investors in particular, investment risks are compounded by the release in August 2017 of overseas investment guidelines by the Chinese government prohibiting certain overseas investments. The Chinese government has also issued a series of new measures to control capital outflow, which makes engaging in M&A activities in the United States and beyond increasingly challenging for cash-rich Chinese enterprises.

Notwithstanding these challenges, significant opportunities are available to Asian investors in the United States, particularly when such investment has the potential to sustain or increase U.S. jobs. How should investors navigate the convergence of regulatory and commercial risk with the significant investment opportunities in the United States? Companies from Asia and around the world may consider taking the following steps.

[1] http://bit.ly/UnclassifiedCFIUSAnnualReport-2015

1. SEEK PROFESSIONAL INSIGHTS ON WHETHER YOUR TRANSACTION MAY RAISE NATIONAL SECURITY CONCERNS.

If your transaction will result in control of a U.S. business, assess whether it may raise national security concerns before seeking CFIUS approval. While CFIUS approval is likely to be challenging in information technology and defense-related industries, national security concerns may also exist in the context of other, less apparent, industries. Therefore, seeking professional guidance before filing your CFIUS notice is prudent. Potential national security concerns should not be ignored, but rather proactively addressed working with professionals to develop mitigation strategies while minimizing commercial impacts.

2. ALIGN YOUR INVESTMENT WITH U.S. GOALS OF MAINTAINING AND CREATING JOBS.

Not withstanding the concerns of the U.S. government about the negative balance of trade with Asian nations including China, Japan, and South Korea, if your investment in the United States will result in existing jobs being maintained and/or new jobs being created, political and commercial risks are more likely to be minimized. As part of your diligence, develop a compelling economic narrative and align your investment with U.S. employment goals.

3. INVESTIGATE REGIONAL SENSITIVITIES ASSOCIATED WITH FOREIGN INVESTMENT.

Sensitivities associated with foreign investment in the United States exist not just at the federal level, but at the state, local, and civil society levels as well. Work with professionals to understand the state and local impact of the industry in which you seek to invest, shape your investment to enhance that impact, and identify allies among civic and community leaders to help promote its merits.

4. IN STRUCTURING YOUR INVESTMENT, LEARN FROM THE EXPERIENCES OF OTHERS.

As part of your due diligence, investigate the experiences of other foreign investors in your industry and in the region of the United States in which you plan to invest. The case studies of similarly situated companies can help prevent costly mistakes and aid the successful launch of your investment.

VIOLET HO
Senior Managing Director,
Head of Greater China,
Beijing and Shanghai Office Head
vho@kroll.com

NICOLE LAMB-HALE
Managing Director,
Investigations and Disputes,
North America
nicole.lamb-hale@kroll.com

NAOKO MURASAKI
Managing Director,
Head of Tokyo Office,
Investigations and Disputes, APAC
nmurasaki@kroll.com

Engaging the Board in Cyber Security Policies

Written by Andrew Beckett, Paul Jackson, and Jason Smolanoff

ANDREW BECKETT
Managing Director, EMEA Leader
Cyber Security and Investigations
andrew.beckett@kroll.com

PAUL JACKSON
Managing Director, APAC Leader
Cyber Security and Investigations
paul.jackson@kroll.com

JASON SMOLANOFF
Senior Managing Director,
Global Practice Leader
Cyber Security and Investigations
jason.smolanoff@kroll.com

Cyber security is often an aspect of business operations in which board members find it challenging to stay actively involved and to give meaningful direction to the organization. This is sometimes due to, or is at least frequently attributed to, the inherently complex nature of modern IT systems (and the equally complex security mechanisms placed around them) being beyond the technical understanding of most board members. But, as has been emphasized in previous Kroll Global Fraud & Risk Reports, it is more often the human element that leads to cyber crime, fraud, and data breaches. This is certainly an area where board members and senior business leaders can and should be playing a truly important role.

It appears from Kroll's latest Global Fraud & Risk Report survey that organizations are coming to this realization as well: 22% of respondents will be expanding their current use of board engagement to mitigate cyber risk, and nearly half (40%) are planning to launch new initiatives in the next 12 months to engage their boards.

Leading from the top matters. Employees are all too often referred to as the weakest link when in fact they should be regarded as the first line of defense. Direct involvement and example-setting by leadership should never be underestimated in shaping this mind-set. Trends also show that data losses are more often due to existing business processes that are exploited rather than direct attacks on the technology. Spotting gaps which ingenious attackers may utilize requires business acumen and people skills in addition to technical knowledge.

So how can boards become more effectively involved in cyber security risk mitigation efforts? Taking steps to become directly involved in thoroughly reviewing cyber security policies and procedures will go a long way toward demonstrating the importance that the board assigns to the subject. But this is only half the story: If led from the top, testing and validating the effectiveness of these policies can be vital in protecting the cyber security health of an organization.

The following seven discussions points form an effective starting point for boards working on establishing an active role in cyber security risk mitigation efforts:

1. DO YOU UNDERSTAND YOUR EXISTING CYBER SECURITY POLICIES AND PROCEDURES?

If not, there is a need for these policies and procedures to be rewritten in concise and clear language. These documents are only effective if they are immediately understandable and workable.

2. ARE YOU GETTING THE ANSWERS THAT YOU NEED ABOUT YOUR CYBER SECURITY POSTURE? INDEED, ARE YOU ASKING THE RIGHT QUESTIONS?

If the IT and/or cyber security leadership cannot properly and fully articulate the strategy for delivering information security, such that this can be fully understood at a board level, then questions need to be asked as to whether the right person is representing the organization in these matters. Boards have a duty to their shareholders and other stakeholders to ask detailed and probing questions relating to the organization's ability to protect its critical data assets.

3. IN DRAWING UP THE POLICIES AND PROCEDURES, HAVE YOU INVOLVED ALL THE BUSINESS HEADS?

Cyber security should not be considered as a silo. This is an organization-wide issue that needs input from leadership across the board, particularly when considering the gaps in business processes that may lead to cyber fraud and business disruption.

4. HAVE YOU INSTRUCTED THAT INCIDENT RESPONSE PLANS BE TESTED?

No matter how clear and well-written the policies and procedures may be, if they are never tested under realistic circumstances, then there is no way to determine whether they will work or not. Cyber crisis table-top exercises (involving leadership) can be the most effective means of identifying (and subsequently remedying) potentially disastrous gaps that would manifest in a real incident. Any test should involve not just your IT/Security team and the points of contact for the executive team and the board, but all those whose expertise you will rely on in the event of an incident – legal, investor relations, HR, external technical experts, external counsel, and the crisis communications teams, to name but a few of the most important stakeholders.

5. HOW ARE YOU MEASURING THE EFFECTIVENESS OF CYBER SECURITY SPENDING?

Boards are often asked to approve large sums for cyber security solutions and hires. Yet, what metrics do they have to measure whether these funds have been well spent? Has consideration been given to engaging independent external specialists to test the cyber security defenses in the same way that a real hacker would, without the prior knowledge of the cyber security team? Testing under real-life scenarios is the only way to effectively know if your security is working. In addition to testing, have you considered having your cyber security plans, projects, organization, and budgets reviewed by an independent third party? Companies like Kroll can review your organization's current state against the threats we see globally targeting others working in your market and geography, and discuss whether your plans are likely to address/detect the threats, and how your resource allocation compares with similar organizations.

6. ARE YOU LEADING BY EXAMPLE?

Enhanced cyber security often leads to restrictions and tighter controls on device access and usage. When properly explained, it should be realized that these are for the benefit of organizational security as a whole. If boards and executives accept these measures and adopt enhanced security controls (rather than requesting exemptions for convenience), then this sends a message that security starts at the top and must be adhered to by everyone. Personalized messages in support of cyber security education programs can also go a long way to promoting organization-wide awareness and responsibility.

7. HAVE YOU CONSIDERED ENLISTING EXPERT ADVISORS?

At the very least, regular board briefings by appropriate and credible cyber security experts is a must. Many boards nowadays are going one step further to engage this expertise in the form of non-executive board members. Boards are recognizing the steep cost that data losses and cyber attacks are exacting in terms of both shareholder and brand value, not to mention operational and litigation costs associated with remediation. By addressing cyber risk in the same way they do other critical organizational risks – i.e., managing the human factor and enlisting specialist support for legal and technical aspects – boards can play a vital role in safeguarding information assets in ways that meet wide-ranging regulatory and stakeholder expectations.

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.

1 CANADA
92% FRAUD
92% CYBER
79% SECURITY

3 MEXICO
85% FRAUD
92% CYBER
60% SECURITY

5 BRAZIL
84% FRAUD
89% CYBER
63% SECURITY

2 UNITED STATES
91% FRAUD
87% CYBER
73% SECURITY

4 COLOMBIA*
61% FRAUD
72% CYBER
55% SECURITY

*Low sample size. Directional data only.

6 UNITED KINGDOM
97% FRAUD
94% CYBER
71% SECURITY

7 ITALY
90% FRAUD
92% CYBER
56% SECURITY

9 MIDDLE EAST
66% FRAUD
71% CYBER
64% SECURITY

11 RUSSIA
89% FRAUD
80% CYBER
77% SECURITY

8 SUB-SAHARAN AFRICA
77% FRAUD
85% CYBER
72% SECURITY

10 INDIA
89% FRAUD
84% CYBER
74% SECURITY

12 CHINA
86% FRAUD
88% CYBER
75% SECURITY

Canada

92

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

▲ **4%** points above 2016
▲ **8%** points above the global average

FRAUD

The number of respondents reporting an incident of fraud grew from 88% in 2016 to 92% in this year's report, well above the global average of 84%. The most common type of fraud experienced by respondents in this country was theft of physical assets or stock, 41% versus 34% last year, and 14 percentage points higher than this year's global average. Information theft, loss, or attack was close behind, experienced by 38% of respondents, which was 9 percentage points higher than the global average.

Customers were reported to be the most likely perpetrators of fraud by those who experienced an incident. Almost four in 10 (39%) said that customers were to blame, compared with those who identified freelance/temporary employees (33%), and junior employees and ex-employees (28% of respondents named both categories).

Despite the significantly high level of reported fraud, respondents in Canada are not feeling highly vulnerable. Respondents were most likely to report feeling highly or somewhat concerned with three risk areas – information theft, management conflict of interest, and internal financial fraud, but at 59% each, these levels are virtually on par with global averages of 57%, 52%, and 52%, respectively.

While the most common anti-fraud measure taken by respondents to this year's survey was financial controls (including fraud detection, reported as being in place by 83%), management controls (78%) and the implementation of staff training and a whistleblower line (75%) were also popular measures.

More than half of those who experienced an incident (53%) said it was discovered through a whistleblower, higher than the global average of 47%.

MOST COMMON TYPES OF FRAUD		Global Avg.
Theft of physical assets or stock	41%	27%
Information theft, loss, or attack *(e.g., data theft)*	38%	29%
Internal financial fraud *(manipulation of company results)*	31%	23%

MOST COMMON PERPETRATORS		Global Avg.
Customers	39%	22%
Freelance/temporary employees	33%	26%
Junior employees	28%	39%
Ex-employees	28%	34%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
Information theft, loss, or attack *(e.g., data theft)*	59%	57%
Management conflict of interest	59%	52%
Internal financial fraud *(manipulation of company results)*	59%	52%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering)*	83%	77%
Management *(management controls, incentives, external supervision such as audit committee)*	78%	74%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
By a whistleblower at our company	53%	47%

92

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

▲ **7%** points above 2016
▲ **6%** points above global average

CYBER SECURITY

Continuing the theme of a growth in incidents reported by executives in Canada, the majority (92%) of respondents said that they had faced a cyber security attack in the previous 12 months, compared with 85% in 2016 and the global average of 86% this year.

In common with those in most other countries, the cyber incidents most likely to be experienced by respondents in Canada were email-based phishing attacks (41%) and data breaches (38%), with customer records most often being targeted, cited by 50% of respondents.

Respondents in Canada are not feeling particularly vulnerable to cyber incidents. At most, they feel highly or somewhat vulnerable to email-based phishing attacks, denial of service attacks, and virus/worm attacks, each cited by 57% of respondents.

Almost a third (31%) of respondents in Canada said that ex-employees were responsible for cyber security incidents. However, random cyber criminals were named as perpetrators by over half (53%) of respondents, highlighting that this is a particularly challenging problem in the region.

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Email-based phishing attack	41%	33%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	38%	27%
Virus/worm attack	33%	36%

MOST COMMON PERPETRATORS		Global Avg.
Random cyber criminals	53%	34%
Ex-employees	31%	28%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Email-based phishing attack	57%	57%
Denial of service attack	57%	52%
Virus/worm attack	57%	62%

MOST COMMON TARGET		Global Avg.
Customer records	50%	48%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service provider	33%	35%
Incident response firm *(investigations, breach notification)*	14%	11%

79

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

▲ **1%** point above 2016
▲ **9%** points above the global average

SECURITY

There was a small increase of 1 percentage point of respondents in Canada reporting a security breach, from 78% in 2016 to 79% in this year's report. While a relatively modest rise, it means respondents in Canada continue to report well over the global average (70% in this year's report) when it comes to security incidents. The incident most often reported was physical theft or loss of intellectual property (56%); this type of incident was also the focus of the greatest feelings of vulnerability for respondents at 59%.

Those responsible for security incidents were identified by respondents in Canada as ex-employees, cited by 45% of respondents.

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	56%	41%
Workplace violence	26%	23%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	26%	28%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	45%	37%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Physical theft or loss of intellectual property	59%	63%
Geographic and political risk *(i.e., operating in areas of conflict)*	48%	53%

United States

91

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

- ▲ **11%** points above 2016
- ▲ **7%** points above global average

FRAUD

Respondents in the United States reported one of the highest overall incidences of fraud in this year's survey at 91% of executives surveyed, well above the global average of 84% and also higher than last year's figure of 80%.

Information loss, theft, or attack was cited by over half of U.S. respondents (51%), the highest incidence in the survey and much higher than the global average of 29%. Respondents also reported one of the highest incidences of fraud caused by management conflict of interest (33%). This was equal to the number reporting thefts of physical assets or stock (33%).

Reflecting their actual experience, 73% of U.S. respondents feel highly or somewhat vulnerable to information theft, compared to a global average of just 57%. Additionally, the percentage who feel especially vulnerable to management conflict of interest is the highest among respondents in all countries in this report.

Technological issues were blamed for an increase in vulnerability to fraud, more than any other reason, with 54% citing the complexity of IT infrastructure and 45% blaming increased exposure to digital touchpoints, both well above global averages.

Internal audits were the most common method of discovery, credited by over half of respondents who had experienced an incident (51%).

Junior employees were reported by nearly half (48%) of respondents as being the main perpetrator of fraud that their organization had experienced, a significant rise on last year's reported figure of 36%.

MOST COMMON TYPES OF FRAUD		Global Avg.
Information theft, loss, or attack *(e.g., data theft)*	51%	29%
Theft of physical assets or stock	33%	27%
Management conflict of interest	33%	26%
IP theft *(e.g., of trade secrets)*, **piracy, or counterfeiting**	31%	20%
Internal financial fraud *(manipulation of company results)*	27%	23%

MOST COMMON PERPETRATORS		Global Avg.
Junior employees	48%	39%
Ex-employees	41%	34%
Senior or middle management employees	30%	27%
Freelance/temporary employees	30%	26%
Vendors/suppliers *(i.e., a provider of technology or services to your company)*	30%	30%
Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	30%	24%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
Information theft, loss, or attack *(e.g., data theft)*	73%	57%
Management conflict of interest	70%	52%
Internal financial fraud *(manipulation of company results)*	63%	52%
IP theft *(e.g., of trade secrets)*, **piracy, or counterfeiting**	60%	56%
Vendor, supplier, or procurement fraud	60%	51%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering)*	84%	77%
Assets *(physical security systems, stock inventories, tagging, asset register)*	82%	77%
Management *(management controls, incentives, external supervision such as audit committee)*	79%	74%
Information *(IT security, technical countermeasures)*	78%	78%
Staff *(background screening)*	78%	73%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
Through an internal audit	51%	44%

87

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **1%** point below 2016
- ▲ **1%** point above global average

CYBER SECURITY

Respondents from the United States were just above the average for the number of cyber incidents suffered (87% against an average of 86%), with email-based phishing attacks the most likely to be experienced (39%). The next most likely cyber incidents to be experienced include a virus or worm attack (37%) and a data breach (33%).

An unusually high proportion of those who experienced cyber incidents said that employee records were the target of the attack (64% against an average of 41%), with customer records being the second most common target (45%).

Ex-employees are the most common perpetrators for cyber incidents in the United States, cited by 36% of respondents who experienced an attack, followed by random cyber criminals (31%).

Respondents in the United States were most likely to feel highly or somewhat vulnerable to virus/worm attacks (71%), followed closely by data deletion and ransomware (each cited by 70%).

IT service vendors would be the most popular first port of call for cyber victims, cited by 48% of respondents in the United States against a global average of 35%.

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Email-based phishing attack	39%	33%
Virus/worm attack	37%	36%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	33%	27%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	36%	28%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Virus/worm attack	71%	62%
Data deletion	70%	58%
Ransomware attack	70%	55%

MOST COMMON TARGET		Global Avg.
Employee records	64%	41%
Customer records	45%	48%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	48%	35%
Federal law enforcement	12%	4%

73

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

- ▲ **15%** points above 2016
- ▲ **3%** points above the global average

SECURITY

Respondents in the United States were slightly more likely than most to report a physical security incident (73%), with incidents caused by environmental risks, including natural disasters, the most common (39%).

With physical security incidents, however, the perpetrators were more likely to be unknown to the company than with fraud or cyber incidents. Random perpetrators were cited by 37% of respondents in the United States, followed by competitors (35%).

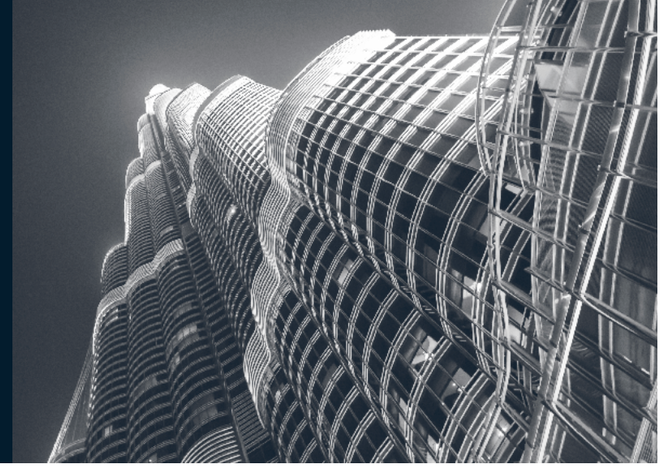
Respondents in the United States are feeling significantly more vulnerable to security risks this year as compared with last year. 69% of respondents report feeling highly or somewhat vulnerable to environmental risk, an increase of 24 points over last year. While slightly fewer – 67% – feel highly or somewhat vulnerable to geographic and political risk, this year's number is fully more than double last year's figure of 28%, an increase of 39 percentage points. Fears over terrorism, reported by 58% of respondents, spiked 30 percentage points this year.

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	39%	28%
Physical theft or loss of intellectual property	37%	41%
Geographic and political risk *(i.e., operating in areas of conflict)*	34%	20%

MOST COMMON PERPETRATORS		Global Avg.
Random perpetrators	37%	30%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	69%	56%
Geographic and political risk *(i.e., operating in areas of conflict)*	67%	53%
Physical theft or loss of intellectual property	65%	63%

Middle East



PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

- ▼ **22%** points below 2016
- ▼ **18%** points below global average

FRAUD

The number of respondents in the Middle East reporting a fraud incident in the last 12 months dropped to 66%, down from 88% last year.

The most widespread fraud incidents were a regulatory or compliance breach, cited by 24% of respondents, management conflict of interest (22%), and theft of physical assets or stock (19%).

Junior employees were the most likely to be named as perpetrators of fraud in the Middle East (62%) compared with just 34% last year. The second highest category of perpetrators of fraud was regulators (36%), more than twice the global average of 15%.

Fraud was more likely to be identified by management within the company, according to respondents in the Middle East. More than half (54%) said that management had uncovered a fraud incident, compared with 38% who said that it was uncovered through an external audit and 36% who named an internal audit. The number of respondents who said fraud was uncovered by a whistleblower fell from the number one position in 2016 (50%) to the fourth most likely source in this year's report (31%).

Executives in the Middle East felt particularly vulnerable to corruption and bribery as well as misappropriation of company funds, both at 61%, and significantly higher than the global averages of 50% and 48%, respectively.

MOST COMMON TYPES OF FRAUD		*Global Avg.*
Regulatory or compliance breach	24%	20%
Management conflict of interest	22%	26%
Theft of physical assets or stock	19%	27%

MOST COMMON PERPETRATORS		*Global Avg.*
Junior employees	62%	39%
Regulators	36%	15%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		*Global Avg.*
Corruption and bribery	61%	50%
Misappropriation of company funds	61%	48%
Information theft, loss, or attack *(e.g., data theft)*	58%	57%
IP theft *(e.g., of trade secrets)*, piracy, or counterfeiting	58%	56%
Internal financial fraud *(manipulation of company results)*	58%	52%
Vendor, supplier, or procurement fraud	58%	51%

MOST COMMON ANTI-FRAUD MEASURES		*Global Avg.*
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	69%	77%
Assets *(physical security systems, stock inventories, tagging, asset register)*	69%	77%
Information *(IT security, technical countermeasures)*	69%	78%

MOST COMMON MEANS OF DISCOVERY		*Global Avg.*
By management at our company	54%	35%

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **19%** points below 2016
- ▼ **15%** points below the global average

CYBER SECURITY

The proportion of respondents in the Middle East reporting a cyber incident also fell, from 90% in 2016 to 71% in this year's report.

Executives in the Middle East were most likely to cite competitors as the perpetrators of cyber incidents faced by their organization (33%), followed by agents/intermediaries (31%) and random cyber criminals (29%). The most common targets for cyber incidents were customer records and company/employee identity, each cited by 45% of respondents. The number one target last year was physical assets/money (47%), which slipped to fifth place in this year's survey (36%).

Respondents in the region felt highly or somewhat vulnerable to virus/worm attacks (80%), data deletion (76%), and wire transfer fraud (65%), all of which were significantly more than the global averages.

MOST COMMON TYPES OF CYBER INCIDENT		*Global Avg.*
Lost equipment with sensitive data	31%	19%
Data deletion	27%	25%
Email-based phishing attack	25%	33%

MOST COMMON PERPETRATORS		*Global Avg.*
Competitors	33%	23%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		*Global Avg.*
Virus/worm attack	80%	62%
Data deletion	76%	58%
Wire transfer fraud *(email account takeover/impersonation)*	65%	50%

MOST COMMON TARGET		*Global Avg.*
Customer records	45%	48%
Company/employee identity	45%	35%
Trade secrets/R&D/IP	43%	40%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		*Global Avg.*
IT service vendor	33%	35%
Incident response firm	17%	11%

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **18%** points below 2016
- ▼ **6%** points below the global average

SECURITY

Two-thirds of respondents in the Middle East (64%) said that they had suffered from a security incident in the previous 12 months, compared with 82% of respondents in last year's survey.

Security incidents were most likely to be caused by ex-employees, according to 39% of respondents in the Middle East. Physical theft or loss of intellectual property was the most common type of security incident (highlighted by 34% of respondents), but almost the same proportion (32%) said they had suffered from incidents associated with environmental risks, including damage caused by natural disasters.

Executives in the Middle East were most likely to feel highly or somewhat vulnerable to physical theft/loss of IP (61%, generally in line with the global average of 63%) and environmental risk (56%).

MOST COMMON TYPES OF SECURITY INCIDENT		*Global Avg.*
Physical theft or loss of intellectual property	34%	41%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	32%	28%

MOST COMMON PERPETRATORS		*Global Avg.*
Ex-employees	39%	37%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		*Global Avg.*
Physical theft or loss of intellectual property	61%	63%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	56%	56%

Italy

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

▲ **13%** points above 2016
▲ **6%** points above global average

FRAUD

The incidence of fraud reported by respondents in Italy was 90%, which is 6 percentage points above the global average of 84% and a significant increase on last year's figure of 77%.

The three most common types of fraud reported were IP theft (28%), theft of physical assets or stock (26%), and information theft, loss, or attack (26%). Regulatory or compliance breach dropped out of the top three reported fraud incidents in this year's report.

Ex-employees were cited as key perpetrators of fraud incidents by just over a third (34%) of respondents in Italy who suffered from attacks, followed by senior or middle management employees (31%) and freelance or temporary employees (26%). Current junior employees, reported as the main perpetrators of fraud in last year's report (50%), were far less likely to be named as the culprits this year (20%).

A majority (62%) of respondents in Italy felt highly or somewhat vulnerable to IP theft, 6 percentage points higher than the global average of 56%. Information theft, loss, or attack was also a major concern, with 54% of respondents feeling highly or somewhat vulnerable to this threat.

While internal whistleblowers were still the most common way in which fraud incidents were identified (46%), it represents a fall from last year's figure (53%) and is marginally below this year's global average of 47%.

MOST COMMON TYPES OF FRAUD		Global Avg.
IP theft *(e.g., of trade secrets)***, piracy, or counterfeiting**	28%	20%
Theft of physical assets or stock	26%	27%
Information theft, loss, or attack *(e.g., data theft)*	26%	29%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	34%	34%
Senior or middle management employees	31%	27%
Freelance/temporary employees	26%	26%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
IP theft *(e.g., of trade secrets)***, piracy, or counterfeiting**	62%	56%
Information theft, loss, or attack *(e.g., data theft)*	54%	57%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Risk *(risk officer and risk management system)*	83%	75%
Assets *(physical security systems, stock inventories, tagging, asset register)*	75%	77%
Information *(IT security, technical countermeasures)*	74%	78%
Board of Director engagement	74%	68%
Staff *(training, whistleblower hotline)*	69%	74%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
By a whistleblower at our company	46%	47%

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

▲ **13%** points above 2016
▲ **6%** points above global average

CYBER SECURITY

The vast majority (92%) of respondents in Italy said they had experienced a cyber incident in the previous 12 months. This was a substantial increase on last year's total of 79% and also higher than this year's global average of 86%.

Email-based phishing attacks were reported as the most common cyber incident, identified by 49% of respondents in Italy. This is a staggering 16 percentage points higher than the global average, and more than twice last year's figure of 21%.

In line with last year, ex-employees were the key perpetrators of cyber incidents in Italy (28%), on par with the global average (28%).

Executives in Italy felt particularly vulnerable to cyber incidents compared to respondents in other regions. They were most likely to feel highly or somewhat vulnerable to a ransomware attack and virus/worm attack (64% each), followed closely by alteration or change of data and data deletion (62% each).

The most likely targets for cyber incidents were customer records (39%), followed by company/employee identity (36%).

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Email-based phishing attack	49%	33%
Virus/worm attack	44%	36%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	28%	28%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Ransomware attack	64%	55%
Virus/worm attack	64%	62%
Alteration or change of data	62%	56%
Data deletion	62%	58%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	61%	55%

MOST COMMON TARGET		Global Avg.
Customer records	39%	48%
Company/employee identity	36%	35%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
ISP/Telecom provider	17%	7%
IT service vendor	14%	35%

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

▼ **12%** points below 2016
▼ **14%** points below the global average

SECURITY

There was a fall in the number of survey participants in Italy reporting a security incident from the prior year, down from 68% to 56% in this year's report and below the global average of 70%.

The three most common security incidents reported were physical theft or loss of IP (33%), geographic or political risk, such as operating in areas of conflict (21%), and environmental risk, including natural disasters (also 21%).

67% of respondents in Italy felt highly or somewhat vulnerable to terrorism threats, 18 percentage points higher than the global average of 49%. Second on the list was physical theft or loss of intellectual property, close behind at 65%.

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	33%	41%
Geographic and political risk *(i.e., operating in areas of conflict)*	21%	20%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	21%	28%

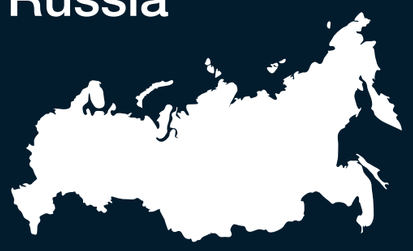
MOST COMMON PERPETRATORS		Global Avg.
Random perpetrator	36%	30%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Terrorism, including domestic and international events	67%	49%
Physical theft or loss of intellectual property	65%	63%

"The vast majority of respondents in Italy had experienced a cyber incident according to this year's survey, demonstrating the growing challenges faced by companies around information security. Executives in Italy are also feeling particularly vulnerable to bribery and corruption, despite significant government efforts and new anti-corruption legislation. Improving whistleblower protection to encourage employees to report suspected wrongdoing early could be a step in the right direction, helping companies stay on the front foot when dealing with these increasingly complex issues."

- Marianna Vintiadis
Managing Director, Head of Southern Europe, Investigations and Disputes, Kroll

Russia



89

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

- ▲ **7%** points above 2016
- ▲ **5%** points above global average

FRAUD

89% of respondents in Russia reported that their organization had uncovered a fraud incident in the past 12 months, an increase of 7 percentage points on the previous year (82%) and 5 percentage points higher than the global average of 84%.

The top three types of fraud experienced by respondents in Russia were internal financial fraud (cited by 34% of survey participants), management conflict of interest (26%), and theft of physical assets or information theft, loss, or attack (both 23%).

Vendors/suppliers were the most common perpetrators of fraud, named by 39% of respondents in Russia who had experienced a fraud incident. This figure was notably higher (9 percentage points) than the global average of 30%. Next most cited perpetrators were senior and middle management (32%) and ex-employees (29%). Junior employees seemed to be less involved in fraud incidents than in other regions, with only 16% of respondents in Russia naming them as key perpetrators of fraud, compared with a global average of 39%.

Executives in Russia were most likely to feel highly or somewhat vulnerable to market collusion, which at 60% was 10 percentage points higher than the global average for this threat. Respondents were also more likely than the global average to feel highly or somewhat vulnerable to modern slavery/human trafficking (51% versus the average of 40%).

MOST COMMON TYPES OF FRAUD		Global Avg.
Internal financial fraud *(manipulation of company results)*	34%	23%
Management conflict of interest	26%	26%
Information theft, loss, or attack *(e.g., data theft)*	23%	29%
Theft of physical assets or stock	23%	27%

MOST COMMON PERPETRATORS		Global Avg.
Vendors/suppliers *(i.e., a provider of technology or services to your company)*	39%	30%
Senior or middle management	32%	27%
Ex-employees	29%	34%
Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	26%	24%
Customers	26%	22%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
Market collusion *(e.g., price fixing)*	60%	50%
Theft of physical assets	51%	55%
Modern slavery/human trafficking	51%	40%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Information *(IT security, technical countermeasures)*	94%	78%
Assets *(physical security systems, stock inventories, tagging, asset register)*	87%	77%
Staff *(training, whistleblower hotline)*	87%	74%
Partners, clients, and vendors *(due diligence)*	87%	73%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
By a whistleblower at our company	74%	47%

80

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **2%** points below 2016
- ▼ **6%** points below the global average

CYBER SECURITY

The number of respondents in Russia reporting a cyber incident fell marginally from 82% in 2016 to 80% in this year's survey. The latest figure was also 6 percentage points lower than the global average of 86%.

Stolen equipment with sensitive data was one of the most prevalent types of cyber incident reported by respondents in Russia, equal to the number of email-based phishing attacks highlighted by just over a third of respondents (34%).

Respondents in Russia were more likely than those in any other country to report stolen equipment with sensitive data, with only the UK coming close with 32%. The global average was 21%.

Customer records were more likely to be targeted by cyber criminals in Russia than in other countries. Well over half (57%) of respondents reporting cyber incidents said customer records had been the target of attacks, higher than the global average of 48%.

There were also strong feelings of vulnerability around cyber incidents in Russia. Respondents in the region felt highly or somewhat vulnerable to email-based phishing attacks (71%), virus/worm attacks (69%), and data breaches (60%).

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Stolen equipment with sensitive data	34%	21%
Email-based phishing attack	34%	33%

MOST COMMON PERPETRATORS		Global Avg.
Random cyber criminal	39%	34%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Email-based phishing attack	71%	57%
Virus/worm attack	69%	62%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	60%	55%

MOST COMMON TARGET		Global Avg.
Customer records	57%	48%
Physical assets/money	46%	34%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	29%	35%
Regulator	21%	6%

77

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

- ▲ **18%** points above 2016
- ▲ **7%** points above the global average

SECURITY

There was a dramatic increase (18 percentage points) in the number of respondents in Russia reporting a security incident in this year's survey, with 77% being affected by security issues. This figure was also 7 percentage points higher than the global average (70%).

Ex-employees (41%) were the main perpetrators of security incidents, according to respondents who had suffered an incident, followed by random perpetrators, senior or middle management employees, and junior employees.

Executives in Russia were most likely to feel highly or somewhat vulnerable to environmental risks, which was cited by 63% of respondents, 7 percentage points higher than the global average of 56%. Workplace violence (54%) was also a key area of concern.

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	37%	28%
Physical theft or loss of intellectual property	31%	41%
Workplace violence	26%	23%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	41%	37%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	63%	56%
Workplace violence	54%	50%

Sub-Saharan Africa

77

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

- ▼ **12%** points below 2016
- ▼ **7%** points below global average

FRAUD

Sub-Saharan Africa is typically a region reporting a high incidence of fraud. However, this year's figure of 77% is a drop of 12 percentage points from the last survey and 7 percentage points below the global average of 84%.

Nevertheless, the region still has the highest prevalence of management conflict of interest (cited by 34% of respondents), money laundering (26%), and regulatory or compliance breach (25%), of all regions surveyed.

Third parties are a commonly cited risk factor, with joint venture partners and customers equally held responsible for incidents (34% each). Ex-employees were also named as key perpetrators by 34% of respondents. However, the most common perpetrators of fraud in the region were junior employees (44%).

Feelings of vulnerability were roughly in line with the global averages, with 53% of respondents feeling highly or somewhat vulnerable to information theft, loss, or attack, compared with a global average of 57%. Strong feelings of vulnerability were also noted around theft of physical assets (49%), followed closely by management conflict of interest, vendor, supplier, and procurement fraud, and misappropriation of company funds, each of which was cited by 47% of respondents.

A higher proportion of respondents in this region than in any other believed their companies were "not at all vulnerable" to a wide range of frauds, including modern slavery (49%), internal financial fraud (38%), misappropriation of company funds (32%), market collusion (32%), corruption or bribery (28%), and vendor, supplier, or procurement fraud (23%).

MOST COMMON TYPES OF FRAUD		Global Avg.
Management conflict of interest	34%	26%
Theft of physical assets or stock	28%	27%
Money laundering	26%	16%
Regulatory or compliance breach	25%	20%
Vendor, supplier, or procurement fraud	23%	20%

MOST COMMON PERPETRATORS		Global Avg.
Junior employees	44%	39%
Ex-employees	34%	34%
Joint venture partners *(i.e., a partner who provides manufacturing or other business function, or a franchisee)*	34%	23%
Customers	34%	22%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
Information theft, loss, or attack *(e.g., data theft)*	53%	57%
Theft of physical assets or stock	49%	55%
Management conflict of interest	47%	52%
Vendor, supplier, or procurement fraud	47%	51%
Misappropriation of company funds	47%	48%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
IP *(intellectual property risk assessment and trademark monitoring program)*	85%	73%
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	80%	77%
Partners, clients, and vendors *(due diligence)*	80%	73%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
By a whistleblower at our company	56%	47%
Through an internal audit	51%	44%

85

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **6%** points below 2016
- ▼ **1%** point below the global average

CYBER SECURITY

85% of respondents in the region reported a cyber security incident in this year's survey, roughly in line with the global average (86%).

The most prevalent cyber incident by far was a virus/worm attack, cited by almost half (47%) of executives, 11 percentage points above the global average of 36%. Alteration or change of data was also a common issue in the region, reported by 30% of respondents compared with a global average of 22%. This was reflected in feelings of vulnerability, with 59% of executives feeling highly or somewhat vulnerable to this type of cyber incident. Data breaches (59%) and email-based phishing attacks (58%) were also key concerns,

A third (33%) of cyber incidents reported in Sub-Saharan Africa were perpetrated by random cyber criminals.

Customer records were targeted in half of all cyber incidents reported (51%). Employee records were the main target in 44% of incidents.

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Virus/worm attack	47%	36%
Alteration or change of data	30%	22%

MOST COMMON PERPETRATORS		Global Avg.
Random cyber criminal	33%	34%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Alteration or change of data	59%	56%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	59%	55%
Email-based phishing attack	58%	57%

MOST COMMON TARGET		Global Avg.
Customer records	51%	48%
Employee records	44%	41%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	40%	35%

72

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **2%** points below 2016
- ▲ **2%** points above the global average

SECURITY

The percentage of respondents in the region experiencing a security incident dropped slightly to 72% compared with last year's 74%, and only 2 percentage points above the global average of 70%.

The top three types of security incident reported, namely physical theft or loss of IP (45%), environmental risk (34%), and workplace violence (26%), were all higher than the global averages of 41%, 28%, and 23%, respectively.

The most common perpetrators of security incidents were ex-employees, named in 39% of security incidents in the region, compared with a global average of 37%.

As well as being the most reported security incident, physical theft or loss of IP was also top of the list relating to feelings of high or moderate vulnerability in the region (68%). About half (51%) of respondents also feel highly or somewhat vulnerable to geographic and political risk.

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	45%	41%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	34%	28%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	39%	37%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Physical theft or loss of intellectual property	68%	63%
Geographic and political risk *(i.e., operating in areas of conflict)*	51%	53%

United Kingdom

97

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

- ▲ **7%** points above 2016
- ▲ **13%** points above global average

FRAUD

Respondents in the UK reported the highest incidence of fraud of all countries in this year's survey at 97%, surpassing last year's figure of 90% by 7 percentage points and this year's global average (84%) by 13 percentage points.

Money laundering was cited by a much higher percentage of UK respondents than any other country. Over a third (35%) said they had suffered a fraud incident involving money laundering, more than twice the global average of 16%.

The same proportion of UK respondents (35%) said they had suffered from theft of physical assets or stock, which was 8 percentage points higher than the global average (27%). The next most common fraud incident reported by UK respondents was information theft, loss, or attack (32%), also above the global average (29%).

Ex-employees were the most likely perpetrators of fraud incidents according to UK respondents. Almost half (45%) said that ex-employees were to blame compared to freelance/temporary employees (36%) and junior employees (33%).

Respondents in the UK were most likely to feel highly or somewhat vulnerable to IP theft, piracy, or counterfeiting; management conflict of interest; regulatory or compliance breach; and market collusion. Each of these threats was cited by 68% of respondents.

The most common anti-fraud measures being carried out by UK respondents' companies focused on employees. Staff background screening (88%) and staff training/whistleblower hotline (81%) were at the top of the list, both higher than the global averages (73% and 74%, respectively).

Fraud was most likely to be discovered through an internal audit, cited by 48% of respondents in the UK, 4 percentage points higher than the global average (44%).

MOST COMMON TYPES OF FRAUD		Global Avg.
Money laundering	35%	16%
Theft of physical assets or stock	35%	27%
Information theft, loss, or attack *(e.g., data theft)*	32%	29%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	45%	34%
Freelance/temporary employees	36%	26%
Junior employees	33%	39%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
IP theft *(e.g., of trade secrets)*, piracy, or counterfeiting	68%	56%
Management conflict of interest	68%	52%
Regulatory or compliance breach	68%	49%
Market collusion *(e.g., price fixing)*	68%	50%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Staff *(background screening)*	88%	73%
Staff *(training, whistleblower hotline)*	81%	74%
Assets *(physical security systems, stock inventories, tagging, asset register)*	81%	77%
Partners, clients, and vendors *(due diligence)*	79%	73%
Information *(IT security, technical countermeasures)*	78%	78%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
Through an internal audit	48%	44%

94

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▲ **2%** points above 2016
- ▲ **8%** points above the global average

CYBER SECURITY

The majority of respondents (94%) in the UK said they had experienced a cyber security incident in the past year, a slight rise on last year's figure of 92% and well ahead of the global average of 86%.

The most common type of cyber security incident was virus/worm attack, reported by 41% of UK respondents. The second most prevalent was email-based phishing attack, reported by 38% of UK respondents.

Respondents in the UK were most likely to feel highly or somewhat vulnerable to stolen equipment with sensitive data, which at 68% is significantly out of proportion to the actual reported experience of this risk (32%). Wire transfer fraud was also a great concern, which at 68% was 18 percentage points higher than the global average.

More than two-thirds (69%) of UK respondents said employee records were targeted in cyber incidents, a remarkable 28 percentage points above the global average of 41%.

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Virus/worm attack	41%	36%
Email-based phishing attack	38%	33%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	35%	27%
Stolen equipment with sensitive data	32%	21%

MOST COMMON PERPETRATORS		Global Avg.
Freelance/temporary employees	31%	18%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Stolen equipment with sensitive data	68%	55%
Wire transfer fraud *(email account takeover/impersonation)*	68%	50%
Virus/worm attack	65%	62%
Lost equipment with sensitive data	62%	53%

MOST COMMON TARGET		Global Avg.
Employee records	69%	41%
Customer records	47%	48%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	31%	35%
Incident response firm *(investigations, breach notification)*	16%	11%

71

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **11%** points below 2016
- ▲ **1%** point above the global average

SECURITY

UK respondents reported fewer security incidents this year, with 71% of respondents saying they had experienced a security incident compared with 82% in 2016.

The most common security incident reported in the UK, as with most regions, was physical theft or loss of intellectual property (44%), followed by geographic and political risk (32%). Perhaps as a result, UK respondents are also most likely to feel highly or somewhat vulnerable to these risks, with 71% citing concerns over terrorism, and 70% worried about physical theft or loss of IP.

Ex-employees top the list of perpetrators of security incidents, cited by 38% of UK respondents. This is a sharp increase of 10 percentage points on last year, and in line with the global average (37%).

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	44%	41%
Geographic and political risk *(i.e., operating in areas of conflict)*	32%	20%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	38%	37%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Terrorism, including domestic and international events	71%	49%
Physical theft or loss of intellectual property	70%	63%
Geographic and political risk *(i.e., operating in areas of conflict)*	67%	53%

China

86

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

= same as 2016

▲ **2%** points above global average

FRAUD

86% of respondents in China experienced fraud in the previous 12 months, 2 percentage points above the global average of 84%. The most common types of fraud experienced were vendor, supplier, or procurement fraud and corruption and bribery, both at 29%, significantly higher than the global averages of 20% and 21%, respectively. The next highest types of fraud experienced by respondents in China were management conflict of interest and information theft, loss, or attack, both at 28%.

Vendors/suppliers (39%) and senior or middle management (25%) were among the most common perpetrators of fraud as reported by survey respondents. Ex-employees were also reported to have been heavily involved in fraud incidents, as identified by 21% of executives in the region.

Respondents in China were most likely to feel highly or somewhat vulnerable to IP theft, piracy, or counterfeiting (48%), market collusion (47%), and management conflict of interest and corruption and bribery (both at 46%).

When asked about fraud prevention measures, respondents in China cited financial controls (82%), internal whistleblower hotline (81%), and asset protection (80%) as the top three measures already implemented at their companies. All three measures were above the global averages of 77%, 74%, and 77%, respectively.

MOST COMMON TYPES OF FRAUD		Global Avg.
Vendor, supplier, or procurement fraud	29%	20%
Corruption and bribery	29%	21%
Information theft, loss, or attack *(e.g., data theft)*	28%	29%
Management conflict of interest	28%	26%

MOST COMMON PERPETRATORS		Global Avg.
Junior employees	50%	39%
Vendors/suppliers	39%	30%
Senior or middle management	25%	27%
Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	23%	24%
Ex-employees	21%	34%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
IP theft *(e.g., of trade secrets)*, piracy, or counterfeiting	48%	56%
Market collusion *(e.g., price fixing)*	47%	50%
Management conflict of interest	46%	52%
Corruption and bribery	46%	50%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering)*	82%	77%
Staff *(training, whistleblowing hotline)*	81%	74%
Assets *(physical security systems, stock inventories, tagging, asset register)*	80%	77%
Information *(IT security, technical countermeasures)*	79%	78%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
Through an internal audit	48%	44%

88

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

▲ **2%** points above 2016

▲ **2%** points above global average

CYBER SECURITY

The percentage of respondents in China saying their company had experienced a cyber incident in the past year (88%) is slightly higher than the global average of 86%.

Data breach is the most common type of cyber incident, reported by 38% of respondents compared to just 27% globally. Despite this, the proportion of respondents based in China who believe their company is highly vulnerable to a data breach (15%) is lower than the global average of 21%.

Competitors were cited as the key perpetrators of cyber incidents at 32%, notably higher than the global average of 23%.

Respondents in China also reported feeling highly or somewhat vulnerable to email-based phishing attacks (55%), data breaches (53%), and wire transfer fraud (52%).

Trade secrets, R&D, or IP is the main target of cyber attacks, with 61% of cyber-related victims in China claiming these assets were targeted, well above the global average of 40% and the highest of all countries surveyed globally. Customer records were the second most common target, named by 42% of victims of cyber incidents.

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	38%	27%
Virus/worm attack	31%	36%
Alteration or change of data	25%	22%
Lost equipment with sensitive data	25%	19%

MOST COMMON PERPETRATORS		Global Avg.
Competitors	32%	23%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Email-based phishing attack	55%	57%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	53%	55%
Wire transfer fraud *(email account takeover/impersonation)*	52%	50%

MOST COMMON TARGET		Global Avg.
Trade secrets/R&D/IP	61%	40%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	26%	35%
Incident response firm *(investigations, breach notification)*	18%	11%

75

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

= same as 2016

▲ **5%** points above the global average

SECURITY

75% of respondents in China were affected by a security incident in the past year, 5 percentage points higher than the global average of 70%.

The two most common types of security incident experienced by respondents in China were physical theft or loss of IP (48%), and environmental risks such as floods or earthquakes (31%). Yet, when asked which security incidents they felt highly or somewhat vulnerable to, respondents put environmental risk at the top of their concerns (60%).

One in three respondents (33%) who experienced a security incident named former employees as the key perpetrators.

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	48%	41%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	31%	28%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	33%	37%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	60%	56%

India

89

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

- ▲ **21%** points above 2016
- ▲ **5%** points above global average

FRAUD

India has seen a significant increase in fraud since last year's report, with 89% of respondents in Indian organizations saying they had experienced a fraud incident in the previous 12 months, compared with just 68% in 2016 and the global average this year of 84%.

Respondents in India report one of the world's highest incidences of theft of physical assets or stock, with two-fifths (40%) saying they had experienced this type of fraud, second only to those in Canada (41%). Theft of intellectual property (36%) and market collusion (36%) are also high on the list of incidents of fraud in India according to respondents.

Executives in India say that perpetrators of fraud are most likely to be joint venture partners (45%), junior employees (43%), and vendors or suppliers (40%).

Reflecting their actual experience, respondents in India are feeling highly or somewhat vulnerable to a number of risks; in fact, India figures among the top three countries globally for every category measuring fraud vulnerability in this survey except for vendor, supplier, or procurement fraud. Nearly nine in 10 respondents (87%) cited information theft, loss, or attack as their greatest concern, 30 percentage points higher than the global average of 57%. Internal financial fraud (85%) and IP theft, piracy, and counterfeiting (80%) were also significantly higher than the global averages of 52% and 56%, respectively.

A higher proportion of respondents in India than in any other country cited joint venture partners (45%) as the main reason for increased exposure to fraud.

Indian organizations are becoming more aware of the risks and, according to respondents, are implementing preventive measures such as financial controls (83%) and physical security systems (83%).

MOST COMMON TYPES OF FRAUD		Global Avg.
Theft of physical assets or stock	40%	27%
IP theft *(e.g., of trade secrets)*, piracy, or counterfeiting	36%	20%
Market collusion *(e.g., price fixing)*	36%	19%

MOST COMMON PERPETRATORS		Global Avg.
Joint venture partners *(i.e., a partner who provides manufacturing or other business function or a franchisee)*	45%	23%
Junior employees	43%	39%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
Information theft, loss, or attack *(e.g., data theft)*	87%	57%
Internal financial fraud *(manipulation of company results)*	85%	52%
IP theft *(e.g., of trade secrets)*, piracy, or counterfeiting	80%	56%
Theft of physical assets or stock	78%	55%
Money laundering	76%	43%
Market collusion *(e.g., price fixing)*	73%	50%
Regulatory or compliance breach	71%	49%
Vendor, supplier, or procurement fraud	71%	51%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering)*	83%	77%
Assets *(physical security systems, stock inventories, tagging, asset register)*	83%	77%
Risk *(risk officer and risk management system)*	81%	75%
Reputation *(media monitoring, compliance controls, legal review)*	80%	72%
IP *(intellectual property risk assessment and trademark monitoring program)*	80%	73%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
By management at our company	55%	35%
By a whistleblower at our company	55%	47%

84

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▲ **11%** points above 2016
- ▼ **2%** points below global average

CYBER SECURITY

84% of respondents in India have experienced a cyber attack in the last year, 11 percentage points more than in 2016 (73%). Nearly half of these respondents experienced email-based phishing attacks (44%). Virus/worm attacks were the second most common type of incident reported (36%).

Reflecting their actual experience, 80% of respondents in India feel highly or somewhat vulnerable to an email-based phishing attack. Other major concerns center on data deletion (78%), alteration or change of data (77%), and virus/worm attacks (72%).

The most common targets for cyber attacks in India were employee records (55%), trade secrets/IP (55%), and customer records (55%). Trade secrets/IP and customer records were targeted significantly more often than last year.

Random cyber criminals were most often cited by respondents (45%) as the perpetrators of cyber incidents.

Respondents in India this year report employee safety, privacy, and morale as being negatively affected (84%) by cyber incidents, along with customer privacy, safety, satisfaction, and company reputation (84%).

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Email-based phishing attack	44%	33%
Virus/worm attack	36%	36%

MOST COMMON PERPETRATORS		Global Avg.
Random cyber criminals	45%	34%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Email-based phishing attack	80%	57%
Data deletion	78%	58%
Alteration or change of data	77%	56%
Virus/worm attack	72%	62%
Denial of service attack	71%	52%

MOST COMMON TARGET		Global Avg.
Customer records	55%	48%
Employee records	55%	41%
Trade secrets/R&D/IP	55%	40%

74

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

- ▲ **2%** points above 2016
- ▲ **4%** points above the global average

SECURITY

Three-quarters (74%) of respondents in India experienced a security incident in the last 12 months, an increase on the number from 2016 (72%) and higher than the global average of 70%.

The most likely type of security incident in India is physical theft or loss of intellectual property (47%), followed by workplace violence (33%). This reality is reflected in respondents' feelings of vulnerability that far outpace the global averages: 80% are highly or somewhat concerned about physical theft or loss of IP (17 percentage points higher than the global average of 63%), while 78% worry about workplace violence (28 percentage points higher than the global average of 50%). Respondents from India were also significantly more apt to be concerned with terrorism threats, 74% versus a global average of 49%.

Employees are a big risk for organizations in India, with more than half of respondents (52%) naming senior or middle management as key perpetrators of security incidents, while ex-employees were named as perpetrators by two-fifths (42%) of respondents.

A vast majority (91%) noted that a security incident had negatively affected employee privacy, safety, and morale; customer privacy, safety, and satisfaction were also affected said 75% of respondents.

Over half (53%) of respondents in India report they have been dissuaded from operating in other regions and countries because of concerns with security risks. The main countries identified were other South Asian countries – i.e., Pakistan, Bangladesh, and Sri Lanka (22%) – with Japan close behind (20%).

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	47%	41%
Workplace violence	33%	23%

MOST COMMON PERPETRATORS		Global Avg.
Senior or middle management employees	52%	25%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Physical theft or loss of intellectual property	80%	63%
Workplace violence	78%	50%
Terrorism, including domestic and international events	74%	49%

Brazil

84

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

▲ **16%** points above 2016
= same as global average

FRAUD

Brazil has seen a significant increase in fraud over the last year, with 84% of respondents reporting an incidence of fraud over the last 12 months compared with just 68% in 2016. The most widespread types of fraud experienced by respondents in Brazil were a regulatory or compliance breach (29%) and internal financial fraud (29%). In 2016, the most prevalent type of fraud in Brazil was theft of physical assets or stock.

Ex-employees are a serious fraud risk for organizations in Brazil, according to executives surveyed for the report. In fact, more than half of respondents in the country (53%) named ex-employees as the key perpetrators of fraud, the second highest response across all regions. The other main group of perpetrators named by respondents was senior or middle management (41%).

The impact of fraud on organizations in Brazil has been predominantly on people – whether that was the privacy, safety, and morale of employees (81%) or the safety, satisfaction, and privacy of customers (81%). Increased outsourcing and offshoring was listed as the main factor for increasing exposure to fraud for half of organizations in Brazil (50%) – more so than any other country.

Respondents in Brazil feel highly or somewhat vulnerable to management conflict of interest (63%), followed by internal financial fraud (58%) and vendor, supplier, or procurement fraud (58%).

According to respondents, organizations in Brazil are becoming more aware of the risks and are implementing fraud prevention measures including financial controls (84%) and asset controls such as physical security systems (82%).

MOST COMMON TYPES OF FRAUD		Global Avg.
Regulatory or compliance breach	29%	20%
Internal financial fraud *(manipulation of company results)*	29%	23%
Information theft, loss, or attack *(e.g., data theft)*	26%	29%
Management conflict of interest	24%	26%
Misappropriation of company funds	21%	20%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	53%	34%
Senior or middle management employees	41%	27%
Freelance/temporary employees	28%	26%
Vendors/suppliers *(i.e., a provider of technology or services to your company)*	25%	30%
Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	19%	24%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
Management conflict of interest	63%	52%
Internal financial fraud *(manipulation of company results)*	58%	52%
Vendor, supplier, or procurement fraud	58%	51%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering)*	84%	77%
Assets *(physical security systems, stock inventories, tagging, asset register)*	82%	77%
Information *(IT security, technical countermeasures)*	76%	78%
Staff *(background screening)*	76%	73%
Risk *(risk officer and risk management system)*	76%	75%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
Through an internal audit	66%	44%

89

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

▲ **13%** points above 2016
▲ **3%** points above global average

CYBER SECURITY

Respondents in Brazil also reported a rise in cyber incidents over the last year, with 89% reporting an attack in 2017, compared with just 76% in 2016. Nearly half of respondents have experienced a virus or worm attack (45%).

This experience has translated to 63% of respondents feeling highly or somewhat vulnerable to virus/worm attacks. 61% have similarly heightened concerns over email-based phishing attacks.

The targets of cyber incidents in Brazil were customer records (47%) as well as trade secrets and research and development of IP (44%).

Ex-employees were cited as the key perpetrators of cyber incidents over the last year in Brazil (32%) followed by competitors (21%). The impact of cyber crime goes beyond the bottom line. Respondents in Brazil reported customer privacy, safety, and satisfaction (80%) as being negatively affected, along with employee safety, privacy, and morale (76%).

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Virus/worm attack	45%	36%
Email-based phishing attack	37%	33%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	32%	28%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Virus/worm attack	63%	62%
Email-based phishing attack	61%	57%
Alteration or change of data	55%	56%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	55%	55%
Ransomware attack	55%	55%
Denial of service attack	55%	52%

MOST COMMON TARGET		Global Avg.
Customer records	47%	48%
Trade secrets/R&D/IP	44%	40%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	47%	35%

63

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

▲ **10%** points above 2016
▼ **7%** points below global average

SECURITY

Two-thirds of respondents in Brazil (63%) have been affected by a security incident in the last year, an increase of 10 percentage points on the number experienced by respondents in 2016 (53%), although still lower than the global average of 70%. The most prevalent type of security incident reported by respondents was physical theft or loss of intellectual property (42%), much higher than the second highest type of security, workplace violence (16%).

Reflecting their actual experience, respondents in Brazil are most likely to feel highly or somewhat vulnerable to physical theft or loss of IP (69%).

Again, ex-employees were the key perpetrators of security incidents, reported by two-fifths of respondents (42%), closely followed by freelance or temporary employees (38%). Over half of respondents in Brazil reported they have been dissuaded from operating in other countries as a result of the threat posed by security risks.

In response to the threat posed by potential security incidents, the majority of respondents have developed security policies and procedures (92%), implemented security training (88%), put a business continuity plan in place (88%), and performed security audits (88%).

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	42%	41%
Workplace violence	16%	23%
Geographic and political risk *(i.e., operating in areas of conflict)*	13%	20%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	13%	28%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	42%	37%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Physical theft or loss of intellectual property	69%	63%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	60%	56%
Geographic and political risk *(i.e., operating in areas of conflict)*	53%	53%

Colombia

61

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.*

FRAUD

Slightly more than six out of 10 respondents in Colombia reported experiencing an incident of fraud in 2017 (61%). The most common type of fraud experienced by respondents was information theft (33%); this level was close behind what respondents in Mexico reported (38%). Misappropriation of company funds was the second most cited incident, reported by 22% of respondents.

In contrast to other respondents globally, respondents in Colombia most commonly identified ex-employees as the perpetrators of fraud (55%) compared with the global average of just 34%.

Respondents in Colombia were most likely to feel highly or somewhat vulnerable to IP theft, piracy, and counterfeiting, which at 67% was the highest level reported for Latin America. Similarly, respondents in Colombia had greater concerns over regulatory and compliance breaches (55%), than did those in Brazil (42%) or Mexico (33%).

In nearly two-thirds (64%) of cases as experienced by respondents, instances of fraud were discovered through a whistleblower in the organization. Respondents also reported an internal audit as the most common method of fraud detection (50%).

Respondents in Colombia were more likely than those in other countries to say that employee privacy, safety, and morale were strongly affected by fraud (55% compared with 34% globally). Over half of respondents in Colombia named high staff turnover as a reason behind their company's vulnerability to fraud (56%), making it the most common contributory factor. Globally, 34% of respondents named high staff turnover as causing vulnerability to fraud.

MOST COMMON TYPES OF FRAUD		Global Avg.
Information theft, loss, or attack *(e.g., data theft)*	33%	29%
Misappropriation of company funds	22%	20%
Management conflict of interest	17%	26%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	55%	34%
Junior employees	36%	39%
Freelance/temporary employees	36%	26%
Customers	27%	22%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
IP theft *(e.g., of trade secrets)*, piracy, or counterfeiting	67%	56%
Regulatory or compliance breach	55%	49%
Theft of physical assets or stock	50%	55%
Corruption and bribery	50%	50%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Risk *(risk officer and risk management system)*	91%	75%
Board of Director engagement	81%	68%
Management *(management controls, incentives, external supervision such as audit committee)*	81%	74%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
By a whistleblower at our company	64%	47%

* Low sample size. Directional Data only.

72

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.*

CYBER SECURITY

72% of respondents in Colombia said that their company had experienced a cyber incident in the past 12 months, with customer records being the most common target in these attacks (46%).

The most common type of cyber incident reported was a virus/worm attack (cited by 44% of respondents), followed by data deletion (33%). In 2017, ex-employees and random cyber criminals were equally cited (31%) as the perpetrators of cyber incidents. Although more respondents reported experiencing a virus/worm attack, they felt more highly or somewhat vulnerable to risks such as alteration or change of data (56%), stolen equipment with sensitive data (56%), and data deletion or lost equipment with sensitive data (each cited by 50% of respondents).

Globally, respondents reported that the most common reaction to a cyber incident is to contact their IT service vendor (35%). In Colombia, however, only 15% selected this option; contacting an incident response firm was selected as the most popular option by respondents (23%).

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Virus/worm attack	44%	36%
Data deletion	33%	25%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	31%	28%
Random cyber criminal	31%	34%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Alteration or change of data	56%	56%
Stolen equipment with sensitive data	56%	55%
Data deletion	50%	58%
Lost equipment with sensitive data	50%	53%

MOST COMMON TARGET		Global Avg.
Customer records	46%	48%
Trade secrets/R&D/IP	38%	40%
Physical assets/money	38%	34%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
Incident response firm	23%	11%

55

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.*

SECURITY

Slightly more than half (55%) of respondents in Colombia said that their organization experienced a security incident in the past 12 months. Physical theft or loss of IP was the most common type of security incident experienced, as identified by 39% of respondents. This experience underscores the finding that 56% of respondents reported feeling highly or somewhat vulnerable to this threat.

As with cyber security, respondents in Colombia were most likely to identify random perpetrators and ex-employees as the perpetrators of security incidents (40% each). 80% of respondents said these incidents have affected company revenue and business continuity.

Respondents in Colombia were less likely than average to say that their company had conducted a threat and vulnerability assessment (50% compared with global average of 72%), and also more likely than average to report that they had no plans to conduct any such assessment (20% compared with global average of 9%). One-fifth reported that they have not implemented, and had no plans to implement, a security audit, a security master plan, a plan for securing intellectual property, an executive protection plan, threat management plans and procedures, an information security plan, or a business continuity plan.

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	39%	41%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	40%	37%
Random perpetrator	40%	30%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Physical theft or loss of intellectual property	56%	63%
Workplace violence	50%	50%
Terrorism, including domestic and international events	50%	49%

Mexico

85

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

- ▲ **3%** points above 2016
- ▲ **1%** point above global average

FRAUD

The number of respondents in Mexico whose organizations experienced a fraud incident rose slightly from 82% in 2016 to 85% in this year's report.

In common with respondents from the United States and Canada, those in Mexico reported higher than average levels of information theft, loss, or attack (38%) than the global average (29%). One-third of respondents also cited incidents of corruption and bribery. Vendor, supplier, or procurement fraud, notably reported by 52% of respondents in Mexico in 2016, was only cited by 17% in this year's survey.

Respondents in Mexico were more likely than the global average to feel highly or somewhat vulnerable to theft of physical assets or stock (58% versus 55% global average). More than half of respondents also have concerns over corruption and bribery (54%) and IP theft, piracy, and counterfeiting (51%).

Respondents said that their organizations had addressed the rising tide of fraud by implementing IT security and technical countermeasures; staff training and whistleblower hotline; and management controls and incentives.

Half (49%) of survey respondents whose organizations had experienced a fraud incident in Mexico cited junior employees as perpetrators, followed by ex-employees and vendors and suppliers.

MOST COMMON TYPES OF FRAUD		Global Avg.
Information theft, loss, or attack *(e.g., data theft)*	38%	29%
Corruption and bribery	31%	21%
Theft of physical assets or stock	29%	27%
Management conflict of interest	27%	26%
Misappropriation of company funds	23%	20%

MOST COMMON PERPETRATORS		Global Avg.
Junior employees	49%	39%
Ex-employees	37%	34%
Vendors/suppliers *(i.e., a provider of technology or services to your company)*	34%	30%
Freelance/temporary employees	24%	26%
Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	24%	24%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
Theft of physical assets or stock	58%	55%
Corruption and bribery	54%	50%
IP theft *(e.g., of trade secrets)*, piracy, or counterfeiting	51%	56%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Staff *(training, whistleblower hotline)*	86%	74%
Information *(IT security, technical countermeasures)*	83%	78%
Management *(management controls, incentives, external supervision such as audit committee)*	80%	74%
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering)*	78%	77%
Assets *(physical security systems, stock inventories, tagging, asset register)*	73%	77%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
Through an internal audit	54%	44%

92

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▲ **10%** points above 2016
- ▲ **6%** points above the global average

CYBER SECURITY

The percentage of respondents in Mexico who reported a cyber incident in the previous 12 months grew to 92% from 82% in the 2016 report. The biggest challenge facing their organizations was reported as data deletion. At 35% of respondents, this was the highest incidence of data deletion across all regions.

Respondents in Mexico are most likely to feel highly or somewhat vulnerable to virus/worm attacks (53%), followed by concerns over data deletion (50%), which might reflect respondents' growing experience or awareness of this fraud.

Well over half (55%) of respondents said that customer records were targeted in cyber incidents experienced by their organizations. The next most likely target was employee records, followed by physical assets or money.

Last year, respondents in Mexico said they were most likely to reach out to federal law enforcement to report a cyber incident. This year, a third of respondents said that they turned first to their IT service vendor.

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Data deletion	35%	25%
Virus/worm attack	33%	36%
Email-based phishing attack	29%	33%
Stolen equipment with sensitive data	27%	21%

MOST COMMON PERPETRATORS		Global Avg.
Random cyber criminal	45%	34%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Virus/worm attack	53%	62%
Data deletion	50%	58%

MOST COMMON TARGET		Global Avg.
Customer records	55%	48%
Employee records	45%	41%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	34%	35%
Insurance carrier hotline	11%	3%

60

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

- ▲ **12%** points above 2016
- ▼ **10%** points below the global average

SECURITY

Respondents in Mexico reported a higher level of security incidents this year (60% compared with 48% in 2016). However, this was still lower than the average globally (70%).

The most common type of security incident experienced by respondents in Mexico by far was physical theft or loss of intellectual property, reported by 38%. Workplace violence, last year's most commonly reported type of security incident by executives in Mexico, was reported by 23%, equal to the global figure.

Respondents in Mexico are most likely to feel highly or somewhat vulnerable to physical theft or loss of IP (58%) followed by workplace violence (40%).

Ex-employees were reported as the most likely cause for security incidents. More than four in 10 (41%) cited them as the perpetrators, compared to a global average of 37% and last year's figure of 31%.

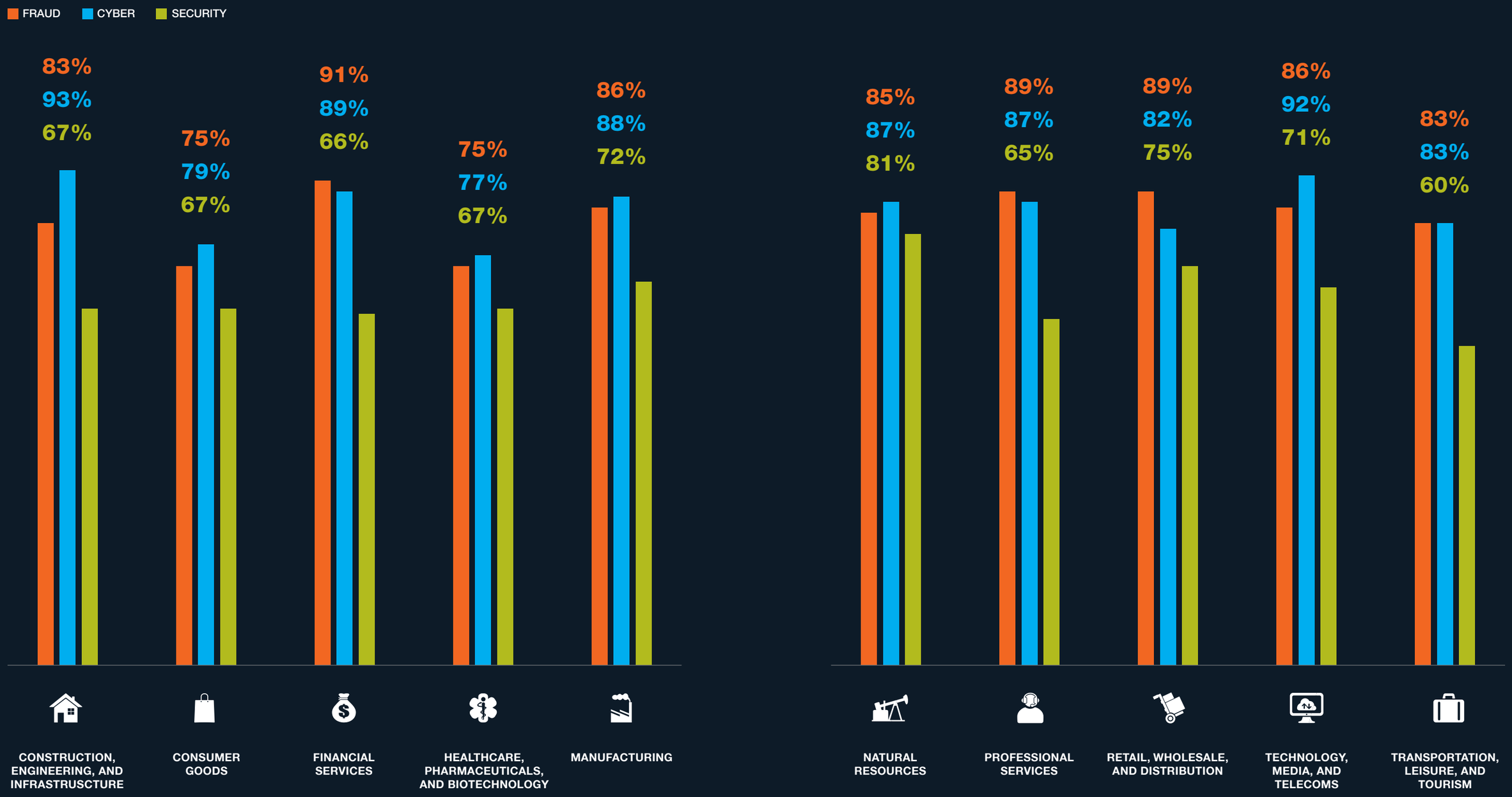
MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	38%	41%
Geographic and political risk *(i.e., operating in areas of conflict)*	25%	20%
Workplace violence	23%	23%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	15%	28%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	41%	37%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Physical theft or loss of intellectual property	58%	63%
Workplace violence	40%	50%

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

83

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

▲ **13%** points above 2016
▼ **1%** point below global average

FRAUD

The construction, engineering, and infrastructure sector posted the greatest year-over-year increase in fraud incidents. More than four in five (83%) respondents reported some type of fraud this year, 13 percentage points higher than the 70% reported in 2016.

Information theft, loss, or attack was the most reported type of fraud (33%), with regulatory breaches and vendor/supplier fraud close behind at 30% each.

Junior employees are most commonly identified by respondents as the key perpetrators of fraud (47%). Most instances of fraud within the sector were revealed by an internal whistleblower (53%).

More than half of respondents (54%) report feeling highly or somewhat vulnerable to theft of intellectual property (e.g., trade secrets), piracy, and counterfeiting, 21 percentage points higher than two years ago. Nearly just as many respondents (52%) have concerns over management conflict of interest, 22 percentage points higher than two years ago, followed by regulatory or compliance breaches (50%).

Financial controls (including fraud detection and internal audits) were the most commonly implemented anti-fraud measures according to those surveyed (82%).

MOST COMMON TYPES OF FRAUD		Global Avg.
Information theft, loss or attack *(e.g., data theft)*	33%	29%
Regulatory or compliance breach	30%	20%
Vendor, supplier, or procurement fraud	30%	20%
Theft of physical assets or stock	28%	27%
Management conflict of interest	28%	26%
Corruption or bribery	28%	21%

MOST COMMON PERPETRATORS		Global Avg.
Junior employees	47%	39%
Vendors/suppliers *(i.e., a provider of technology or services to your company)*	38%	30%
Senior or middle management employees	38%	27%
Freelance/temporary employees	36%	26%
Joint venture partners *(i.e., a partner who provides manufacturing or other business function, or a franchisee)*	29%	23%

RESPONDENTS ARE MOST OR SOMEWHAT LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING FRAUD RISKS	Global Avg.
IP theft *(e.g., of trade secrets)*, piracy, or counterfeiting	54%	56%
Management conflict of interest	52%	52%
Regulatory or compliance breach	50%	49%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	82%	77%
Staff *(background screening)*	76%	73%
Management *(management controls, incentives, external supervision such as audit committee)*	74%	74%
Partners, clients, and vendors *(due diligence)*	73%	73%
Risk *(risk officer and risk management system)*	73%	75%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
By a whistleblower at our company	53%	47%

93

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

▲ **16%** points above 2016
▲ **7%** points above global average

CYBER SECURITY

The construction, engineering, and infrastructure sector experienced more cyber incidents than any other sector in this year's report, with 93% of respondents reporting their company had been attacked in the last 12 months. This sector also posted the greatest year-over-year increase, 16 percentage points higher than 2016.

The most common type of cyber attack was a virus/worm attack (39%), followed by email-based phishing attacks (37%), wire transfer fraud (31%), and data breaches (31%). Customer records were targeted in 52% of these instances.

Respondents most commonly reported that random cyber criminals are to blame (38%) for incidents. This sector's respondents say they feel highly or somewhat vulnerable to virus/worm attacks (65%) and data breaches (55%).

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Virus/worm attack	39%	36%
Email-based phishing attack	37%	33%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	31%	27%
Wire transfer fraud *(email account takeover/impersonation)*	31%	19%

MOST COMMON PERPETRATORS		Global Avg.
Random cyber criminal	38%	34%
Competitors	30%	23%

RESPONDENTS ARE MOST OR SOMEWHAT LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING CYBER RISKS	Global Avg.
Virus/worm attack	65%	62%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	55%	55%
Data deletion	52%	58%
Stolen equipment with sensitive data	52%	55%

MOST COMMON TARGET		Global Avg.
Customer records	52%	48%
Company/employee identity	46%	35%
Physical assets/money	46%	34%
Employee records	46%	41%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	36%	35%
Incident response firm *(investigations, breach notification)*	16%	11%

67

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

▲ **4%** points above 2016
▼ **3%** point below global average

SECURITY

Over two-thirds (67%) of respondents within the sector said their organization had experienced a security incident. The most common type of security incident was physical theft or loss of intellectual property, reported by 43%, followed by environmental incidents such as natural disasters (30%).

Senior and middle management, ex-employees, and random perpetrators were identified equally by respondents (36%) as being most often responsible for security incidents.

Nearly six in 10 respondents (57%) in the sector believe their company is highly or somewhat vulnerable to physical theft or loss of intellectual property, followed by geopolitical and environmental risks (55% and 52%, respectively). Concerns over geopolitical risks are more than double over last year, when the number was only 25%.

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	43%	41%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	30%	28%
Geographic and political risk *(i.e., operating in areas of conflict)*	28%	20%

MOST COMMON PERPETRATORS		Global Avg.
Senior management or middle management employees of our own company	36%	25%
Ex-employees	36%	37%
Random perpetrator	36%	30%

RESPONDENTS ARE MOST OR SOMEWHAT LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Global Avg.
Physical theft or loss of intellectual property	57%	63%
Geographic and political risk *(i.e., operating in areas of conflict)*	55%	53%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	52%	56%

Consumer Goods

75

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

- ▼ **7%** points below 2016
- ▼ **9%** points below global average

FRAUD

Respondents within the consumer goods sector were less likely to say their company had experienced fraud in the last 12 months (75%), which is 9 percentage points lower than the global average (84%). This was also a decrease of 7 percentage points on the previous year's survey.

The most common type of fraud experienced in the sector was theft of physical assets or stock (23%), followed closely behind by information theft, loss, or attack (21%) and vendor/supplier fraud (21%).

Four in 10 (41%) respondents attributed their fraud incidents to junior employees, while 36% named ex-employees as the key perpetrators of fraud. The most common method of discovering fraud incidents was through an internal audit (54%).

Respondents in this sector feel most highly or somewhat vulnerable to theft of physical assets or stock (48%), vendor, supplier, or procurement fraud (48%), and information theft, loss, or attack (46%).

The most commonly implemented anti-fraud measures as reported by respondents within the sector are IT security and technical countermeasures (72%), staff training that includes a whistleblower hotline (69%), and intellectual property risk assessments and trademark monitoring programs (69%).

MOST COMMON TYPES OF FRAUD		Global Avg.
Theft of physical assets or stock	23%	27%
Information theft, loss, or attack *(e.g., data theft)*	21%	29%
Vendor, supplier, or procurement fraud	21%	20%
Corruption and bribery	19%	21%
Management conflict of interest	15%	26%

MOST COMMON PERPETRATORS		Global Avg.
Junior employees	41%	39%
Ex-employees	36%	34%
Vendors/suppliers	26%	30%
Freelance/temporary employees	26%	26%
Senior or middle management employees	18%	27%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
Theft of physical assets or stock	48%	55%
Vendor, supplier, or procurement fraud	48%	51%
Information theft, loss, or attack *(e.g., data theft)*	46%	57%
IP theft *(e.g., of trade secrets)*, piracy, or counterfeiting	42%	56%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Information *(IT security, technical countermeasures)*	72%	78%
Staff *(training, whistleblower hotline)*	69%	74%
IP *(intellectual property risk assessment and trademark monitoring program)*	69%	73%
Staff *(background screening)*	67%	73%
Partners, clients, and vendors *(due diligence)*	66%	73%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
Through an internal audit	54%	44%

79

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **4%** points below 2016
- ▼ **7%** points below global average

CYBER SECURITY

The majority (79%) of respondents in the consumer goods sector said that their company had been the victim of a cyber incident in the last year, compared with 83% in the previous year. Most of these incidents were virus/worm attacks (29%) and email-based phishing attacks (23%).

Most respondents attributed cyber incidents to ex-employees (27%). Respondents also said most cyber incidents targeted customer records (41%) or physical assets and money (37%).

Reflecting their actual experience, respondents are most likely to feel highly or somewhat vulnerable to virus/worm attacks (59%). More than half of respondents also report feeling highly or somewhat vulnerable to data breaches (55%) and ransomware attacks (52%). Concerns over ransomware attacks are 19 percentage points higher than last year, when 33% of respondents felt highly or somewhat vulnerable to this threat.

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Virus/worm attack	29%	36%
Email-based phishing attack	23%	33%
Alteration or change of data	19%	22%
Lost equipment with sensitive data	19%	19%
Data deletion	19%	25%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	27%	28%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Virus/worm attack	59%	62%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	55%	55%

MOST COMMON TARGET		Global Avg.
Customer records	41%	48%
Physical assets/money	37%	34%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	34%	35%
Webhosting/website provider	10%	8%
Insurance portal	10%	5%

67

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **8%** points below 2016
- ▼ **3%** point below global average

SECURITY

There has been an increase of 2 percentage points in security incidents in the consumer goods industry since last year's report according to those surveyed (experienced by 67% of respondents compared to 65% in 2016). Physical theft or loss of intellectual property is the most common type of security incident experienced (40%), followed by workplace violence (27%) and environmental risks (25%).

Respondents in the sector identified the key perpetrators of security incidents as ex-employees (49%), and are most likely to report feeling highly or somewhat vulnerable to physical theft or loss of intellectual property (57%). The greatest year-over-year increase in feelings of vulnerability relates to workplace violence, which at 52% is 15 percentage points higher than last year's figure of 37%.

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	40%	41%
Workplace violence	27%	23%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	25%	28%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	49%	37%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Physical theft or loss of intellectual property	57%	63%
Workplace violence	52%	50%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	47%	56%

Financial Services

91

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

▲ **2%** points above 2016
▲ **7%** points above global average

FRAUD

More than nine in 10 (91%) respondents in the financial services sector reported incidents of fraud this year, the highest percentage reported by any sector in this year's report. This is 2 percentage point higher than last year's number (89%) and significantly higher than this year's global average (84%).

Respondents in the financial services sector said that management conflict of interest (27%) and information theft, loss, or attack (27%) were the main types of fraud experienced. Ex-employees (39%) were cited as the main perpetrators of fraud, followed by junior employees (33%) and vendors/suppliers (33%). Over half of these instances of fraud were detected through an internal audit (53%).

This year's respondents are feeling significantly more vulnerable to a number of risks as compared to two years ago. Respondents are most likely to report feeling highly or somewhat vulnerable to internal financial fraud (64%) and IP theft (62%), which stand 25 percentage points and 29 percentage points higher, respectively, than when last reported. Feelings of vulnerability over the theft of physical assets or stock are similarly high at 61%. Two areas of risk that did not rise to the level of top concerns this year – market collusion and misappropriation of company funds – nevertheless posted some of the highest increases at 24 percentage points and 25 percentage points, respectively, as compared to two years ago.

When asked what anti-fraud measures have been implemented, 84% of respondents mentioned IT security and technical countermeasures, and the same percentage reported staff training that includes a whistleblower hotline. These percentages are significantly higher than the global averages of 78% and 74%, respectively.

MOST COMMON TYPES OF FRAUD		*Global Avg.*
Information theft, loss, or attack (e.g., data theft)	27%	29%
Management conflict of interest	27%	26%
Corruption and bribery	23%	21%
Regulatory or compliance breach	21%	20%
Vendor, supplier, or procurement fraud	21%	20%
Market collusion (e.g., price fixing)	21%	19%
Money laundering	21%	16%

MOST COMMON PERPETRATORS		*Global Avg.*
Ex-employees	39%	34%
Junior employees	33%	39%
Vendors/suppliers *(i.e., a provider of technology or services to your company)*	33%	30%
Senior or middle management employees	24%	27%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		*Global Avg.*
Internal financial fraud *(manipulation of company results)*	64%	52%
IP theft *(e.g., of trade secrets)*, piracy, or counterfeiting	62%	56%
Theft of physical assets or stock	61%	55%
Management conflict of interest	59%	52%

MOST COMMON ANTI-FRAUD MEASURES		*Global Avg.*
Information *(IT security, technical countermeasures)*	84%	78%
Staff *(training, whistleblower hotline)*	84%	74%
Partners, clients, and vendors *(due diligence)*	80%	73%
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	80%	77%
Assets *(physical security systems, stock inventories, tagging, asset register)*	80%	77%

MOST COMMON MEANS OF DISCOVERY		*Global Avg.*
Through an internal audit	53%	44%

89

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

= same as 2016
▲ **3%** points above global average

CYBER SECURITY

Respondents in the financial services sector reported above-average numbers of cyber incidents this year, with 89% experiencing a cyber attack versus a global average of 86%. The most prevalent cyber incidents reported by financial services organizations were email-based phishing attacks (41%), which was the second-highest incidence among all sectors in this report.

Most respondents said the targets of cyber incidents were customer records (44%), trade secrets/R&D/IP (38%), and physical assets and money (38%). When asked to identify the perpetrators of these attacks, 38% of respondents named random cyber criminals.

In the context of cyber risks, nearly seven out of 10 respondents report feeling highly or somewhat vulnerable to data deletion (67%), which is 19 percentage points higher than last year. Nearly as many have concerns over potential virus/worm attacks (62%), stolen equipment with sensitive data (61%), and denial of service attacks (61%), with DOS attacks 22 percentage points higher than last year. It is worth taking note that although almost half of respondents reported experiencing an email-based phishing attack, only 23% say they feel highly vulnerable to this threat.

MOST COMMON TYPES OF CYBER INCIDENT		*Global Avg.*
Email-based phishing attack	41%	33%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	34%	27%

MOST COMMON TARGET		*Global Avg.*
Customer records	44%	48%
Trade secrets/R&D/IP	38%	40%
Physical assets/money	38%	34%

MOST COMMON PERPETRATORS		*Global Avg.*
Random cyber criminals	38%	34%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		*Global Avg.*
Data deletion	67%	58%
Virus/worm attack	62%	62%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		*Global Avg.*
IT service vendor	36%	35%
ISP/Telecom provider	12%	7%

66

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

▲ **9%** points above 2016
▼ **4%** points below global average

SECURITY

Security incidents reported by financial services respondents increased by 9 percentage points in 2017, with two-thirds (66%) having been a victim of a security incident compared to just 57% in 2016. This is, however, still lower than the global average of 71%.

Two-fifths (41%) of respondents in the financial services sector reported security incidents related to physical theft or loss of intellectual property, and 29% experienced an environmental event. The most common perpetrators according to those who took the survey were ex-employees (49%).

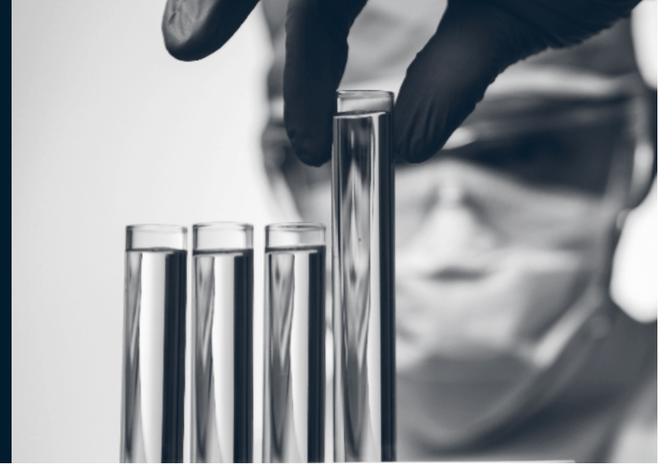
When respondents were asked to consider the security risks to which they feel highly or somewhat vulnerable, 65% identified physical theft or loss or property, 62% reported environmental risk, and nearly as many (61%) pointed to geopolitical risks. Concerns over environmental and geopolitical risks spiked 22 percentage points and 17 percentage points, respectively, over last year.

MOST COMMON TYPES OF SECURITY INCIDENT		*Global Avg.*
Physical theft or loss of intellectual property	41%	41%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	29%	28%
Geographic and political risk *(i.e., operating in areas of conflict)*	18%	20%

MOST COMMON PERPETRATORS		*Global Avg.*
Ex-employees	49%	37%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		*Global Avg.*
Physical theft or loss of intellectual property	65%	63%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	62%	56%
Geographic and political risk *(i.e., operating in areas of conflict)*	61%	53%

Healthcare, Pharmaceuticals, and Biotechnology



75

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

- ▼ **5%** points below 2016
- ▼ **9%** points below global average

FRAUD

Three-quarters (75%) of respondents in the healthcare, pharmaceuticals, and biotechnology sector in this year's survey reported experiencing an incident of fraud. This is the lowest incidence reported by any sector in this year's report, 9 percentage points lower than the global average.

Respondents experienced several types of fraud, reporting in equal numbers (29%) theft of physical assets; IP theft; and misappropriation of company funds.

Junior employees were most often identified as the perpetrators of fraud (cited by 56% of respondents); this was the highest reported incidence of junior employee fraud among any sector in this report, and 17 percentage points higher than the global average.

Respondents from this sector reported that when they do suffer from a fraud incident, it is more likely to be identified by management (49%).

Feelings of vulnerability to a host of risks are running extremely high in this sector. Almost three-quarters (73%) of respondents this year say they feel highly or somewhat vulnerable to IP theft, piracy, or counterfeiting, which represents a remarkable 41-percentage-point increase from just two years ago. Nearly just as many report feeling vulnerable to corruption and bribery (71%, an increase of 39 percentage points), internal financial fraud (70%, an increase of 34 percentage points), and information theft (70%, an increase of 25 percentage points). Concerns over market collusion spiked the highest, more than quadrupling from just 14% two years ago to a stunning 62% this year.

The most commonly implemented anti-fraud measure, as identified by respondents in the sector, is background screening of staff (85%), followed by IT security and technical countermeasures (80%).

MOST COMMON TYPES OF FRAUD		Global Avg.
Theft of physical assets or stock	29%	27%
IP theft *(e.g. of trade secrets)***, piracy, or counterfeiting**	29%	20%
Misappropriation of company funds	29%	20%
Management conflict of interest	27%	26%
Information theft, loss, or attack *(e.g., data theft)*	23%	29%
Internal financial fraud *(manipulation of company results)*	23%	23%

MOST COMMON PERPETRATORS		Global Avg.
Junior employees	56%	39%
Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	41%	24%
Ex-employees	38%	34%
Regulators	38%	15%
Joint venture partners *(i.e., a partner who provides manufacturing or other business function, or a franchisee)*	36%	23%
Senior or middle management employees	36%	27%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
IP theft *(e.g., of trade secrets)***, piracy, or counterfeiting**	73%	56%
Corruption and bribery	71%	50%
Internal financial fraud *(manipulation of company results)*	70%	52%
Information theft, loss, or attack *(e.g., data theft)*	70%	57%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Staff *(background screening)*	85%	73%
Information *(IT security, technical countermeasures)*	80%	78%
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	79%	77%
Reputation *(media monitoring, compliance controls, legal review)*	79%	72%
Assets *(physical security systems, stock inventories, tagging, asset register)*	77%	77%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
By management at our company	49%	35%

77

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **9%** points below 2016
- ▼ **9%** points below global average

CYBER SECURITY

More than three-quarters (77%) of executives surveyed from this sector reported cyber incidents. This is a 9-percentage-point decrease from not only last year's figure (86%), but also this year's global average (86%).

The most common type of incidents reported by respondents were virus/worm attacks (38%). This was followed by lost equipment with sensitive data (33%), which was the highest incidence reported by any sector in this report and well above the global average of 19%. The most often named perpetrators were competitors (43%).

82% respondents in this sector reported feeling highly or somewhat vulnerable to data deletion, 23 percentage points higher than last year. Other areas that sparked high levels of vulnerability included virus/worm attacks (78%, an increase of 27 percentage points); stolen equipment with sensitive data (73%); denial of service attacks (73%, an increase of 26 percentage points); and email-based phishing attacks (73%, an increase of 20 percentage points).

Customer records and employee records were named as primary target of cyber attacks (63% and 58%, respectively). Given the nature of the sector, it was unsurprising to see that over half (55%) of respondents reported trade secrets/R&D/IP being targeted in the cyber incidents they faced.

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Virus/worm attack	38%	36%
Lost equipment with sensitive data	33%	19%
Email-based phishing attack	31%	33%

MOST COMMON TARGET		Global Avg.
Customer records	62%	48%
Employee records	57%	41%
Trade secrets/R&D/IP	55%	40%

MOST COMMON PERPETRATORS		Global Avg.
Competitors	42%	23%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Data deletion	82%	58%
Virus/worm attack	78%	62%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	45%	35%
Incident response firm *(investigations, breach notification)*	15%	11%

67

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

- ▲ **2%** points above 2016
- ▼ **3%** points below global average

SECURITY

Two-thirds (67%) of respondents from the healthcare, pharmaceuticals, and biotechnology sector reported a security incident in the previous 12 months. Unlike the decreases for the sector in fraud and cyber security, this represented a slight increase over last year's figure of 65%.

Respondents were most likely to have experienced physical theft or loss of intellectual property (40%), workplace violence (35%), and environmental risk (35%). Reflecting their actual experience, they report feeling highly or somewhat vulnerable to physical thefts (79%) and environmental risks (66%). The most common perpetrators named by respondents in the sector were ex-employees.

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	40%	41%
Workplace violence	35%	23%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	35%	28%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	54%	37%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Physical theft or loss of intellectual property	79%	63%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	66%	56%
Geographic and political risk *(i.e., operating in areas of conflict)*	60%	53%

Manufacturing

86

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

▼ **3%** points below 2016
▲ **2%** points above global average

FRAUD

Although respondents in the manufacturing sector reported above-average levels of fraud this year (86% versus global average of 84%), this was 3 percentage points lower than last year.

The most common type of fraud experienced by respondents in the sector was information theft, loss, or attack, reported by a third (33%), followed by corruption and bribery (28%), management conflict of interest (26%), and internal financial fraud (26%).

Respondents were most likely to report junior employees as the perpetrators of fraud incidents (42%), followed by ex-employees (34%). Most fraud instances were identified by a whistleblower within the company (46%).

In terms of current vulnerabilities, respondents are most likely to feel highly or somewhat vulnerable to information theft, loss, or attack (62%), internal financial fraud (57%), and vendor, supplier, or procurement fraud (56%). More than four in five respondents (84%) said their company has financial controls (including fraud detection and internal audits) in place to prevent fraud. The same percentage reported the implementation of asset controls, such as physical security systems, stock inventories, tagging, and asset registers.

MOST COMMON TYPES OF FRAUD		Global Avg.
Information theft, loss, or attack *(e.g., data theft)*	33%	29%
Corruption and bribery	28%	21%
Management conflict of interest	26%	26%
Internal financial fraud *(manipulation of company results)*	26%	23%

MOST COMMON PERPETRATORS		Global Avg.
Junior employees	42%	39%
Ex-employees	34%	34%
Vendors/suppliers *(i.e., a provider of technology or services to your company)*	30%	30%
Freelance/temporary employees	26%	26%
Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	22%	24%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
Information theft, loss, or attack *(e.g., data theft)*	62%	57%
Internal financial fraud *(manipulation of company results)*	57%	52%
Vendor, supplier, or procurement fraud	56%	51%
IP theft *(e.g., of trade secrets)***, piracy, or counterfeiting**	52%	56%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	84%	77%
Assets *(physical security systems, stock inventories, tagging, asset register)*	84%	77%
Information *(IT security, technical countermeasures)*	80%	78%
Management *(management controls, incentives, external supervision such as audit committee)*	80%	74%
Staff *(training, whistleblower hotline)*	80%	74%
Risk *(risk officer and risk management system)*	80%	75%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
By a whistleblower at our company	46%	47%

88

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

▼ **3%** points below 2016
▲ **2%** points above global average

CYBER SECURITY

While manufacturing sector respondents reported a higher than average number of cyber incidents (88%), this is a slight improvement of 3 percentage points from last year (91%). The most common cyber incidents experienced by manufacturing respondents were virus/worm attacks (38%), followed by email-based phishing attacks and data breaches (26% each).

Almost half (49%) of respondents who had experienced a cyber attack said the target was most often customer records, followed by trade secrets (45%) and employee records (35%).

More than half (57%) felt their company is highly or somewhat vulnerable to data deletion, while nearly as many said that email-based phishing attacks (55%) and virus/worm attacks (55%) are key vulnerabilities. Wire transfer fraud sparked the greatest increase in feelings of vulnerability, up 19 percentage points from last year.

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Virus/worm attack	38%	36%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	26%	27%
Email-based phishing attack	26%	33%
Data deletion	22%	25%

MOST COMMON TARGET		Global Avg.
Customer records	49%	48%
Trade secrets/R&D/IP	45%	40%
Employee records	35%	41%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Data deletion	57%	58%
Email-based phishing attack	55%	57%
Virus/worm attack	55%	62%

MOST COMMON PERPETRATORS		Global Avg.
Random cyber criminal	41%	34%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	25%	35%
Incident response firm *(investigations, breach notification)*	18%	11%

72

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

▼ **9%** points below 2016
▲ **2%** points above global average

SECURITY

Security incidents reported by manufacturing sector respondents fell significantly from last year's total of 81% to 72% this year. Although this is still higher than the global average of 70%, it is the largest year-over-year decrease among all sectors.

Physical theft or loss of intellectual property was the most common type of security incident according to respondents (45%). The second most frequently occurring security incident was environmental risk (24%). According to respondents, attacks were most commonly committed by random perpetrators (31%).

Respondents reported feeling most highly or somewhat vulnerable to physical theft or loss of IP (53%). Concerns over terrorism (47%) rose the most, increasing 21 percentage points since last year.

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	45%	41%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	24%	28%
Workplace violence	19%	23%
Geographic and political risk *(i.e., operating in areas of conflict)*	19%	20%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Physical theft or loss of intellectual property	53%	63%
Terrorism, including domestic and international events	47%	49%
Geographic and political risk *(i.e., operating in areas of conflict)*	45%	53%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	45%	56%

MOST COMMON PERPETRATORS		Global Avg.
Random perpetrator	31%	30%

Natural Resources

85

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

- ▲ **5%** points above 2016
- ▲ **1%** points above global average

FRAUD

85% of respondents in the natural resources sector reported a fraud incident last year, slightly above the global average of 84% and an increase of five percentage points over last year.

When asked which types of fraud they had faced, respondents in this sector most often reported management conflict of interest (35%) and market collusion (29%). One in four (27%) said they had suffered from IP theft over the past 12 months. All of these were well above the global averages of 26%, 19%, and 20%, respectively.

Junior employees were reported as the main perpetrators of fraud in this sector (45%), followed by former employees (41%) and senior or middle management (34%). Inside information is key to the discovery of fraud in the sector, with 70% of fraud incidents discovered by a whistleblower. In fact, at 23 percentage points higher than the global average, this was the highest reported incidence of whistleblowing as a means of discovery among all sectors.

Respondents in the natural resources sector are most likely to feel highly or somewhat vulnerable to management conflict of interest (68%), which is 21 percentage points higher than two years ago. These respondents also feel significantly vulnerable to information theft, loss, or attack (65%) and misappropriation of company funds (61%).

To decrease the risk of fraud incidents, four in five (80%) respondents report their companies have intellectual property risk assessments and three-quarters (75%) say financial controls that include fraud detection have been implemented.

MOST COMMON TYPES OF FRAUD		Global Avg.
Management conflict of interest	35%	26%
Market collusion *(e.g., price fixing)*	29%	19%
IP theft *(e.g., of trade secrets)*, piracy, or counterfeiting	27%	20%
Theft of physical assets or stock	25%	27%
Money laundering	23%	16%

MOST COMMON PERPETRATORS		Global Avg.
Junior employees	45%	39%
Ex-employees	41%	34%
Senior or middle management employees	34%	27%
Vendors/suppliers *(i.e., a provider of technology or services to your company)*	32%	30%
Joint venture partners *(i.e., a partner who provides manufacturing or other business function, or a franchisee)*	32%	23%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
Management conflict of interest	68%	52%
Information theft, loss, or attack *(e.g., data theft)*	65%	57%
Misappropriation of company funds	61%	48%
Theft of physical assets or stock	60%	55%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
IP *(intellectual property risk assessment and trademark monitoring program)*	80%	73%
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	75%	77%
Management *(management controls, incentives, external supervision such as audit committee)*	73%	74%
Partners, clients, and vendors *(due diligence)*	73%	73%
Reputation *(media monitoring, compliance controls, legal review)*	68%	72%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
By a whistleblower at our company	70%	47%

87

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▲ **1%** point above 2016
- ▲ **1%** point above global average

CYBER SECURITY

The majority (87%) of respondents in this sector said their organization had experienced a cyber incident over the previous year, with email-based phishing attacks being the most common type (38%). Other common incidents include virus/worm infestations (37%) and alteration or change of data (31%).

According to respondents, ex-employees were most often the perpetrators of cyber attacks (33%), followed by freelance or temporary employees (29%) and competitors (27%).

Respondents in this sector say the most common target of cyber incidents are trade secrets/R&D/IP (47%), employee records (42%), and company or employee identity (42%).

Generally in line with their actual experience, respondents in the sector feel most vulnerable to email-based phishing attacks (69%), which is 21 percentage points higher than last year. These respondents also feel highly or somewhat vulnerable to virus/worm attacks (64%) and wire transfer fraud (59%).

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Email-based phishing attack	38%	33%
Virus/worm attack	37%	36%
Alteration or change of data	31%	22%

MOST COMMON TARGET		Global Avg.
Trade secrets/R&D/IP	47%	40%
Employee records	42%	41%
Company/employee identity	42%	35%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	33%	28%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Email-based phishing attack	69%	57%
Virus/worm attack	64%	62%
Wire transfer fraud *(email account takeover/impersonation)*	59%	50%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	24%	35%
Insurance broker	11%	4%
State law enforcement	11%	6%

81

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

- ▲ **11%** points above 2016
- ▲ **11%** points above global average

SECURITY

Respondents from the natural resources sector saw a big increase in the prevalence of security incidents, with 81% affected by at least one in the past year, up 11 percentage points on 2016, and 11 percentage points above the global average.

Physical theft or loss of intellectual property was the most common incident (44%), followed by environmental incidents (42%). Two in five respondents (40%) named senior or middle management as the key perpetrators of security incidents.

Almost three in four respondents felt most highly or somewhat vulnerable to environmental risk (71%), which would seem to be out of proportion to actual experience for this risk. Similarly, 64% of respondents reported feeling vulnerable to workplace violence even though this did not make the top three categories of incidents actually experienced.

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	44%	41%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	42%	28%
Geographic and political risk *(i.e., operating in areas of conflict)*	27%	20%

MOST COMMON PERPETRATORS		Global Avg.
Senior or middle management employees	40%	25%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	71%	56%
Workplace violence	64%	50%
Physical theft or loss of intellectual property	58%	63%

Professional Services

89

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

- ▲ **5%** points above 2016
- ▲ **5%** points above global average

FRAUD

The number of respondents in the professional services sector who reported fraud incidents increased 5 percentage points over last year, from 84% in 2016 to 89% this year. Information theft, loss, or attack (33%) and internal financial fraud (29%) were the main types of fraud reported by survey respondents.

The most common perpetrators of fraud were junior employees (37%), followed by senior or middle management (31%) and ex-employees (31%), according to respondents. These instances of fraud were discovered equally (43%) through whistleblowing or by management at the company.

IT security and technical countermeasures are implemented at most professional services companies as reported by 88% of respondents. Other commonly reported anti-fraud measures include risk officers and risk management systems (82%). These are both higher than the global averages of 77% and 75%, respectively.

Respondents in this sector are most likely to feel highly or somewhat vulnerable to theft of physical assets or stock (56%), IP theft (56%), and information theft or loss (51%).

MOST COMMON TYPES OF FRAUD		Global Avg.
Information theft, loss, or attack *(e.g., data theft)*	33%	29%
Internal financial fraud *(manipulation of company results)*	29%	23%
Vendor, supplier, or procurement fraud	27%	20%
Corruption and bribery	27%	21%
Theft of physical assets or stock	25%	27%
Management conflict of interest	25%	26%

MOST COMMON PERPETRATORS		Global Avg.
Junior employees	37%	39%
Senior or middle management employees	31%	27%
Ex-employees	31%	34%
Vendors/suppliers *(i.e., a provider of technology or services to your company)*	29%	30%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Information *(IT security, technical countermeasures)*	88%	77%
Risk *(risk officer and risk management system)*	82%	75%
Assets *(physical security systems, stock inventories, tagging, asset register)*	80%	77%
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	79%	77%
Staff *(training, whistleblower hotline)*	78%	74%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
Theft of physical assets or stock	56%	55%
IP theft *(e.g., of trade secrets)*, piracy, or counterfeiting	56%	56%
Information theft, loss, or attack (e.g., data theft)	51%	57%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
By a whistleblower at our company	43%	47%
By management at our company	43%	35%

87

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▲ **3%** points above 2016
- ▲ **1%** point above global average

CYBER SECURITY

Cyber incidents are also on the rise in the professional services sector, according to respondents: 87% experienced an attack this year versus 84% last year. The most cited types of cyber incidents experienced were virus/worm attacks (38%), followed by deletion of data (29%).

Around half of respondents who faced a cyber incident in the professional services sector reported employee records (52%) and customer records (46%) as the main targets for cyber attacks. The key perpetrators of these attacks were cited as ex-employees (33%) and senior or middle management (25%).

When asked to consider what cyber risks they feel highly or somewhat vulnerable to, respondents most frequently mentioned stolen equipment with sensitive data (67%), an increase of 16 percentage points from last year. Respondents also had concerns over denial of service attacks (64%) and data deletion (63%).

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Virus/worm attack	38%	36%
Data deletion	29%	25%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	27%	27%

MOST COMMON TARGET		Global Avg.
Employee records	52%	41%
Customer records	46%	48%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Stolen equipment with sensitive data	67%	55%
Denial of service attack	64%	52%
Data deletion	63%	58%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	33%	28%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	40%	35%
Webhosting/website provider	10%	8%
Incident response firm *(investigations, breach notification)*	10%	11%

65

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

- ▲ **2%** points above 2016
- ▼ **5%** point below global average

SECURITY

More than two-thirds (65%) of those surveyed from the professional services sector had experienced a security incident in the last 12 months. This is an increase from 63% in 2016, but still lower than the global average of 70%. The main types of security incidents reported were physical theft or loss of intellectual property (38%) and environmental risks (29%).

Over a third of respondents identified ex-employees as the perpetrators of security incidents (36%). In line with their actual experience, respondents reported feeling most highly or somewhat vulnerable to physical theft or loss of IP (67%). They also felt equally vulnerable to geographic and political risks (55%) and environmental risks (56%).

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	38%	41%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	29%	28%
Workplace violence	24%	23%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	36%	37%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Physical theft or loss of intellectual property	67%	20%
Geographic and political risk *(i.e., operating in areas of conflict)*	57%	25%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	56%	21%

Retail, Wholesale, and Distribution

89

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

- ▲ **6%** points above 2016
- ▲ **5%** points above global average

FRAUD

89% of respondents from the retail, wholesale, and distribution sector experienced a fraud incident in the previous 12 months, 5 percentage points higher than the global average and an increase of 6 percentage points over last year.

Respondents in the sector also reported higher than average levels of information theft (39%). This was followed by theft of physical assets (33%), management conflict of interest (32%), and internal financial fraud (28%). Misappropriation of funds, last year's most prevalent type of fraud in the sector, continues to be an issue but was only the fifth most common type of fraud reported by respondents this year alongside bribery and corruption (also 23%).

Customers were reported as the joint most likely perpetrators of fraud in this sector (31%), which may account for the high levels of physical theft experienced. Joint venture partners and franchisees and vendors/suppliers were both reported to be perpetrators by 31% of respondents.

Almost three in four respondents (74%) in this sector were most likely to feel highly or moderately vulnerable to information theft, a significant increase of 30 percentage points from two years ago. Similar increases in feelings of vulnerability were reported for market collusion, which at 63% was more than triple what it was two years ago; IP theft (more than double at 67%); and regulatory and compliance breaches (almost double at 62%).

Given the high incidence of theft of physical assets reported by respondents in the sector, it is not surprising that 86% said that they had initiated anti-fraud measures relating to assets, including physical security systems and stock inventories. This figure was significantly higher than the global average of 77%.

External audits uncovered the most fraud in this sector (41%); however, other channels including whistleblowing, internal audits, and discovery by management (all 39%) were also likely to be reported as the source of discovery.

MOST COMMON TYPES OF FRAUD		Global Avg.
Information theft, loss, or attack *(e.g., data theft)*	39%	29%
Theft of physical assets or stock	33%	27%
Management conflict of interest	32%	26%
Internal financial fraud *(manipulation of company results)*	28%	23%

MOST COMMON PERPETRATORS		Global Avg.
Customers	31%	22%
Joint venture partners *(i.e., a partner who provides manufacturing or other business function, or a franchisee)*	31%	23%
Vendors/suppliers *(i.e., a provider of technology or services to your company)*	31%	30%
Senior or middle management employees	29%	27%
Ex-employees	29%	34%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		Global Avg.
Information theft, loss, or attack *(e.g., data theft)*	74%	57%
Theft of physical assets or stock	68%	55%
IP theft *(e.g., of trade secrets)***, piracy, or counterfeiting**	67%	56%

MOST COMMON ANTI-FRAUD MEASURES		Global Avg.
Assets *(physical security systems, stock inventories, tagging, asset register)*	86%	77%
Management *(management controls, incentives, external supervision such as audit committee)*	84%	74%
Staff *(background screening)*	80%	73%
Information *(IT security, technical countermeasures)*	78%	73%
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	78%	77%
IP *(intellectual property risk assessment and trademark monitoring program)*	78%	78%

MOST COMMON MEANS OF DISCOVERY		Global Avg.
Through an external audit	41%	35%

82

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **5%** points below 2016
- ▼ **4%** points below global average

CYBER SECURITY

The majority (82%) of respondents in the sector had experienced a cyber incident over the previous 12 months, a decrease of 5 percentage points from last year (87%). Email-based phishing attacks were the most common type of cyber incident reported, by 40% of respondents, a much higher incidence than the global average of 33%.

Despite measures taken to mitigate against cyber incidents, 72% of respondents from the sector reported that they still feel highly or somewhat vulnerable to virus/worm attacks, and 61% feel vulnerable to ransomware attacks.

Employee records were the most common target of cyber attacks faced by respondents in this sector (53%), followed by customer records (38%) and trade secrets (also 38%). Random cyber criminals were cited as the most likely perpetrators (34%), followed by competitors (28%), who would potentially stand the most to gain from customer records and trade secrets. In the event of a cyber incident, respondents in this sector were most likely among all those in this survey to contact an incident response firm for investigation and breach notification services; that was according to 19% of respondents versus a global average of 11%.

MOST COMMON TYPES OF CYBER INCIDENT		Global Avg.
Email-based phishing attack	40%	33%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	33%	27%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		Global Avg.
Virus/worm attack	72%	62%
Ransomware attack	61%	55%
Data deletion	56%	58%
Lost equipment with sensitive data	56%	53%

MOST COMMON TARGET		Global Avg.
Employee records	53%	41%
Customer records	38%	48%
Trade secrets/R&D/IP	38%	40%

MOST COMMON PERPETRATORS		Global Avg.
Random cyber criminals	34%	34%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		Global Avg.
IT service vendor	43%	35%
Incident response firm *(investigations, breach notification)*	19%	11%

75

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **4%** points below 2016
- ▲ **5%** points above global average

SECURITY

Three-quarters (75%) of respondents in the retail, wholesale, and distribution sector said they had experienced a security incident in the past year, higher than the global average of 70%, but 4 percentage points lower than last year. They were most likely to report security incidents relating to physical theft or loss of intellectual property (42% of respondents), followed by environmental risk (26%) and geographic and political risk (21%).

Ex-employees were reported as the most likely perpetrators of security incidents in the sector (35%), followed by competitors (33%). Reflecting the type of incident most often experienced, respondents reported feeling most highly or somewhat vulnerable to physical theft or loss of intellectual property (65%).

MOST COMMON TYPES OF SECURITY INCIDENT		Global Avg.
Physical theft or loss of intellectual property	42%	41%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	26%	28%
Geographic and political risk *(i.e., operating in areas of conflict)*	21%	20%

MOST COMMON PERPETRATORS		Global Avg.
Ex-employees	35%	37%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		Global Avg.
Physical theft or loss of intellectual property	65%	63%
Geographic and political risk *(i.e., operating in areas of conflict)*	54%	53%
Terrorism, including domestic and international events	50%	49%

Technology, Media, and Telecoms

86

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

▲ **7%** points above 2016
▲ **2%** points above global average

FRAUD

86% of respondents in the technology, media, and telecoms sector experienced a fraud incident in the previous 12 months, slightly more than the global average (84%) and up 7 percentage points over last year's reported 79%.

Those surveyed for the report from this sector experienced higher than average levels of information theft, loss, or attack (35%) when compared with the global average (29%). The next most common fraud types reported by respondents in this sector were theft of physical assets or stock (31%) and regulatory or compliance breaches (29%).

Freelance/temporary employees were cited as joint most likely perpetrators (41%), much higher than the global average of 26%. Perpetrators cited by respondents were equally likely to be junior employees (also 41%), followed by ex-employees and vendors/suppliers (each at 30%).

Insiders are the main source for uncovering fraud in this sector, with whistleblowing the most prevalent way in which fraud was detected (59%).

Respondents in this sector are most likely to report that they feel highly or somewhat vulnerable to management conflict of interest (63%), more than double the number reported two years ago (31%). Similarly, the number of respondents with concerns over market collusion more than tripled from two years ago, 55% versus 17%.

The most common anti-fraud measure reported to be taken relates to assets, such as physical security systems, stock inventories, and tagging, according to 88% of respondents. Anti-fraud measures taken by respondents in this sector relating to information, such as IT security, were reported to be slightly lower (at 84%).

MOST COMMON TYPES OF FRAUD		*Global Avg.*
Information theft, loss, or attack *(e.g., data theft)*	35%	29%
Theft of physical assets or stock	31%	27%
Regulatory or compliance breach	29%	20%
IP theft *(e.g., of trade secrets)*, **piracy, or counterfeiting**	27%	20%
Management conflict of interest	27%	26%

MOST COMMON PERPETRATORS		*Global Avg.*
Freelance/temporary employees	41%	26%
Junior employees	41%	39%
Ex-employees	30%	34%
Vendors and suppliers *(i.e., a provider of technology or services to your company)*	30%	30%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING FRAUD RISKS		*Global Avg.*
Management conflict of interest	63%	52%
Information theft, loss, or attack *(e.g., data theft)*	62%	57%
IP theft *(e.g., of trade secrets), piracy, or counterfeiting*	59%	56%

MOST COMMON ANTI-FRAUD MEASURES		*Global Avg.*
Assets *(physical security systems, stock inventories, tagging, asset register)*	88%	77%
Information *(IT security, technical countermeasures)*	84%	78%
Risk *(risk officer and risk management system)*	82%	75%
IP *(intellectual property risk assessment and trademark monitoring program)*	82%	73%

MOST COMMON MEANS OF DISCOVERY		*Global Avg.*
By a whistleblower at our company	59%	47%

92

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

▲ **15%** points above 2016
▲ **6%** points above global average

CYBER SECURITY

The majority (92%) of respondents in this sector reported that they had experienced a cyber incident during the previous year, compared with a global average of 86%. This sector posted the second greatest year-over-year increase (15 percentage points) in cyber incidents after the construction, engineering, and infrastructure sector. Email-based phishing attacks were the most common type of cyber incident respondents experienced (43%), which was the highest reported for this type of cyber incident experienced among all sectors. This was followed by virus/worm infestations (41%). Both of these percentages were significantly higher than the global averages (33% and 36%, respectively).

Respondents in this sector also reported a relatively high incidence of ex-employees being responsible for cyber incidents. More than four in 10 (43%) said that ex-employees were the most common perpetrators, compared to a global average of 28%.

Executives in the technology, media, and telecoms sector surveyed for this year's report feel most vulnerable to email-based phishing attacks (67%). They also feel vulnerable to ransomware attacks (65%), which is an increase of 21 percentage points from last year.

Customer records (cited by 53% of respondents) were the most frequent target of cyber incidents in the technology, media, and telecoms sector.

MOST COMMON TYPES OF CYBER INCIDENT		*Global Avg.*
Email-based phishing attack	43%	33%
Virus/worm attack	41%	36%
Alteration or change of data	35%	22%

MOST COMMON PERPETRATORS		*Global Avg.*
Ex-employees	43%	28%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING CYBER RISKS		*Global Avg.*
Email-based phishing attack	67%	57%
Ransomware attack	65%	55%

MOST COMMON TARGET		*Global Avg.*
Customer records	53%	48%
Employee records	51%	41%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		*Global Avg.*
IT service vendor	38%	35%
ISP/Telecom provider	17%	7%

71

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

▼ **1%** point below 2016
▲ **1%** point above global average

SECURITY

Overall, 71% of respondents in this sector reported a security incident within their company. The most reported security incident in this sector was physical theft or loss of intellectual property (39%). However, respondents also reported a high incidence of workplace violence (35%), compared to the global average (23%).

Junior employees (42%) are the most likely perpetrators of security incidents in this sector according to those surveyed for the report. Respondents are most likely to say they feel highly or somewhat vulnerable to physical theft or loss of intellectual property (66%), 19 percentage points higher than last year) as well as workplace violence (64%).

MOST COMMON TYPES OF SECURITY INCIDENT		*Global Avg.*
Physical theft or loss of intellectual property	39%	41%
Workplace violence	35%	23%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	25%	28%

MOST COMMON PERPETRATORS		*Global Avg.*
Junior employees	42%	26%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY OR SOMEWHAT VULNERABLE TO THE FOLLOWING SECURITY RISKS		*Global Avg.*
Physical theft or loss of intellectual property	66%	47%
Workplace violence	64%	49%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	59%	51%

Transportation, Leisure, and Tourism

83

PERCENTAGE OF RESPONDENTS AFFECTED BY FRAUD IN THE PAST 12 MONTHS.

- ▼ **2%** points below 2016
- ▼ **1%** point below global average

FRAUD

The majority (83%) of respondents from the transportation, leisure, and tourism sector reported their business had experienced a fraud incident in the last year, a decrease of 2 percentage points from last year (85%).

Respondents from this sector said they experienced thefts of physical assets or stock (34%) and information theft, loss, or attack (34%), both of which are higher than the global averages of 27% and 29%, respectively. These were followed by internal financial fraud (23%). Ex-employees (36%), customers (27%), and senior or middle management (27%) were reported as the most likely perpetrators of fraud by respondents in this sector.

Those surveyed for the report from this sector reported that fraud is most often discovered internally, with whistleblowing and internal audits the most common ways in which incidents are discovered (each at 39%).

Respondents were most likely to say that they feel highly or somewhat vulnerable to theft of physical assets or stock (53%) and corruption and bribery (51%). Additionally, the number of those concerned over market collusion nearly tripled from the number reported two years ago, 51% versus 18%.

The most common anti-fraud measures put in place by organizations in this sector, as reported by respondents, were the introduction of measures relating to risk, such as a risk officer (82%); intellectual property (78%); reputation, such as media monitoring (78%); partner, client, and vendor due diligence(78%); and financial controls (78%).

MOST COMMON TYPES OF FRAUD		*Global Avg.*
Theft of physical assets or stock	34%	27%
Information theft, loss, or attack *(e.g., data theft)*	34%	29%
Internal financial fraud *(manipulation of company results)*	23%	23%
Management conflict of interest	19%	26%
Money laundering	19%	16%

RESPONDENTS ARE MOST OR SOMEWHAT LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING FRAUD RISKS		*Global Avg.*
Theft of physical assets or stock	53%	55%
Corruption and bribery	51%	50%
Market collusion *(e.g., price fixing)*	51%	50%
Management conflict of interest	49%	52%
Money laundering	49%	43%

MOST COMMON PERPETRATORS		*Global Avg.*
Ex-employees	36%	34%
Senior or middle management employees	27%	27%
Customers	27%	22%
Junior employees	20%	39%

MOST COMMON ANTI-FRAUD MEASURES		*Global Avg.*
Risk *(risk officer and risk management system)*	82%	75%
IP *(intellectual property risk assessment and trademark monitoring program)*	78%	73%
Reputation *(media monitoring, compliance controls, legal review)*	78%	72%
Partners, clients, and vendors *(due diligence)*	78%	73%
Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	78%	77%

MOST COMMON MEANS OF DISCOVERY		*Global Avg.*
By a whistleblower at our company	39%	47%
Through an internal audit	39%	44%

83

PERCENTAGE OF RESPONDENTS AFFECTED BY CYBER INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **4%** points below 2016
- ▼ **3%** points below global average

CYBER SECURITY

83% of respondents in the sector have experienced a cyber incident over the past year, which is slightly lower than the global average (86%) as well as the percentage reported in last year's report (87%).

Virus/worm infestations were named as the most common type of attack (43%). This was followed by email-based phishing attacks (28%) and data deletion (25%).

Customer records (55%) and company/employee identities (39%) were the two top targets for cyber incidents. Random cyber criminals (32%) and ex-employees (27%) were reported as the most likely perpetrators.

Respondents were most likely to feel highly or somewhat vulnerable to alteration of data (58%), followed closely by ransomware attacks and virus/worm attacks (each cited at 56%).

MOST COMMON TYPES OF CYBER INCIDENT		*Global Avg.*
Virus/worm attack	43%	36%
Email-based phishing attack	28%	33%
Data deletion	25%	25%

MOST COMMON TARGET		*Global Avg.*
Customer records	55%	48%
Company/employee identity	39%	35%

MOST COMMON PERPETRATORS		*Global Avg.*
Random cyber criminals	32%	34%

RESPONDENTS ARE MOST OR SOMEWHAT LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING CYBER RISKS		*Global Avg.*
Alteration or change of data	58%	56%
Ransomware attack	56%	55%
Virus/worm attack	56%	62%
Data breach *(e.g., resulting in loss of customer or employee data, IP/trade secrets/R&D)*	55%	55%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		*Global Avg.*
IT service vendor	34%	35%
Incident response firm *(investigations, breach notification)*	11%	11%
Webhosting/website provider	11%	8%

60

PERCENTAGE OF RESPONDENTS AFFECTED BY SECURITY INCIDENTS IN THE PAST 12 MONTHS.

- ▼ **10%** points below 2016
- ▼ **10%** points below global average

SECURITY

Only 60% of respondents in the transportation, leisure, and tourism sector experienced a security incident in the past year, well below the global average of 70% and the lowest rate reported among all sectors.

The most common security incident reported by respondents was physical theft or loss of intellectual property (40%). This continues to be a concern for the sector, as 63% of respondents feel highly or somewhat vulnerable to physical theft or loss of intellectual property.

MOST COMMON TYPES OF SECURITY INCIDENT		*Global Avg.*
Physical theft or loss of intellectual property	40%	41%
Workplace violence	17%	23%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.*	17%	28%

MOST COMMON PERPETRATORS		*Global Avg.*
Ex-employees	38%	37%
Random perpetrator	38%	30%

RESPONDENTS ARE MOST OR SOMEWHAT LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS		*Global Avg.*
Physical theft or loss of intellectual property	63%	63%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	60%	56%
Geographic and political risk *(i.e., operating in areas of conflict)*	51%	53%

Kroll Mission and Values

WHO WE ARE

Kroll is the leading global provider of risk and investigative services.

OUR MISSION

We help our clients anticipate, detect, mitigate, and respond to risk.

WHAT MAKES US DIFFERENT

More than forty-five years ago, Kroll pioneered the business investigations industry and, as times have changed, we have too. We are always evolving and tailoring our skills and offerings to meet the demands of the ever-changing risk and threat landscape.

- We are a global firm. Our experts possess a diverse range of industry and country experience in both mature and emerging markets. We draw on this diversity to bring together multi-disciplinary teams of experts, data, language, and technology – anywhere, anytime. We serve a global clientele of businesses, law firms, government agencies, non-profit institutions, and individuals.
- We are distinguished by our investigative approach – a relentless pursuit of facts, robust forensic expertise, insightful analysis, and resourcefulness built on our unique experience. This fundamental focus defines us and is in our DNA.
- We understand that surface-level information alone does not lead to informed and sound decisions. We leverage our expertise, global reach, and technology to provide our clients with an informational advantage. Deeper, more refined, and more contextual information results in better decision-making.
- **Our clients look to us to provide the knowledge and intelligence edge they need to make confident choices.**

OUR VALUES

- We work tirelessly to earn the trust and confidence of our clients
- We are responsive and take pride in understanding our clients' needs
- We look beyond the commonplace to find answers that others do not see
- We work together across the globe and embrace the entrepreneurial spirit of our people
- We make a difference

Contact Kroll

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

CORPORATE HEADQUARTERS

600 Third Avenue, New York, NY 10016

NORTH AMERICA

Boston
Daniel Linskey
T +1 617 210 7471
daniel.linskey@kroll.com

Chicago
Baltazar Vallenilla
T +1 312 345 2767
bvallenilla@kroll.com

Los Angeles
Jason Smolanoff
+1 213 700 4312
jason.smolanoff@kroll.com

Nashville
Marc Brawner
T +1 615 577 6765
mbrawner@kroll.com

New York
Dan Karson
T +1 212 833 3266
dkarson@kroll.com

Philadelphia
Mark Ehlers
T +1 215 568 8305
mehlers@kroll.com

Reston
Mari Davies-DeMarco
T +1 571 521 6160
mdavies@kroll.com

San Francisco
Betsy Blumenthal
T +1 415 743 4825
bblument@kroll.com

Toronto
Peter McFarlane
T +1 416 813 4401
pmcfarlane@kroll.com

Washington, D.C.
David Fontaine
T +1 202 833 6866
david.fontaine@kroll.com

LATIN AMERICA

Bogota
Pablo Iragorri
T +57 1 742 5556
pablo.iragorri@kroll.com

Buenos Aires
Juan Cruz Amirante
T +54 11 4706 6024
jcamirante@kroll.com

Grenada
Glen Harloff
T +1 786 340 6753
gharloff@kroll.com

Mexico City
Brian Weihs
T +52 55 5279 7250
bweihs@kroll.com

Miami
James Faulkner
T +1 786 801 8214
jfaulkner@kroll.com

Sao Paulo
Fernanda Barroso
T +55 11 3897 0907
fernanda.barroso@kroll.com

EMEA

London
Neil Kirton
T +44 20 70 29 5000
nkirton@kroll.com

Dubai
Amine Antari
T +971 4 449 6700
amine.antari@kroll.com

Madrid
Marcelo Correia
T +34 91 2747974
marcelo.correia@kroll.com

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

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

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

APAC

Hong Kong
Paul Jackson
T +852 2884 7763
paul.jackson@kroll.com

Beijing, Shanghai
Violet Ho
T +86 10 5964 7600
vho@kroll.com

Mumbai
Reshmi Khurana
T +91 22 6724 0504
rkhurana@kroll.com

Singapore
Richard Dailly
T +65 6645 4521
rdailly@kroll.com

Japan
Naoko Murasaki
T +81 3 3509 7103
nmurasaki@kroll.com

kroll.com