BUSINESSES REPORT ALL-TIME HIGH LEVELS OF FRAUD, CYBER, AND SECURITY INCIDENTS DURING 2017

84% of companies surveyed worldwide experienced a fraud incident in 2017, 86% reported at least one cyber incident, and 70% reported security incidents, according to the Kroll Annual Global Fraud & Risk Report

Confidential information is coming under increasing threat

Executives are feeling a heightened sense of vulnerability to fraud, cyber, and security risks

NEW YORK – January 22, 2018 – Fraud, cyber, and security risks are at an all-time high, according to senior corporate executives surveyed worldwide for the 2017/18 Kroll Annual Global Fraud & Risk Report[1].

The proportion of executives reporting that their companies fell victim to at least one instance of fraud over the past 12 months increased to 84%, from 82% in the previous survey. Levels of reported fraud have steadily risen every year since 2012, when the reported occurrence was just 61%.

An even greater percentage of executives surveyed (86%) said their companies had experienced a cyber incident or information theft, loss, or attack over the past 12 months, slightly up from 85% in 2016. Seven in 10 respondents (70%) reported the occurrence of at least one security incident during the past year, compared to 68% in the previous survey.

The Kroll Report reveals that respondents are experiencing a heightened sense of vulnerability to fraud, cyber, and security risks, with information-related risks now being the area of greatest concern. As criminals and other threat actors continue to find new ways to monetize confidential data, including personal data, data assets are becoming increasingly valuable and attractive targets.

Confidential information subject to increasing threats

For the first time in the Kroll Report's 10-year history, information theft, loss, or attack was the most prevalent type of fraud experienced, cited by 29% of respondents, up 5 percentage points from the previous year. This edged out theft of physical assets or stock, long the most common type of organizational loss, which this year was the second most frequently cited incident (27%).

Cyber attacks represent one of the most persistent threats to confidential information. In fact, the reported level of occurrence for every type of cyber incident included in the survey increased in the last 12 months.

In the year when major viruses such as WannaCry and Petya hit across the world, nearly four in 10 (36%) executives surveyed said their companies had been impacted by a virus or worm attack, an increase of 3 percentage points year-over-year. One in three (33%) said they had suffered an email-based phishing attack (up 7 percentage points from the last report), 27% had suffered a data breach, and 25% were affected by data deletion. Beyond digital threats, information was highly susceptible to loss through other means: 29% of executives surveyed said equipment with sensitive data was stolen, while 27% said equipment was "lost."

Physical theft or loss of intellectual property (IP) was by far the most prevalent type of security incident. Of those executives whose company experienced a security incident this past year, 41% said their organizations fell victim to IP theft or loss.

Top three types of incidents reported by survey respondents (by category)

	Fraud	Cyber	Security
1.	Information theft, loss, or attack (29%)	Virus/worm attack (36%)	Physical theft or loss of intellectual property (41%)
2.	Theft of physical assets or stock (27%)	Email-based phishing attack (33%)	Environmental risk (including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.) (28%)
3.	Management conflict of interest (26%)	Data breach resulting in loss of customer or employee data, IP/trade secrets/R&D (27%)	Workplace violence (23%)

Jason Smolanoff, Senior Managing Director and Global Cyber Security Practice Leader for Kroll, explained: "In a digitized world with growing levels of data creation, collection, and reliance for businesses, information assets have become increasingly valuable and exposed

to threats. Exacerbating the challenge of safeguarding data is that criminals and other threat actors are continually developing new ways to monetize confidential information, including personal data.

“People instinctively think about data being targeted by cyber attacks, but not all threats to information are confined to the digital realm. There is a convergence between physical and digital threats, with issues arising from equipment with sensitive data being stolen or lost, for example, or employees with access to highly sensitive information accidentally or intentionally causing a breach.”

Costly and wide-ranging repercussions

In addition to reporting extremely high incidence levels, respondents indicated that the repercussions of fraud, cyber, and security events were costly and wide-ranging, affecting employees, customers, as well as the organization’s reputation and bottom line.

Employee privacy, safety, or morale was negatively affected by incidents according to 82% of respondents whose companies had experienced fraud, 81% of those that reported a cyber incident, and 80% of executives whose companies endured a security event.

Approximately three quarters of respondents stated that customers had been negatively impacted by all three risk factors – 76% by a fraud incident, 74% by a cyber incident, and 74% by a security incident. Almost two-thirds said that the impacted company’s reputation had suffered due to a fraud (65%), cyber (67%), or security (66%) incident.

Businesses suffered significant economic damage from fraud, with nearly one in four respondents (23%) reporting losses of 7% or more of company revenues, an extremely worrisome increase from the prior year when only 3% of respondents reported this magnitude of financial impact.

Executives feeling increasingly vulnerable to risks

The Kroll Report further reveals mounting concerns among surveyed executives about their companies’ potential exposure to fraud, cyber, and security risks.

In particular, information-related risks overwhelmingly represent the top worries for respondents across every risk category – fraud, cyber, and security. Almost six in 10 (57%)

respondents believe their companies are highly or somewhat vulnerable to information theft, loss, or attack, up 6 percentage points from the previous survey.

With reported cyber incidents at an all-time high and perpetrators seeming to develop new methods of attack virtually every day, at least half of all executives surveyed are apprehensive about every type of cyber incident identified in the survey – with almost two-thirds (62%) especially wary of a virus or worm attack.

The proportion of respondents who said they feel highly or somewhat vulnerable to physical security threats also grew over the last year. In particular, 63% of respondents stated their companies could be particularly prone to physical theft or loss of IP, the greatest single concern.

Culprits inside and outside

Insiders and ex-employees continue to pose the greatest threat to companies around the world. Respondents revealed that fraud, cyber, and security incidents are often inside jobs perpetrated by members of management or current, former, or temporary/freelance employees.

Of those reporting a fraud incident, 81% cited one or more insiders as perpetrators; likewise, 58% of respondents who reported a cyber incident and 71% of those who experienced a security incident primarily identified insiders as the perpetrators.

Junior employees were the most commonly named perpetrators of fraud incidents (39%) and former employees were cited most frequently for security incidents (37%). However, for respondents who had experienced a cyber incident in the last 12 months, a random cyber-criminal or threat actor was the single most commonly named perpetrator (34%).

Imperative to mitigate risks

Nearly all anti-fraud measures mentioned in the survey were widely adopted by over 70% of respondents, with information controls the most widely implemented anti-fraud measure at 78%.

Reflecting the high levels of vulnerability reported by respondents to cyber intrusions, the top three cyber risk mitigation measures that executives expect their companies to implement in the next 12 months all address the problem of intrusions: i.e., intrusion detection systems that

are device-based (57%), endpoint threat monitoring tools (55%), and intrusion detection systems that are network-based (54%).

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

A large proportion of respondents have adopted security risk mitigation measures, but given the high incidence and feelings of vulnerability around theft/loss of IP, it was surprising to see that only 66% of respondents have a plan for securing intellectual property. However, almost a quarter (24%) of respondents plan to implement these measures over the next 12 months.

Kroll CEO David Fontaine commented: "Senior executives are becoming acutely aware that threats to their organizations can arise at any time and originate from any place. Insiders and ex-employees continue to pose a significant threat and have, together with external criminals and threat actors, more tools at their disposal than ever before with which to target and exploit companies.

"In the face of these mounting threats, organizations seeking to manage and mitigate the possibility of loss must take a holistic approach to enterprise risk management and implement diverse and layered measures that can enhance their ability to anticipate, detect, and respond to threats rooted not only in human error or intentional misconduct, but also in technological or internal control gaps."

ENDS

For further information please contact:

Ada Oni-Eseleh
Infinite Global
646-685-8075
adaoe@infiniteglobal.com

Notes to editors

[1] The Kroll Annual Global Fraud & Risk Report 2017/18 includes a full detailed analysis across a range of industries and regions.

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 physical 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. Eighty-four percent 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, 10% from Sub-Saharan Africa, 11% from the Middle East, and 19% from Latin America.

About Kroll:
Kroll is the leading global provider of risk solutions. For more than 40 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. Headquartered in New York with more than 35 offices in 20 countries, Kroll has a multidisciplinary team of nearly 1,000 employees and serves a global clientele of law firms, financial institutions, corporations, non-profit institutions, government agencies, and individuals. For more information visit www.kroll.com