KROLL

Cyber Risk and CFOs:

Over-Confidence is Costly

2022 Edition

Cyber Risk and CFOs: Over-Confidence is Costly

Introduction

Our research has shown that CFOs are highly confident in their companies' abilities to ward off cyber security incidents, despite being somewhat unaware of the cyber vulnerabilities their business faces. Almost 87% of the surveyed executives expressed this confidence, yet 61% of them had suffered at least three significant cyber incidents in the previous 18 months. Moreover, they admitted to being out of the loop: 6 out of 10 were not regularly briefed by the cyber team, and nearly 4 out of 10 had never received such an update, according to the survey conducted by Kroll and studioID of Industry Dive.

The CFOs also put a price tag on the cyberattacks they had suffered in the previous 18 months: between $10 million and $25 million for about one-third of companies who suffered a significant security incident, and more than $25 million for almost 16% of the companies. It is imperative that CFOs and their finance teams up their involvement in cyber investment, from planning to prevention and response strategies. Failing to do this leaves CFOs out of the loop on cyber issues and threatens the business with significant—and, critically, unexpected—financial consequences.

Key Points

- A total of 87% of CFOs are confident in their companies' cyber security capabilities, but 4 out of 10 had never had a briefing from information security leadership
- Comparatively, 66% of Chief Information Security Officers (CISOs) in the State of Incident Response 2021 report thought that their organization was vulnerable, and 82% said that the average organization in their industry was vulnerable to cyberattack
- 71% have suffered more than $5 million in financial losses stemming from cyber incidents in the last 18 months
- 82% of the executives in the survey said their companies suffered a loss of valuation of 5% or more following their largest cyber security incident in the last 18 months
- Cyber security spending is increasing: 45% of respondents plan to increase the percentage of their overall IT budget dedicated to information security by at least 10%
- CFOs need to understand cyber security strategies and the resulting investments required, as well as potential financial risks from cyber incidents

Ignorance Is Bliss

The survey polled 180 CFOs, CEOs and other financial executives worldwide, all of whom are involved with quantifying the financial impact of cyberattacks at their companies and with budget oversight or planning for information security.

The survey shows a sharp disconnect between the confidence that CFOs have in their organizations' cyber security abilities, and the actual, significant damage that cyber incidents are inflicting.

- More than 99% of the survey respondents are confident to some extent, including 87% who are very or extremely so.
- Yet most of the surveyed executives—61%—said their companies suffered at least three significant cyber incidents in the previous 18 months.
- What's more, only 40% of finance teams receive regular briefings or updates from the information security team, and almost 37% have never received such an update.

When you consider that 66% of Chief Information Security Officers (CISOs) in the *State of Incident Response 2021* report thought that their organization was vulnerable and 82% said that the average organization in their industry was vulnerable to cyberattack, it is clear that confidence among security types is much lower.

The CFO overconfidence could indicate a larger problem: a lack of understanding of cyber risk and its consequences, which often weigh heavily on budgets. While more regular briefings and a closer alignment of the finance and security teams would undoubtedly raise visibility and the knowledge level around cyber risk, there are other potential reasons for the disconnect. Only in recent years has it become commonplace to include security risks on the board-level agenda. If organizations haven't made this transition, cyber risk can potentially be lost as part of the broader financial risk evaluation. Furthermore, if the board itself doesn't have enough experience to fully understand cyber risk, the severity of this risk could be overlooked. This is something that is being regulated against in the U.S., with the U.S. *Securities and Exchange Commission (SEC) requiring disclosure of the cyber expertise of boards*.

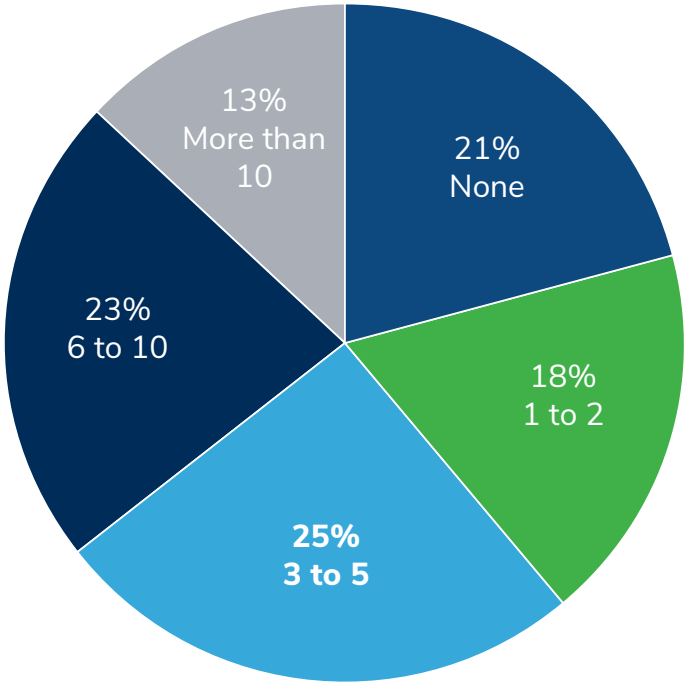
> **"To bring themselves into the loop on cyber security, CFOs should participate in cyber security planning at multiple layers in the company, including advising the board and as part of the company's risk and audit committees. CFOs should be fully involved in crisis and incident response planning for cyberattacks. They should participate in tabletop exercises where a team can walk through a simulated cyber security crisis to map out how they would respond to a real attack. Ultimately, this will enable them to understand the overall investment strategy around cyber and to evaluate financial risk and possible expenditures."**
>
> 
>
> — **James McLeary,**
> Managing Director in the Cyber Risk practice at Kroll

Target No. 1: You

Nearly four out of five of the companies represented in the survey—79%—have had at least one security incident that resulted in compromised data or financial loss in the last 18 months. And that's counting just high-severity cyber incidents—breaches where data is compromised or financial losses are incurred—not lower-level incidents. A worrying 13% have had more than 10 such significant incidents in the last 18 months.

How many security incidents resulted in a compromise of data or financial impact at your organization over the past 18 months?

n=180



79% of companies have had at least one security incident that resulted in compromised data or financial loss in the last 18 months

The top cause of significant cyber incidents was business email compromise (BEC), experienced by 65% of the organizations represented in the survey. This indicates how important employees are in defending against cyberattacks, as they will be the target of BEC.

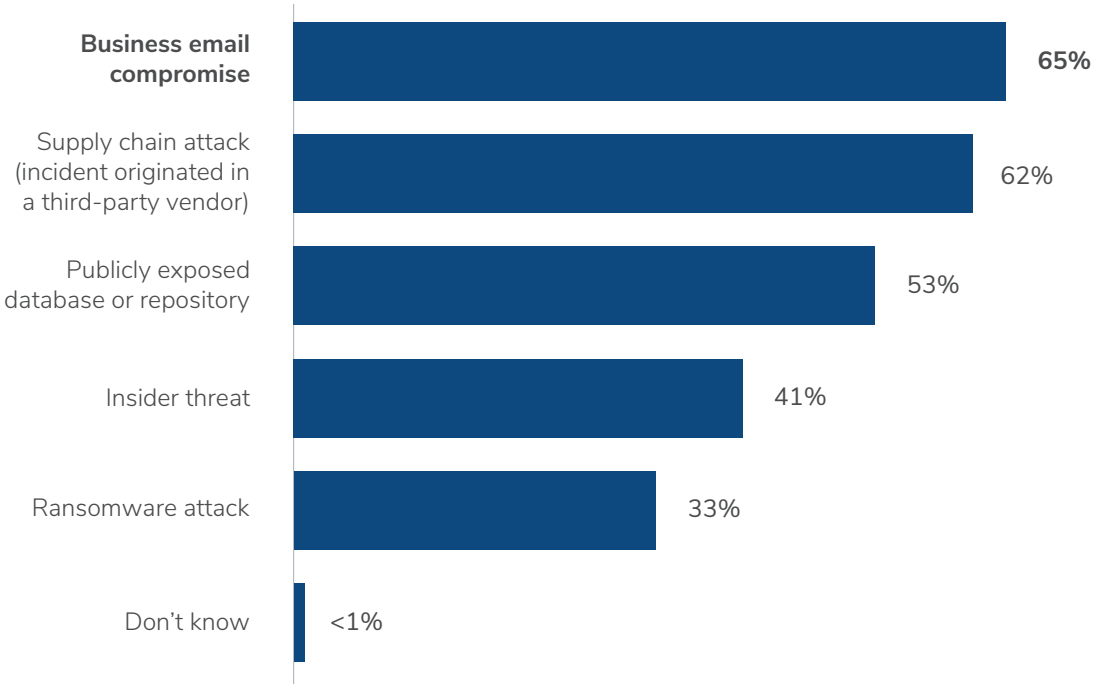
There is a possibility that BEC is magnified across our sample, because finance teams are particularly susceptible to BEC attacks, making it the most likely type of attack for them to experience firsthand. Finance team susceptibility to BEC attacks is due to them regularly receiving instructions to pay invoices or make company transactions, a common BEC scenario.

KROLL

Typically, fraudsters will send a phishing email from what appears to be a known source making a legitimate request—to wire money somewhere, for example. The victim is convinced that the request is legitimate and initiates the wire transfer to the cyber-attacker. In a variation of the scam, payment instructions are received from a third party that has been compromised, so the payment itself looks legitimate.

What type of incident led to the compromise(s)?

n=142



From the attacker's point of view, BEC is a relatively easy scam with a high success rate. High-worth transaction requests are not unusual for the finance team. The scam also has a low barrier of entry as an attack method because no sophisticated coding or malware is necessary. Also, multiple transactions can build up quickly, adding to the potential value for scammers.

BEC is difficult to defend against because it is based on social engineering. While there are technical defenses that can be deployed, such as flagging external incoming emails and multifactor authentication, the most effective security precaution is building awareness of these types of scams among your workforce and providing mechanisms for flagging suspicious emails.

To defend against BEC, employees should be well educated on this type of scam and how to avoid it:

Be careful with what information is shared online or on social media, and don't click on an unsolicited email or text message asking you to update or verify account information.

Verify requests independently: Look up the company's phone number—don't use one provided by a potential scammer—and call to determine if a request is legitimate.

Carefully examine the email address, URL and spelling on any communication and never open email attachments from an unknown sender.

Be wary of any request that presses for quick action.

Embrace the use of multifactor authentication and encourage colleagues to do the same

Next on the list of top causes of significant cyber incidents were attacks arising from a vendor—also known as supply chain attacks—cited by 62% of the survey respondents, and publicly exposed databases, cited by 53%. Insider threats were the source of compromises for 41%.

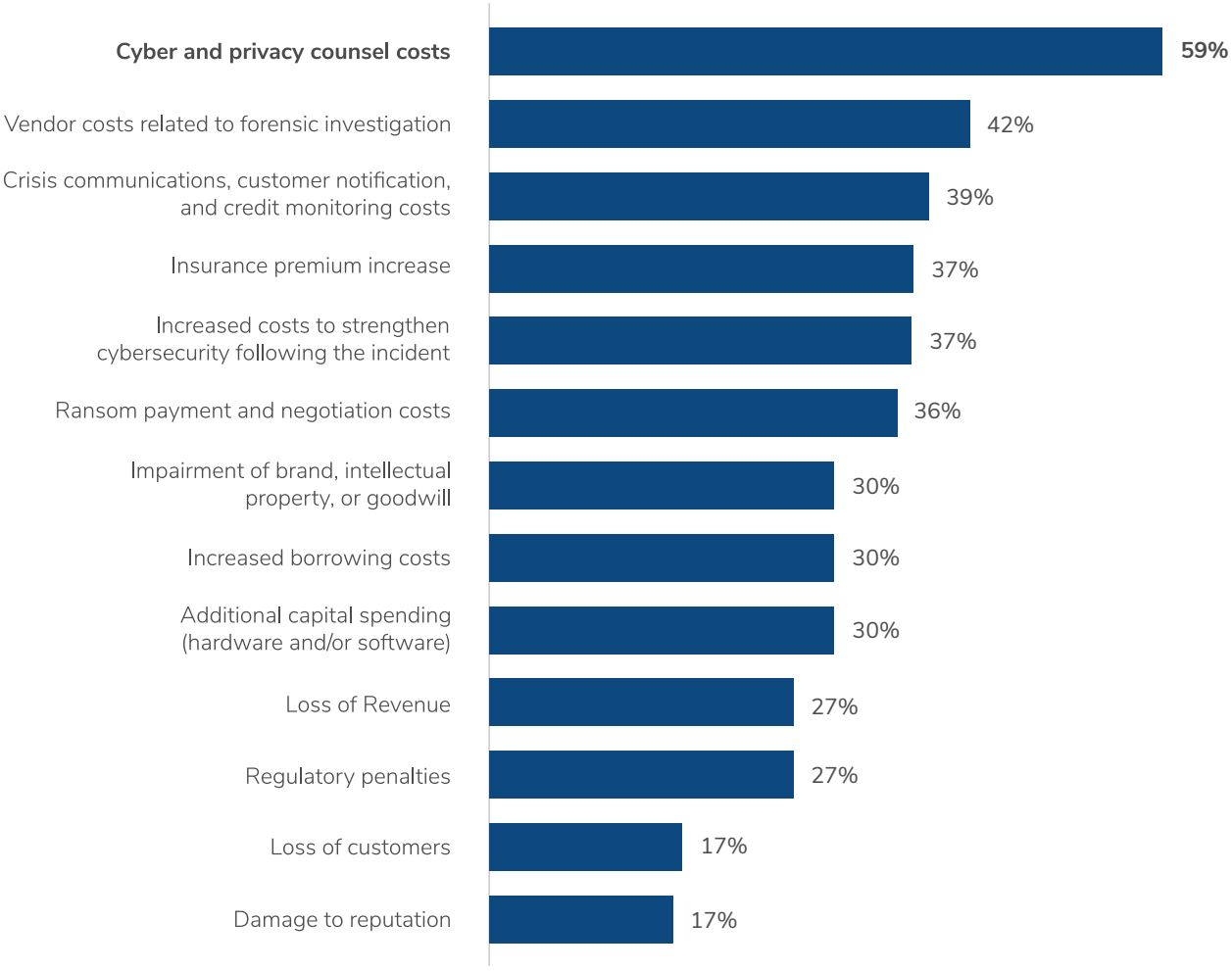
Despite intense media coverage, organizations seemed to experience ransomware attacks less. Only 33% indicated ransomware as the cause of incidents in the last 18 months, the least of any cyber threat cited.

Wide-Ranging Damages

Companies suffer damage from cyberattacks across a wide spectrum of areas.

What type(s) of impact did your organization suffer?

n=142

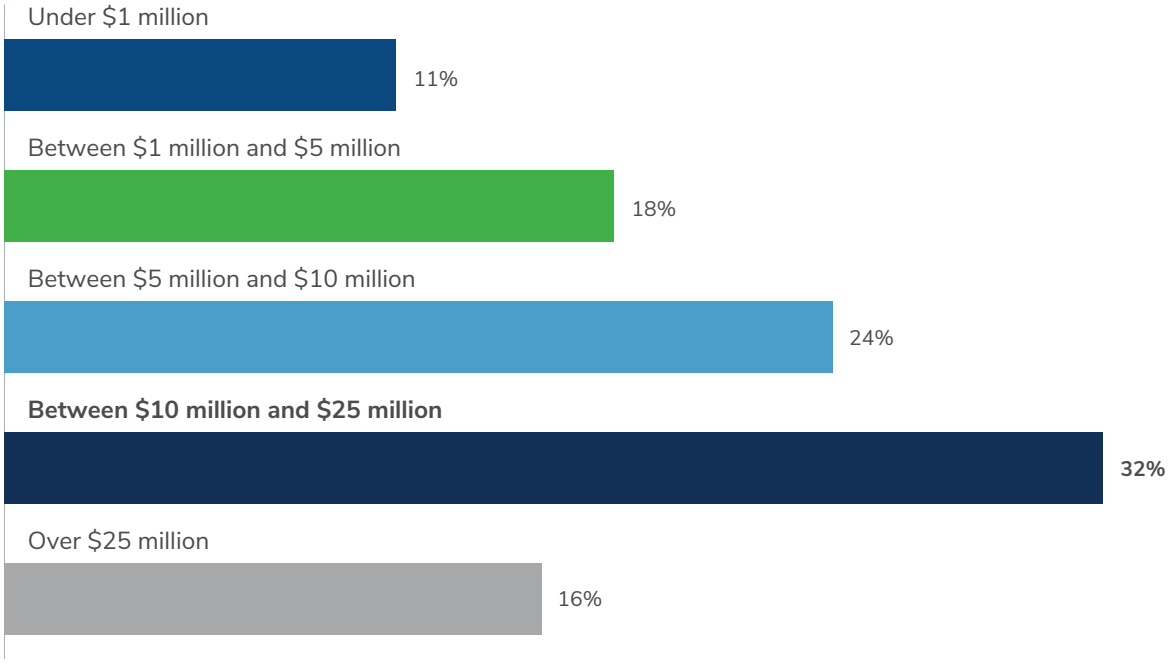


The survey identified the top financial impact coming from cyber and privacy counsel, followed by vendor costs related to forensic investigations. Next on the list were crisis communications, customer notification and credit monitoring costs, followed by insurance premium increases and ransom payment and negotiation costs as the fifth-most-cited impact. Even though ransomware wasn't high on the list of incident causes, CFOs still reported ransom payment and negotiation as one of the highest financial impact drivers.

Other tangible financial impacts cited from cyberattacks include strengthening cyber security following an incident, capital spending for hardware and software, borrowing costs, regulatory penalties, and loss of revenue. Intangible costs cited by the survey were impairment of brand, intellectual property or goodwill; loss of customers; and reputational damage.

Which of the following best captures the total financial impact of all security incidents in the last 18 months?

n=142



The survey shows that the cost of cyberattacks is significant, both in the dollar amount of damages and in their impact on company valuations. For organizations that had a security incident resulting in a compromise of data or financial impact in the past 18 months, nearly 9 out of 10 of them experienced a financial impact of more than $1 million, and 82% of the executives say their companies suffered a loss of valuation of 5% or more following their largest cyber security incident in the last 18 months.

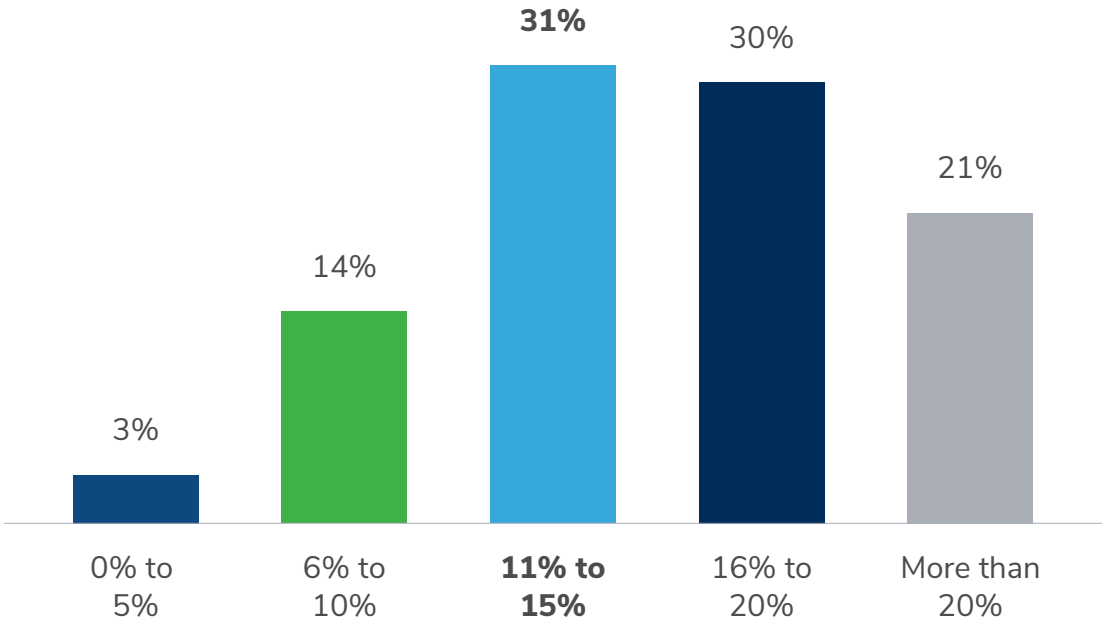
Cyber insurance is sometimes presented as a solution to cyber incident risk, but it should not be viewed as a catch-all. Many policies don't cover all impacts from a cyber incident, and cyber insurance premiums and deductibles have increased exponentially. A well-rounded security strategy would include one or more carefully crafted cyber insurance policies as well as robust investments into technical controls and awareness training.

How CFOs Are Responding

The survey offers some insights into what CFOs plan to spend on IT security in the coming fiscal year. Nearly half of the executives in the survey—45%—will increase their IT budget for information security by more than 10%. Gartner reports that financial services organizations spend 10–15% of their total IT budget on cyber security (click here). For outsourced cyber security services, nearly half of the respondents will increase their spending by more than 10%. Currently, 75% of respondents outsource between 10% and 50% of their information security budget.

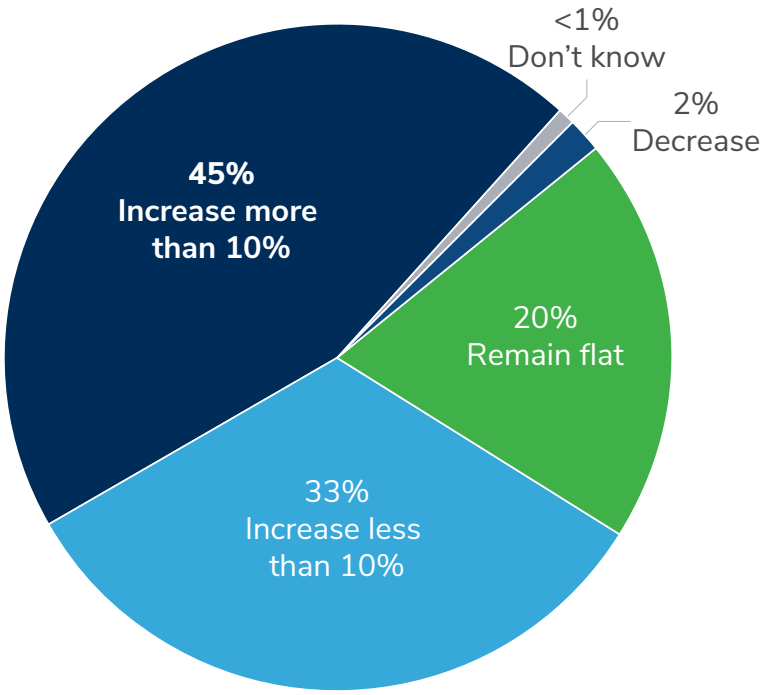
Approximately what percentage of the overall IT budget was dedicated to information security in the last fiscal year?

n=180



With regards to the next fiscal year, the percentage of the overall IT budget dedicated to information security will...

n=180



For many companies, the pandemic hit cyber security budgets hard, as security became too difficult and costly to handle in-house. Outsourced CISOs and virtual CISO advisory services can help develop strategies for preventing, detecting and mitigating cyber threats, either as an ongoing service or an interim service until a permanent CISO can be hired.

CFOs need to keep in mind that outsourcing does not absolve them of responsibility for cyber security. The CFO has a responsibility to understand the cybersecurity strategy—outsourced or in-house—because of the financial investment involved and the potential impact of an incident on company value and financial health.

45% of executives will increase their IT budget for information security by more than 10%

KROLL

Regional Perspectives: North America

Of the 180 CFOs, CEOs and other financial executives surveyed – all of whom were involved with quantifying the financial impact of cyber attacks at their companies and with budget oversight or planning for information security – nearly 60% (107) were from North America.

24%

of respondents in North America are briefed monthly by the information security team

59%

of respondents in North America had more than 3 security incidents in the last 18 months, compared to 61% globally

55%

of North American respondents were extremely confident in their company's ability to respond to a cyber incidents within the next 12 months

> **"We often see that CFOs are not aware enough of the financial risk presented by cyber threats until they face an incident. At that point, it's clear that they need to be involved not only in the recovery—including permitting access to emergency funds and procuring third-party suppliers—but also in the strategy and investment around cyber both pre- and post-incident. Ultimately, cyberattacks represents a financial risk to the business, and incidents can have a significant impact on value. It is, therefore, critical that this is included in wider business risk considerations. A CFO and CISO should be peers, helping the business navigate the operational and financial risk of cyber."**

— **Greg Michaels,**
Global Head of Cyber Governance and Risk in the Cyber Risk practice at Kroll

Regional Perspectives: EMEA

Of the 180 CFOs, CEOs and other financial executives surveyed – all of whom were involved with quantifying the financial impact of cyber attacks at their companies and with budget oversight or planning for information security – nearly 20% (35) were from EMEA.

40%

of respondents in EMEA are briefed monthly by the information security team compared to 24% globally

43%

of respondents in EMEA had had over 3 security incidents in the last 18 months compared to 61% globally

28%

of EMEA respondents were extremely confident in their company's ability to respond to a cyber incident within the next 12 months, compared to 53% who said the same globally

> **"It seems that CFOs in EMEA are much more involved with the cyber security team than in other parts of the world. Forty percent of CFOs reported being briefed monthly by their information security teams, compared to 24% globally. Interestingly, despite suffering less incidents—43% of respondents in EMEA had suffered more than three security incidents in the last 18 months, compared to 61% globally—they were less confident in their company's ability to respond to a cyberattack. This could be cultural, or perhaps tied to the fact that cyber insurance is less common in EMEA, making the threat of a cyberattack arguably more significant for the role of CFO."**

— **William Rimington,**
Co-Practice Leader for Kroll's EMEA Cyber Risk practice

Regional Perspectives: APAC

Of the 180 CFOs, CEOs and other financial executives surveyed – all of whom were involved with quantifying the financial impact of cyber attacks at their companies and with budget oversight or planning for information security – just over 20% (38) were from APAC.

8%

of respondents in APAC are briefed monthly by the information security team compared to 24% globally

84%

of respondents in APAC had more than 3 security incidents in the last 18 months compared to 61% globally

68%

of APAC respondents were extremely confident in their company's ability to respond a cyber incident within the next 12 months, compared to 53% who said the same globally

> **"Cyber security incidents appeared to be more common in APAC, with 84% of respondents suffering from more than three security incidents within the past 18 months, compared to 61% globally. This may have had an impact on CFO confidence in their company's ability to respond to an attack, as 68% of respondents in APAC were extremely confident, compared to 53% globally. It's intriguing to see that despite the number of attacks happening, CFOs in APAC rarely get briefed by the information security team, perhaps indicating different organizational sets-ups in APAC where cyber security and finance are much more siloed."**

— **James McLeary,**
Managing Director in the Cyber Risk practice at Kroll

Next Steps

Embrace regulatory trends to drive change

The U.S. Securities and Exchange Commission has proposed rules for publicly traded companies that would amplify CFOs' role in cyber security. These rules would require reporting of cyber incidents and updates on previous incidents, reporting on policies and procedures to identify and manage cyber risks, reporting boards of directors' oversight of cyber risk, management's assessing and managing of cyber risk, and annual reporting on the board's cyber expertise. The SEC's focus on cyber security reflects how important this issue has become for shareholders and customers—it is one that CFOs need to pay particular attention to.

CFOs can turn the SEC requirements and other regulators' requirements on cyber into more effective management of cyber risk by:

- Building cyber risk assessments—which are required by regulators—into the overall cyber security program
- Ensuring that policies and procedures meet or exceed the minimum standards spelled out by regulations and best practices, and that they are adequately implemented
- Considering the unique requirements of their organization in how it manages data and what controls are in place to protect that data

Join forces with your CISO to build security "muscle memory" in the organization

As the CISO role increasingly becomes more distinct from the CIO and IT department, a natural alignment should begin to form between the CISO and the CFO. With both concerned about risk, they can work together from both a strategy and investment

perspective, as well as find a rhythm for how their combined response would work in an incident. Simulating incidents ahead of time builds the "muscle memory" of incident response, avoiding bureaucracy that could slow operations or risk further damage.

As part of an incident response plan, the CFO should know whom to call, what emergency funds they have available, and what legal steps they need to take when an incident occurs. For example, if a ransomware payment is necessary, it will lead to significant financial, legal and risk considerations for the business that should be well thought-out ahead of time. There are also practical questions to consider, such as the need for a cryptocurrency account or third-party engagement.

Align information security to key business metrics

CFOs can help CISOs navigate the financial risks of cyber while meeting key business metrics such as profit margin and operational efficiency. Part of the CFO's cyber responsibilities lie in measuring the financial impact of potential and actual cyber incidents. Besides the costs of money or stolen data, response, restoration and recovery costs need to be considered, as well as the funds needed to improve cyber resilience for the future. There are also further losses to incorporate around reputation, customer attrition and company value.

With the tactical response underway, the CFO can keep an eye on wider business goals, with a sense of what "good" looks like in terms of the financial overhead of an incident response.

Conclusion

As cyber security takes on more importance for a company—impacting operations, revenue and costs, reputation, and company value—so does the financial risk of cyberattacks. Judging by the survey results, CFOs are out of the loop when it comes to cyber planning. To engage, they need to participate at multiple levels, from tabletop exercises for simulated cyberattacks to close coordination with CISOs in advising and participating in audit and risk committees at the board level. Cyber risks and their consequences are ever evolving, and CFOs' understanding of them must be as well.

At a time when cyberattacks are rife and continue to cause millions of dollars in costs while shaving off company value, failing to become involved in cyber security would be a misstep by the CFO, one that needs to be rectified fast.

Methodology

studioID of Industry Dive, in partnership with Kroll, surveyed senior finance executives to determine how cybersecurity is impacting finance at their organization. More specifically, we asked 180 finance leaders across industries about their confidence in their organization's ability to detect and respond to cyber incidents, how many cyber incidents they've encountered, and the impacts, both tangible and intangible, of these incidents on their organization.

Stay Ahead With Kroll

Data, technology and insights for risk, governance, and growth

Kroll provides proprietary data, technology and insights to help our clients stay ahead of complex demands related to risk, governance and growth. Our solutions deliver a powerful competitive advantage, enabling faster, smarter and more sustainable decisions. With over 6,000 experts around the world, we create value and impact for our clients and communities.

Advantage through our Data and Technology

Our solutions, grounded in deep expertise, facilitate smarter and more sustainable decisions.

Our Data and Platforms help:

- Stop cyberattacks with unrivaled threat intelligence and automated playbooks
- Quantify investment risk and opportunity through cost of capital benchmarking
- Standardize global fund and asset governance, reporting and valuation methodology
- Stay ahead of compliance requirements and filing deadlines
- Drive operational efficiency through workflow automation
- Scale risk assessments, background checking and diligence reviews

KROLL

About Kroll

Kroll provides proprietary data, technology and insights to help our clients stay ahead of complex demands related to risk, governance and growth. Our solutions deliver a powerful competitive advantage, enabling faster, smarter and more sustainable decisions. With over 6,000 experts around the world, we create value and impact for our clients and communities. To learn more, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.