FORTINET

REPORT

The CISO and Cybersecurity

A Report on Current Priorities and Challenges

Table of Contents

Executive Summary

The CISO and Cybersecurity Report from Fortinet takes a snapshot of how CISOs are approaching cybersecurity, and how their organizations view the CISO. Most certainly, the CISO's role has increased in scale, scope, and importance over the past decade, moving into the ranks of executive management at many organizations. Mounting complexity of IT networks, increasing sophistication of threat actors, and the rising cost of cyber crime add up to a CISO role that can potentially make or break a business. Based on survey findings from CISOs of large enterprises, here are some of the key takeaways:

1. The CISO holds an **expanding role in executive management** with responsibilities to protect on-premises, cloud, operational technology (OT), and DevOps environments. Their charter now includes physical security for 70% of respondents.
2. Despite acknowledging product-related challenges, CISOs have **high confidence in their organizations' risk posture** while acknowledging challenges with manual processes and false positives.
3. Unfortunately, CISOs' high level of confidence about security seems unfounded, as most organizations experience a significant number of intrusions, and these events have a deleterious effect on the business.

Given these trends and challenges, we analyzed the data more deeply and identified a subset of respondents who reported no intrusions in the past 12 months, and another subset that had more than six intrusions in the same time frame. The differences in practice between these two groups are instructive. We analyzed traits representative of **top-tier CISOs** versus those of their **bottom-tier counterparts.** These best practices reflect a holistic, integrated approach to cybersecurity that eliminates silos, enables automation of security response, and provides the best protection against advanced threats.

Infographic: Key Findings

63%

of CISOs report to the **CEO or board**

70%

are responsible for **physical security**

61%

have cybersecurity as a **standing topic** at every board meeting

81% have had **one or more intrusions** in the past year

53%
have had **3+** intrusions

22%
have had **6+** intrusions

40% have experienced outages that impacted **productivity, brand value, and revenue**

74%
do **not** have a fully integrated security architecture

57%
cite **too many manual processes** as one of their top three security concerns

59%
use **MSSPs** to supplement their security staff

Best-in-class CISOs are:

74% more likely to be **dramatically increasing** their cybersecurity budget

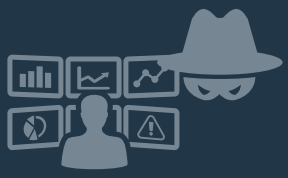
93% more likely to **measure and report vulnerabilities** found and blocked

52% more likely to have an **end-to-end, integrated** security solution

45% more likely to have **full centralized visibility and control**

Introduction

The position of chief information security officer (CISO) has existed for just 25 years[1]—and far less than that at most organizations. Despite this, the definition of the role has been in flux from the beginning. For the most part, this evolution has been toward the addition of responsibilities rather than substituting one responsibility for another.[2] As the scope of their job responsibilities grows, CISOs find themselves in a more prominent position in many organizations than in the past.[3]



"Cybersecurity has changed rapidly over the last few years. I'm now finding myself not only carrying out my day-to-day operations, but also studying to learn of new risks."
– Survey Respondent

But along with the increased prestige comes more scrutiny from top management than ever before. CISOs now must interface regularly with leaders such as the CFO, the CEO, and even the board of directors.[4] Cybersecurity has become increasingly critical to the bottom line for many organizations, and the associated risks and costs have increased dramatically over the past decade. As an example, one study found that cyber crime cost the typical organization $13 million in 2018—a 12% increase over 2017 and a 72% increase over five years.[5] And managing this risk is complicated by several factors:

1. **An expanded attack surface.** Digital transformation (DX) initiatives in progress at most organizations have brought greater complexity to IT networks,[6] and securing them is equally complicated. A company's data and applications now reside in multiple clouds, network traffic often travels over the public internet using software-defined networking (SDN) technologies, and huge volumes of new data originate at Internet-of-Things (IoT) devices that often lack adequate security protection.[7] As these technologies come online, security teams often scramble to protect them. Frequently, the result is that various point products protect different parts of the infrastructure, creating a siloed security architecture that increases manual work on the part of the security team—and reduces the organization's overall security posture.
2. **Increasing security complexity.** As networks become more complex, the task of securing them becomes more difficult. The volume of data is increasing at an alarming rate,[8] and it is often difficult to identify all the business-critical and confidential data—let alone protect it. Compliance requirements have become more complex, with 58% of compliance professionals in one survey expecting to spend more time communicating with regulators in the coming year—and nearly two-thirds requiring an increase in the compliance budget.[9] And a siloed security architecture with disaggregated tools makes both compliance reporting and threat response more complicated.
3. **A rapidly changing threat landscape.** Cyber criminals are using highly sophisticated approaches,[10] and unknown threats are increasing in frequency and scope.[11] The speed of attacks is also accelerating, with exfiltration of corporate data now happening in a matter of minutes.[12] The widely distributed networks resulting from DX mean that perimeter-based approaches to network security are obsolete. And signature-based approaches to malware detection miss the large number of zero-day threats—which now comprise as much as 40% of threats detected on a given day.

As a result, CISOs can no longer afford to simply be technologists, but rather must become drivers of business strategy.[13] They must move beyond compliance checkboxes to a broad approach based on an organization's overall risk management strategy. And they must move beyond a "band-aid" approach to covering the attack surface to a holistic, proactive stance toward threat response.

Methodology for This Study

The CISO and Cybersecurity Report is based on a survey conducted in January and February of 2019. Respondents had the job titles of CISO, chief security officer (CSO), and vice president of IT security at companies with more than 2,500 employees. Our respondents come from a variety of industries, including technology, financial services, retail, and manufacturing.

This study utilizes data from the survey to identify several current trends around the CISO role. Next, we analyze the freeform answers CISOs gave to several open-ended questions about their key challenges, to get a picture of what impacts their daily work. Finally, we then delve more deeply into the data to identify a subset of organizations that avoided any intrusions over the past 12 months, and another subset that had six or more intrusions in the past year. We compare the two groups and identify security best practices of "top-tier" CISOs versus those that fall into the bottom bucket.

Cybersecurity Trends Per the CISO

Trend: The CISO holds an increasingly important role in executive management with a broadening portfolio of responsibilities.

Confirming the findings of other research, our survey results indicate that CISOs are increasingly in the top tier of executive management, with 63% of respondents reporting directly to the CEO or board of directors (Figure 1). This seems to be a developing trend; for example, one 2017 survey showed that only 40% of CISOs reported to the CEO.[14] This trend is playing out alongside the increasing importance of cybersecurity to a company's overall profitability.

Respondents report a broad set of responsibilities, with overwhelming majorities listing cloud security, IoT security, security operations, cybersecurity training, standards and audits, and data privacy (Figure 2). Interestingly, 70% of respondents report being responsible for physical security, reflecting a growing trend toward the integration of cyber and physical security, which is a response to the convergence of cyber and physical risk.[15]

Significant majorities also listed the security of OT systems (64%) and DevSecOps (59%) as being within their charter. Regarding DevOps in particular, another survey by Fortinet found that 75% of organizations were planning to roll DevSecOps under the CISO in the coming 12 months.[16] Perhaps reflecting these expansions of the CISO's responsibilities and the increasing importance of cybersecurity, 59% of respondents report a budget increase for 2019, with 18% seeing a dramatic increase.

CISOs tend to interact frequently with the top management of the organization, with 61% reporting regular conversations about cybersecurity with the board of directors, 59% with the CEO, and 50% with the CFO (Figure 3). As both the risks and costs associated with cybersecurity increase, all of these leaders have a growing stake in the work of the CISO. Communicating effectively with them can require a learning curve for many CISOs, who largely come from technical rather than business roles,[17] and most have only technical degrees and few hold an MBA degree.[18] Yet, justifying security spend and demonstrating return on investment (ROI) for security investments can be critical for the CISO's success.

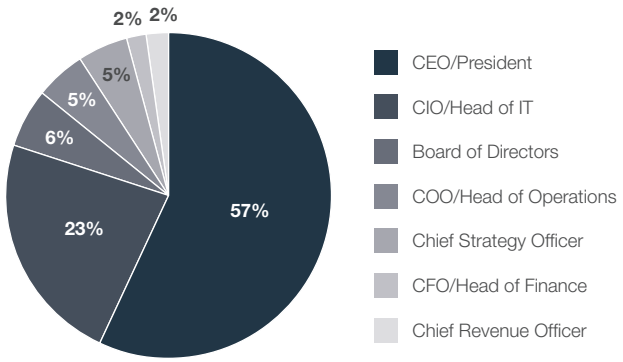


Figure 1: CISOs' direct supervisor

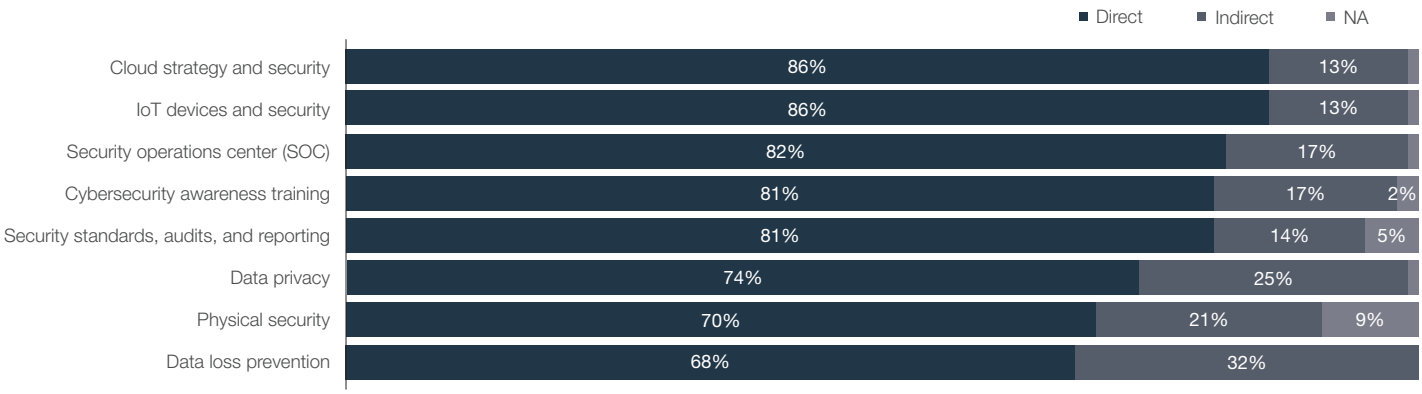


Figure 2: Top personal job responsibilities for CISOs

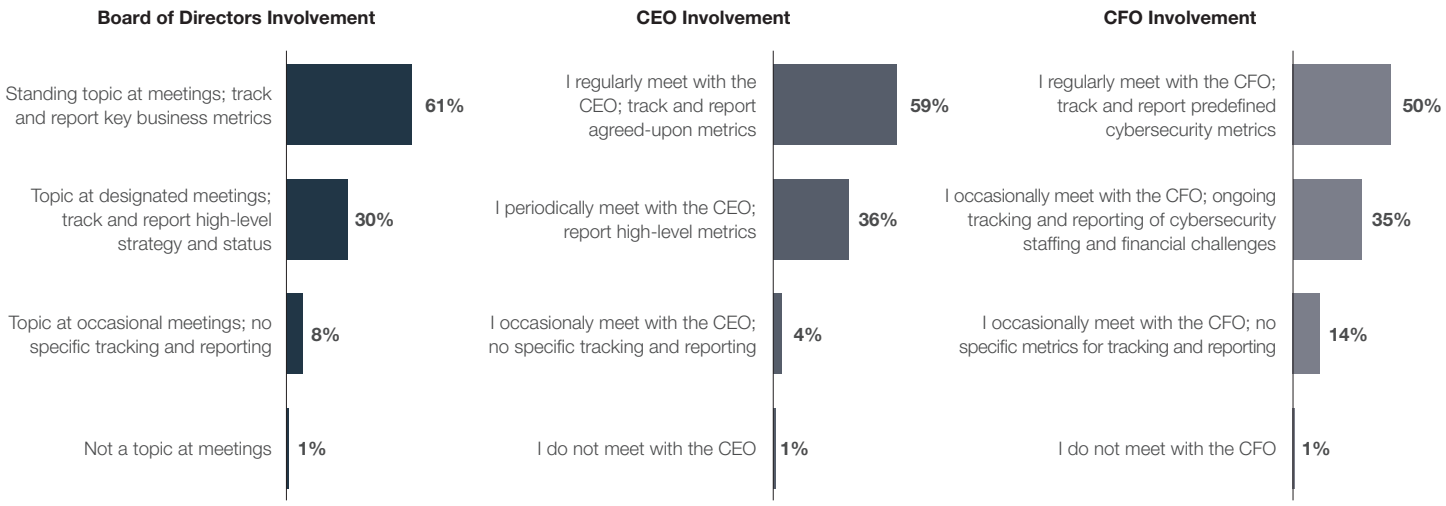


Figure 3: CISO interaction with board of directors, CEO, and CFO

Trend: The CISO is measured by key security and productivity metrics and tracks broad trends internally.

When asked for the top four criteria used by their management (often the CEO) to evaluate their success, responses were very broad. DevOps security was cited in the top four more than any other category (Figure 4), suggesting that executive management sees the increased risk that accompanies the business agility gains afforded by the methodology.[19]

The next two most often cited success measurements, both mentioned by more than 40% of respondents, are operationally focused: staff productivity and operational efficiency. Indeed, if the top two responses are viewed only, these two areas are cited more than any other measurement (23% for staff productivity and 24% for operational efficiencies). While obsession with efficiency may seem counter to security goals at first glance, achieving these efficiencies through integration of the security architecture and automation of security processes can improve an organization's security posture as well.[20] Plus, in the face of a cybersecurity skills shortage, ever-evolving advanced threat landscape, and increased security complexity, it becomes much clearer why CISOs would see these measurements as critical.

Within their teams, CISOs do significant tracking of security metrics, with more than half tracking intrusions detected and remediated, tangible risk management outcomes, and cost reduction and avoidance (Figure 5). When these measurements are taken in aggregate, they suggest that CISOs are attentive to both risk management issues and the total cost of ownership (TCO) of their security investments.

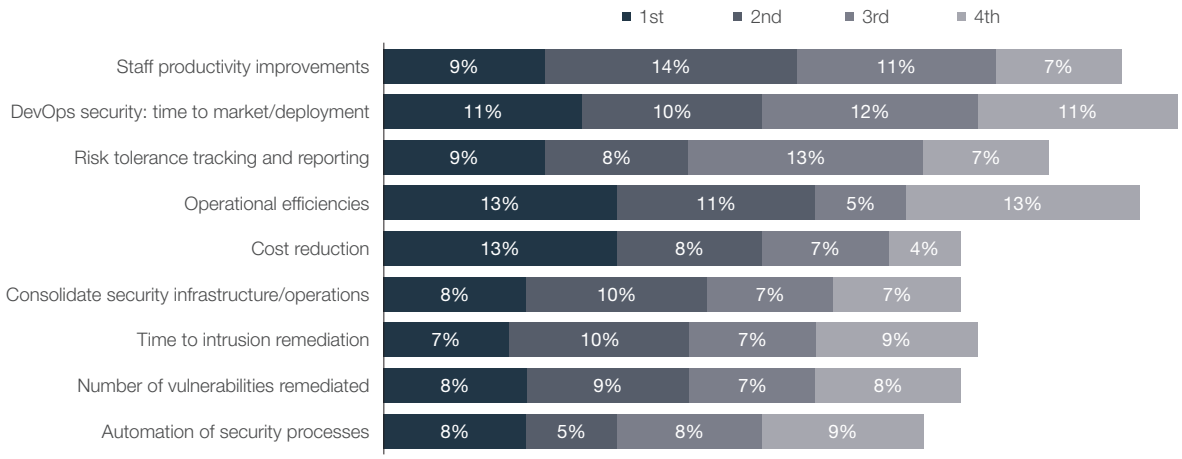


Figure 4: Top 4 success measurements for CISOs

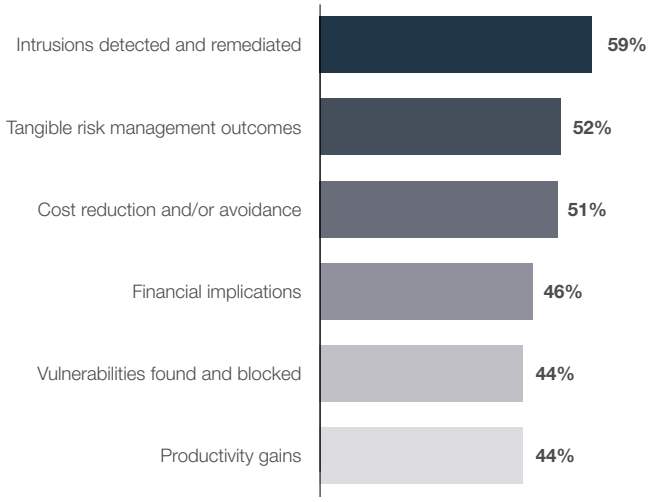


Figure 5: Cybersecurity measurements tracked and reported by CISOs

Trend: The CISO has high confidence in the organization's threat posture, but is challenged with manual processes and relies on outside help.

Two-thirds of our respondents (67%) claim that their organizations were "early movers" in DX and have applications and data residing in the cloud, active connected IoT devices, and extensive mobile adoption. It is clear that these technologies are now mainstream and widely adopted.

Despite the complexity brought by these initiatives, CISOs are overwhelmingly confident in their organizations' security posture (Figure 6). More than eight in 10 (81%) claim that they are protected because they have full visibility and control, and more than 70% believe their risk management posture is strategic and proactive. A smaller but significant majority (62%) believes they have unknown threats under control.

This high confidence contrasts starkly with what CISOs report regarding their security architecture. Namely, despite the overwhelming majority who claim to have full visibility and control across their security architecture, just over one quarter (26%) report that they use an end-to-end integrated security solution (Figure 7). Another 38% state that they are in the process of integrating point products together to increase efficiency and lower risk, but it is unknown how successful those efforts will ultimately be. Another 11% have a partially integrated solution with gaps for certain point products.

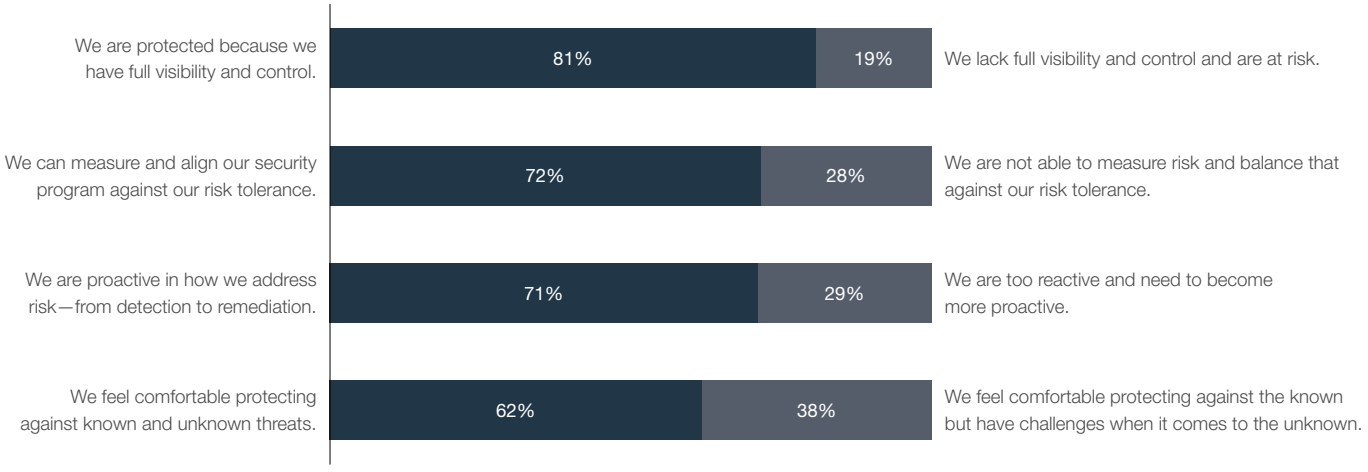


Figure 6: CISO confidence in their organizations' cybersecurity approach

When these three response types are tallied, they add up to nearly three-quarters of respondents. Here the adage "you do not know what you cannot see" may be apropos—and thus the reason many CISOs *think* they have full visibility and control. This is corroborated by another question, to which 57% of CISOs named "too many manual processes" as one of their top three challenges (Figure 8).

When these and other issues are too much for their internal teams to handle, CIOs do not hesitate to engage outside help. 59% of respondents use MSSPs to supplement their security staffs in specific areas, but only 6% engage them for a majority of security functions (Figure 9).

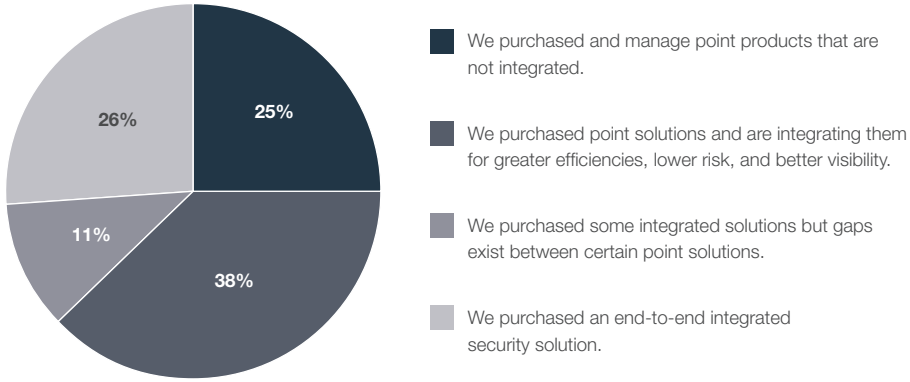


Figure 7: DX security architecture for CISO

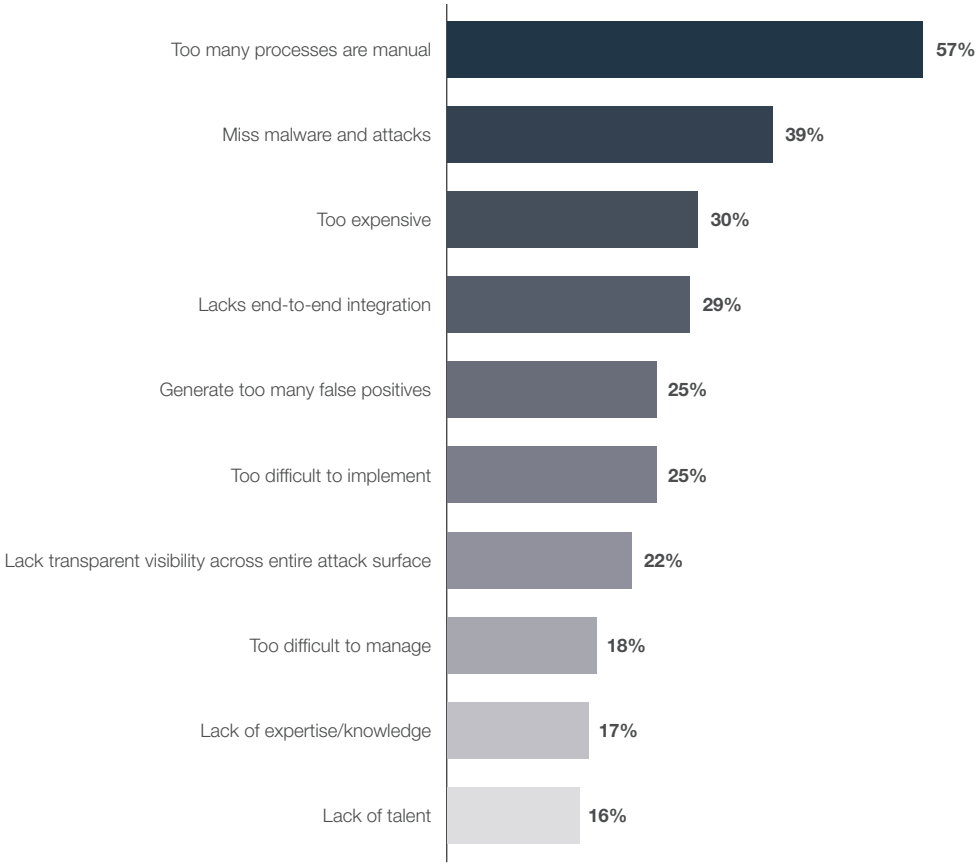


Figure 8: Security issues named in top three by CISOs

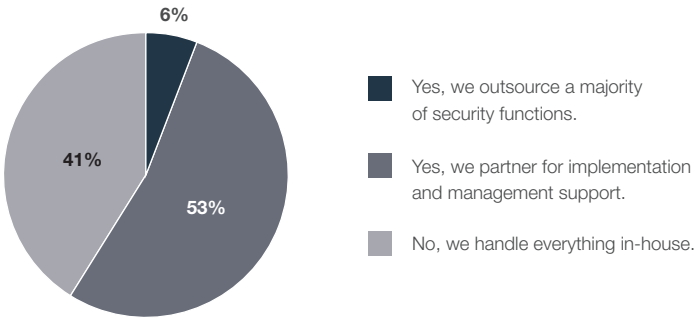


Figure 9: CISO engagement with MSSPs

Trend: CISOs still experience a significant number of intrusions that have a tangible impact on their businesses.

While CISOs express high confidence in their security posture, more than eight in 10 (81%) saw at least one intrusion in the past year (Figure 10). More than half (53%) saw more than three intrusions, and 22% saw more than six. Malware, spyware, and distributed denial-of-service (DDoS) attacks topped the list of attack types.

These intrusions are causing not only headaches for the security team but also detrimental business outcomes. More than 40% of respondents experienced an outage that impacted productivity (47%), brand value (44%), or revenue (41%). Alarmingly, 32% saw an attack that put physical safety at risk—a reminder of the reasons why so many CISOs are now responsible for both cyber and physical security.

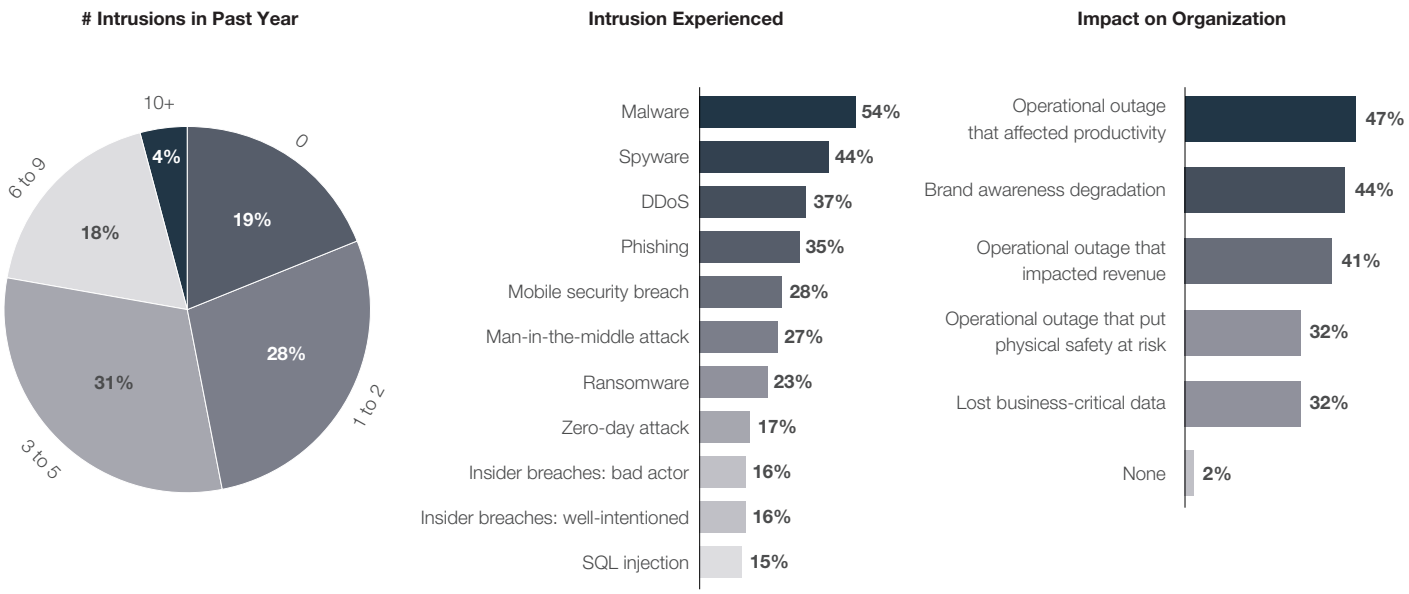


Figure 10: CISO-reported intrusions in the past year

Key Challenges for CISOs

Our survey also asked respondents to answer several open-ended questions around the key challenges they face in their jobs. While responses varied greatly, we categorized their answers in order to get a feel for what is top of mind for CISOs.

Challenge: Hackers and attackers are the most prominent industry challenge for CISOs.

When asked to give the top three industry challenges that are causing them to enhance or change their security posture, nearly half of CISOs who gave a response cited hackers and other attackers—by far the most common answer (Figure 11). As IT systems and threats become more complex, CISOs likely feel they are fighting attackers on multiple fronts. This makes it more challenging to maintain a proactive posture toward threats, which helps explain the second most common challenge cited—strategy.

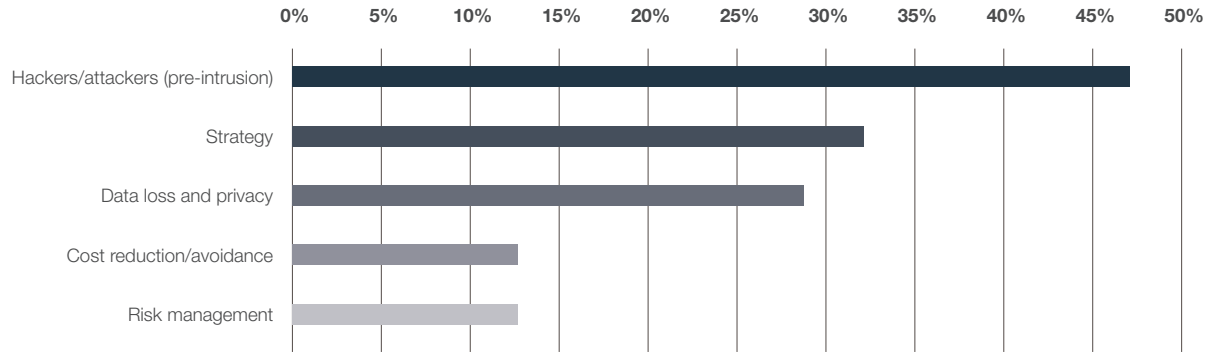


Figure 11: Top security challenges cited by CISOs (when asked to name three)

Challenge: Complexity is the biggest challenge deriving from an expanding attack surface.

Regarding the challenges brought on by the expanding attack surface, CISOs cited increased complexity nearly twice as often as any other response. This is not surprising given the increased complexity of networking that drives the expanded attack surface. Services on multiple clouds, mobile connectivity on the fly, proliferating IoT devices, and SDN all bring further complexity to the network. This is the source of other common challenges cited, such as the increased need for learning and development and security tool proliferation.

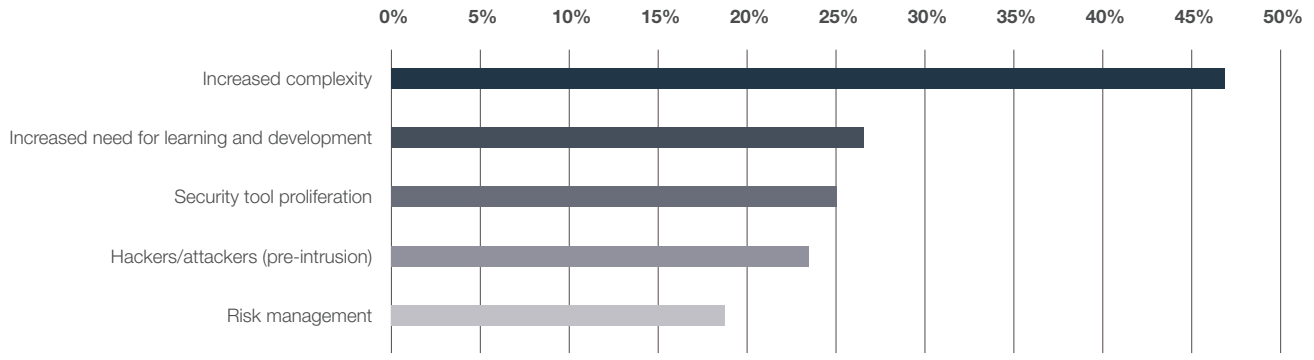


Figure 12: CISO challenges resulting from an increased attack surface

Challenge: More learning and development opportunities for the security teams is needed.

When asked to comment on how the expanding complexity of cybersecurity impacts their ability to fulfill their responsibilities, the increased need for learning and development for security team members was the predominant response from CISOs (cited by more than 40% of respondents). Nearly one-quarter of CISOs listed risk management as another challenge; namely, defining and reporting risk management measurements becomes more difficult as security becomes more complicated. Nearly 20% included issues around job stress and burnout, a problem that has not gone unnoticed elsewhere.[21]

"[The expanding attack surface] is making us take risks and use newer security technology to keep our protection up to date." – Survey Respondent

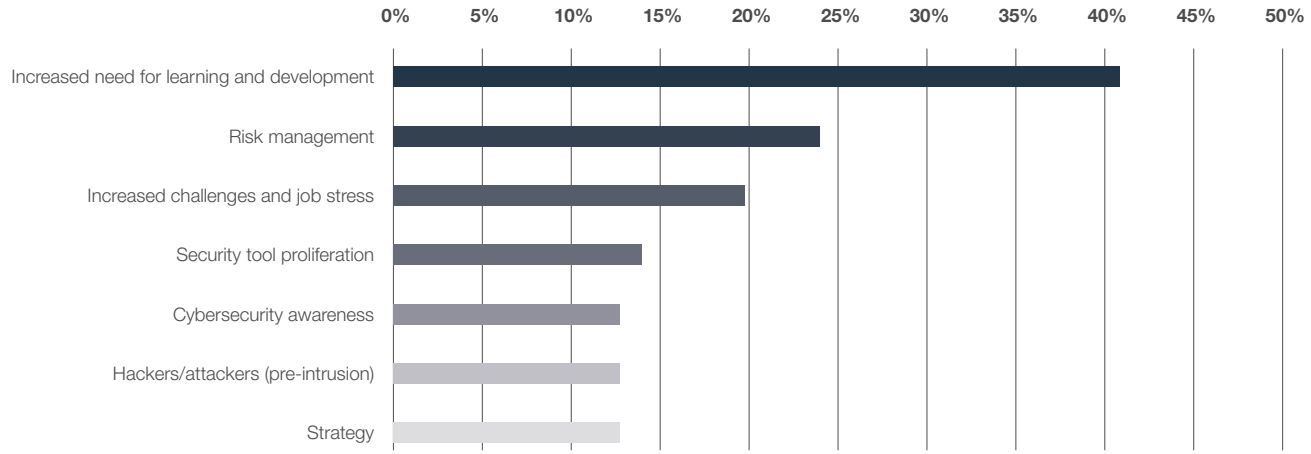


Figure 13: CISO challenges as a result of increased security complexity

Challenge: The current threat landscape compounds many of the same challenges.

CISOs cite many of the same challenges when asked how today's threat landscape affects their fulfillment of job responsibilities. The need for learning and development, the problem of hackers and attackers, and the challenges of risk management are exacerbated further by the increasing sophistication of threat actors and the multivector nature of many attacks.

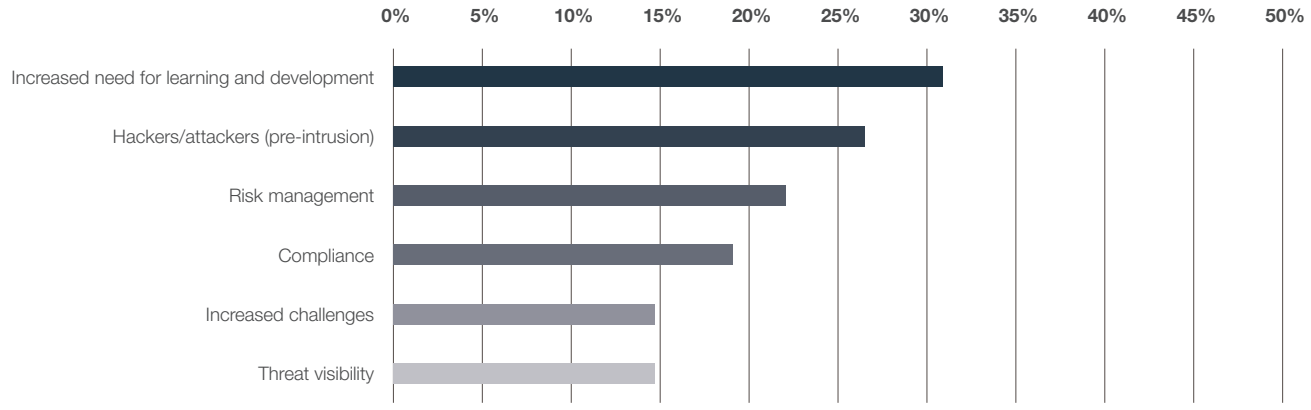


Figure 14: CISO challenges as a result of an advanced threat landscape

Best Practices of Top-Tier Enterprises

As mentioned, only 19% of CISOs reported zero intrusions in the past year, while 22% admitted to having experienced more than six intrusions. We compared the survey responses from these two subsets—our "top-tier" and "bottom-tier" respondents. This analysis identified a number of best practices that top-tier CISOs were more likely to employ:

1. Top-tier CISOs are 266% more likely to be dramatically increasing their 2019 security budgets.

While it may be counterintuitive for organizations that have been intrusion-free for 12 months to dramatically increase their cybersecurity budgets, top-tier CISOs were nearly four times as likely to be doing so than bottom-tier ones. When security is a part of corporate culture, investment in security is easier to sell, and the company understands that the evolving threat landscape requires proactive action.

2. Top-tier CISOs are 93% more likely to measure and report vulnerabilities found and blocked.

As the old adage goes, what gets measured gets improved. And in cybersecurity, a team can only track and measure information that it has access to. Gathering data about vulnerabilities is critical—especially in organizations heavily involved in DevOps activities—and requires intentional effort on the part of the development, operations, and security teams.

3. Top-tier CISOs are 52% more likely to have purchased an end-to-end integrated security solution.

In addition to providing centralized visibility and control, an integrated security architecture enables full automation of security processes and threat response. This is important given that threats now move at machine speed, meaning manual response is often not fast enough.

4. Top-tier CISOs are 45% more likely to have a security architecture with full centralized visibility and control.

A siloed security architecture not only reduces efficiency but also degrades an organization's security posture. Part of the reason for this is siloed visibility, which makes it easier to miss an attack to one silo before it impacts others.

5. Top-tier CISOs are 35% more likely to address risk proactively—from detection to remediation.

The best CISOs approach cybersecurity from a risk management perspective, understanding the risks posed by each type of attack, each portion of the attack surface, and each compliance checkbox. A big part of proactive risk management is the automation of security processes—detection, prevention, response, and remediation. Policies can be set that address each step of the process according to the level of risk posed.

6. Top-tier CISOs are 27% more likely to measure risk and align their security program against risk tolerance.

Resources are finite in every organization, and the best CISOs set their teams' priorities according to their organizations' proactively defined risk tolerance. Of course, this requires the ability to measure risk and an objective of an organization's risk tolerance—things that have not been developed at many organizations. CISOs who can truly use such a strategy can identify their most critical systems and data and ensure their protection first.

7. Top-tier organizations are 26% more likely to measure productivity gains from their security solutions.

When the overall organization—including the CEO, CFO, and board of directors—understands the business value derived from the security infrastructure, the program is more likely to get the funding and support it needs.

8. Top-tier CISOs are 25% more likely to have robust protection against known and unknown threats.

Signature-based approaches to malware protection are no longer adequate in a world where polymorphic malware constantly changes form and unknown threats are more common. Robust solutions use artificial intelligence (AI), machine learning (ML), and sandbox analysis to identify threats by their behavior and characteristics.

"Tools are important, but it is also critical to understand how they fit into your overall security strategy."
– Survey Respondent

Conclusion

Our research shows that CISOs are increasingly important to the success of their organizations. As such, they have heightened status in the organization—and increasing responsibilities. CISOs have a high view of where their organizations are with regard to security, but their frequent experience of damaging intrusions says otherwise. CISOs still experiencing significant intrusions can learn from the best practices of those who have had no recent intrusions. Some of these include:

Increasing investment in cybersecurity in response to an increasingly complex threat landscape

Taking a risk management approach to cybersecurity

Measuring cybersecurity performance against benchmarks and peer organizations

Deploying an end-to-end, integrated security architecture with full visibility and protection against known and unknown threats

In addition, as the job of CISOs becomes increasingly complex, the best approach they can take is to simplify operations through integration and automation. A strategic, risk management-based approach helps to eliminate silos and enables organizations to be proactive rather than reactive with cybersecurity.

References

[1] Steve Katz is credited as the first CISO, starting with Citigroup in 1994. See Demetrios Lazarikos, "CISO: The Evolution Of The Species," ITSP Magazine, September 19, 2016.

[2] Todd Fitzgerald, "The 5 Stages of CISO Success, Past & Future," Dark Reading, January 25, 2019.

[3] "2018 Global State of Information Security Survey," IDG, December 8, 2017.

[4] "NACD Director's Handbook on Cyber-Risk Oversight," National Association of Corporate Directors, January 12, 2017.

[5] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, accessed March 12, 2019.

[6] Benson Chan, "Digital transformation reimagines everything," Strategy of Things, September 7, 2017.

[7] "Anticipating the Unknowns: Chief Information Security Officer (CISO) Benchmark Survey," Cisco, March 2019.

[8] Bernard Marr, "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," Forbes, May 21, 2018.

[9] "Cost of Compliance Report 2018," Thomson Reuters, accessed March 27, 2019.

[10] For example, see Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018; Kevin Williams, "Threat Spotlight: Advanced polymorphic malware," SmarterMSP.com, June 13, 2018.

[11] According to internal research, 75% of unknown malware detected by FortiGuard Labs was not found in the VirusTotal tool—which aggregates threat information from more than 100 security vendors.

[12] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[13] Justin Somaini, "The Evolving Role of the CISO: From Risk Manager to Business Enabler," SecurityRoundtable.org, July 31, 2018.

[14] "2018 Global State of Information Security Survey," IDG, December 8, 2017.

[15] Peter High, "Former NSA Cyber Leader Now Leads Security For Fortinet," Forbes, March 11, 2019.

[16] "2019 State of DevOps Security Report," Fortinet, February 25, 2019.

[17] 82% of current CISOs rose to their position out of technical, operational, or consulting roles, per Taryn Aguas, et al., "The new CISO: Leading the strategic security organization," Deloitte Review, 2016.

[18] Joseph Schorr, "CISOs: You need to manage by 'walking around,'" VentureBeat, March 16, 2019;
Andrew Rose, "Evolve To Become The 2018 CISO Or Face Extinction," Forrester, August 20, 2014.

[19] "2019 State of DevOps Security Report," Fortinet, February 25, 2019.

[20] "Fortinet Security Fabric Powers Digital Transformation: Broad, Integrated, and Automated," Fortinet, March 29, 2019.

[21] Macy Bayern, "Burnout warning: High stress levels impacting CISOs' physical, mental health," TechRepublic, February 14, 2019.

FORTINET

www.fortinet.com

April 26, 2019 11:40 PM

D:\Fortinet\Work\April\042419\Task 1\report-ciso-and-cybersecurity

327523-0-0-EN