FORTINET

REPORT

The CIO and Cybersecurity

A Report on Current Priorities and Challenges

Table of Contents

Executive Summary 3

Infographic: Key Findings. 4

Introduction 5

Methodology for This Study 6

Trends for the CIO and Cybersecurity 6

Key Challenges for CIOs 12

Best Practices of Top-Tier CIOs 15

Conclusion 16

References 17

Executive Summary

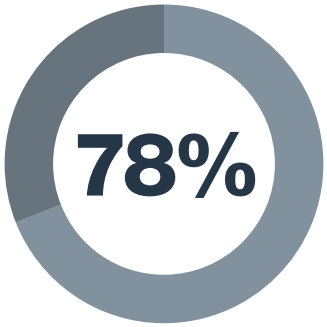
The CIO and Cybersecurity Report looks at the CIO's increasingly important role, and how that role interacts with the practice of cybersecurity. With the explosive growth of digital transformation (DX), the position of the CIO in the success of a business is unprecedented. At the same time, CIOs face new and more complex challenges with regard to cybersecurity.

And while the CISO/CSO role is moving out from underneath the CIO in a growing number of organizations, primary cybersecurity responsibilities still reside underneath the CIO in a significant number of organizations. In addition, even for those CIOs who no longer have cybersecurity reporting directly to them, cybersecurity remains a critical key performance indicator (KPI) for them.

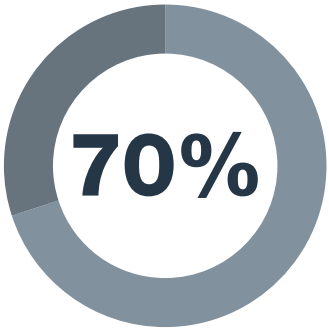
Our data uncovered a number of trends about the CIO and cybersecurity, including:

1. CIOs tend to see their organizations as technologically advanced and are confident in their security posture.
2. Despite this confidence, a majority of CIOs disclose that their organizations still experience significant intrusions, and that these events are having negative impacts.
3. CIOs say their organizations tend to use point security products to cover the attack surface and compensate for this siloed architecture by attempts at integration and reliance on managed security service providers (MSSPs) to fill gaps.

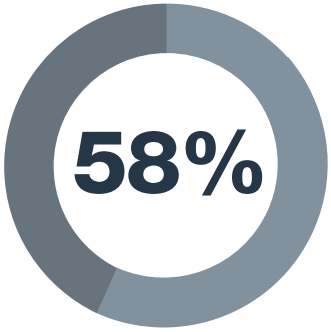
Analyzing the data more deeply, the report identifies a subset of respondents who reported no intrusion in the past 12 months, and compared their responses with a subset that had more than six intrusions in the same period. These operational and technology best practices leverage both hard skills and soft skills, enabling a holistic approach to security. For CIOs, a proactive, integrated approach to technology, people, and processes is vital for their success in cybersecurity.



of CIOs report to the CEO

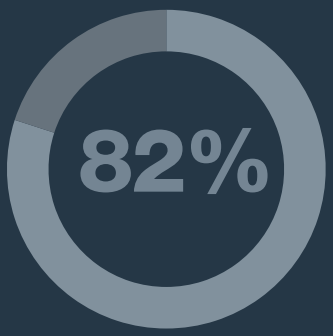


have high confidence in their visibility and control of cybersecurity systems

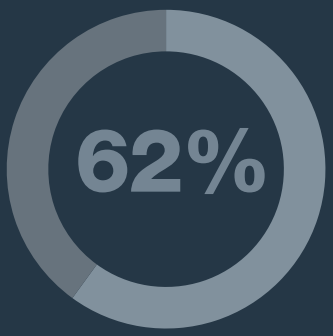


of CIOs partner with MSSPs

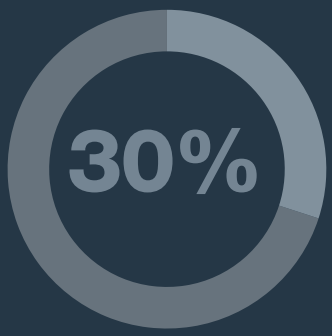
Infographic: Key Findings



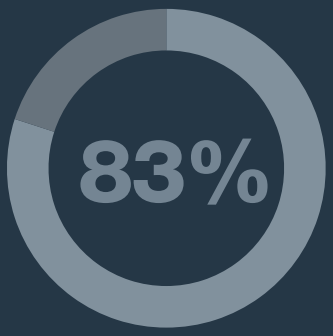
are responsible for cybersecurity



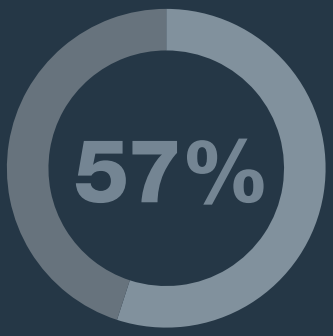
are responsible for physical security



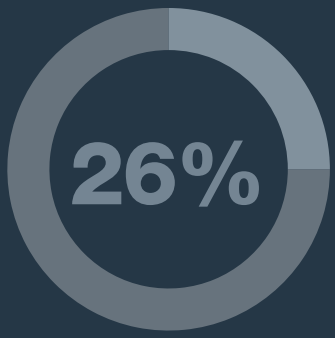
list cybersecurity risk management as their #1 performance measure



of organization experienced at least one malicious intrusion in the past year



experienced 3+ intrusions in the past year



experience 6+ intrusions in the past year

Best-in-class cybersecurity CIOs are:

4x as likely to outsource a majority of functions to an MSSP

2x as likely to have an end-to-end integrated security architecture

134% more likely to track and report productivity gains from cybersecurity

71% more likely to regularly discuss cybersecurity with the CEO

Introduction

Technology is more important to the functioning of enterprises—and to their profitability—than ever before. As a result, according to one recent survey, more than 80% of CIOs believe their role has increased in importance over the past five years.[1] CIOs have grown from technical experts to key business decision-makers who play a central part in formulating corporate strategy, optimizing operations, and increasing profit margins.[2] And the role continues to evolve: A recent survey found that CIOs believe their skills at delivering major organizational change will be more pivotal to their success in three years than at present.[3] Given these trends, it is not surprising that 70% of CIOs believe that chances are increasing for CIOs to be promoted to the CEO role[4]—something that has been rare to this point.

At the same time, CIOs face many challenges. Their jobs are now more structurally complex, involving problems such as technology sprawl, siloed infrastructure, and operational challenges due to the competing needs of different stakeholders.[5] This additional complexity means that more than half of CIOs rate their companies' IT/business alignment as moderate or worse.[6] Another challenge is finding team members with the right skills: while 47% of CIOs expect their IT headcount to increase, 65% report that a shortage of talent is holding their organizations back.[7]

Another challenge is that many CIOs are playing catch-up with their personal leadership skills. Fully 43% of CIOs rose to their positions from the application development discipline—a technical role that traditionally downplayed "soft skills."[8] Only 10% of CIOs have earned an MBA degree,[9] and 71% came to their positions from internal ranks—meaning that they may have work experience in a limited number of companies.[10] Many CIOs acknowledge these gaps, with 42% conceding they need to improve their communication skills and seven in 10 admitting they need to improve their interactions with other executives.[11]

Things are changing for the CIO regarding cybersecurity as well. An increasingly complex threat landscape brings significant risks to an organization, and network security is currently the top spending category in the area of networking.[12] At the same time, protecting against these risks has become a topic of intense interest for the leaders above the CIO. For example, cybersecurity is now discussed in 89% of board meetings.[13]

How CIOs Got to Their Current Role
43% of CIOs rose to their positions from the application development field, and **71%** came to their current roles through internal ranks.

CIO Skills
Only **10%** of CIOs have earned an MBA and business skills remain in high demand for the CIO; this includes soft skills that often are associated with business management.

Methodology for This Study

The CIO and Cybersecurity Report is based on a survey completed in late January and early February 2019. Respondents are CIOs with more than 2,500 employees. Respondents come from a variety of industries, including technology, financial services, manufacturing, retail, and healthcare.

The study utilizes data from the survey to paint a picture of today's CIO—role, responsibilities, and position within the organization, with an emphasis on cybersecurity responsibilities. Based on data gathered in the survey, the examination identifies several trends for CIOs with regard to cybersecurity and the special challenges that they face. We then delve more deeply into the data, identifying best practices more commonly used by "top-tier" cybersecurity CIOs—those who have not experienced any intrusions in the past 12 months—versus CIOs that struggle when it comes to cybersecurity.

Trends for the CIO and Cybersecurity

Trend: The CIO is a first-tier executive with responsibilities for on-premises and cloud infrastructures.

While the CIOs of the last decade often sat two or three levels down on the organizational chart, they currently sit at the top tier of executive management at most organizations (Figure 1). Among respondents to our survey, 78% report directly to the CEO, and an additional 4% report directly to the board of directors alongside the CEO. Of those that remain, 15% report to the chief operating officer (COO), and just 2% report to the chief financial officer (CFO)—a number that is significantly lower than a decade ago.

A large majority are responsible for all aspects of cybersecurity (Figure 2)—including for cloud (75%), Internet of Things (IoT) (78%), email (70%), and even operational technology (OT) (70%) systems. More than two-thirds are also responsible for security awareness (82%), IT governance (73%), and compliance (68%) programs. Two-thirds also report being responsible for managing the security of the DevOps infrastructure—a critically important function at many organizations. Given the increasing complexity of the threat landscape, it is not surprising that 47% of respondents are increasing their cybersecurity budgets in 2019.

Commensurate with their significant security responsibilities and their level in the organization, large majorities of CIOs converse regularly with the board of directors and CEO about cybersecurity matters (65% and 63%, respectively), and a smaller majority (53%) regularly discuss these issues with the CFO (Figure 3). The percentage of those meeting regularly with the CFO on the topic is interesting. As the risks and costs involved grow, the CFO will become a key player in cybersecurity strategy—and in many cases will need to learn more about cybersecurity in the process.[14]

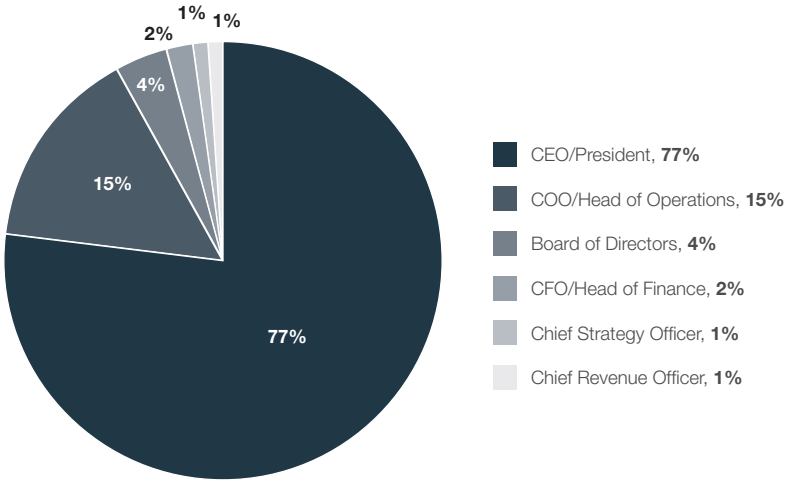


Figure 1. Positions to whom the CIO reports

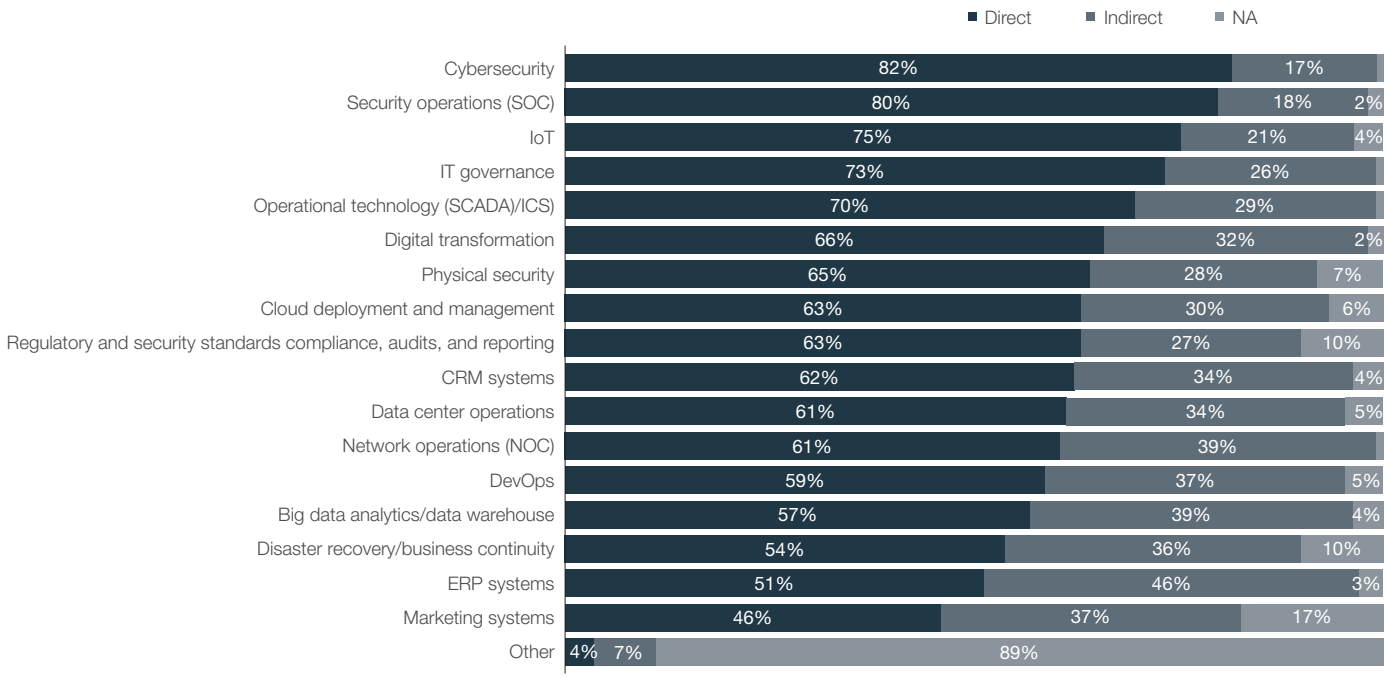


Figure 2. CIO personal job responsibilities

It should be noted that these numbers do not reflect a trend toward the CISO reporting directly to the CEO as a peer of the CIO. This trend has been noted in a number of studies,[15] including Fortinet's own forthcoming study based on a survey of CISOs. This discrepancy is likely explained by the fact that CIOs who still hold significant security responsibilities are more likely to complete a security-related survey. However, even CIOs who no longer have the cybersecurity team reporting to them often still own aspects of security, and certainly have input into cybersecurity decisions.

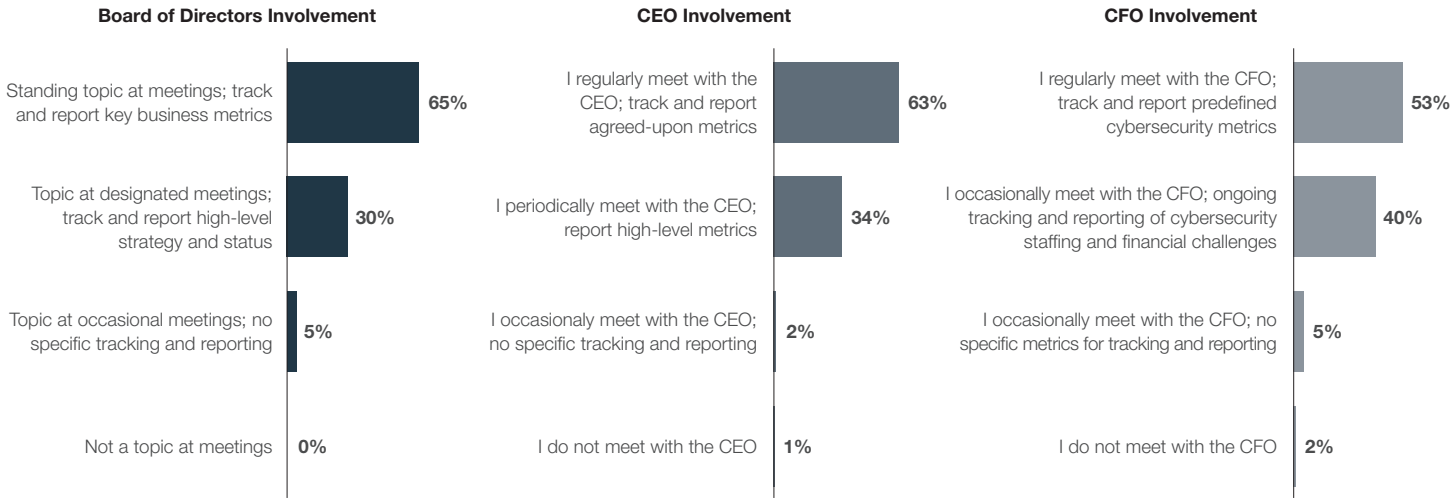


Figure 3. CIOs' interactions with the board, CEO, and CFO

Trend: The CIO tracks cybersecurity metrics and is measured on risk management.

CIOs tend to be measured more often by strategic risk management metrics related to cybersecurity rather than more tactical considerations (Figure 4), with 30% of respondents ranking this first among their measurements of success and 55% ranking it in the top three. However, managing the efficiency and cost of cybersecurity is in the top three success measurements for even more CIOs (59%), although it is less frequently cited as the top measurement. These rankings suggest a strategic orientation toward both risk management and operational efficiency.

For their teams, more than half of CIOs report that they track and report vulnerabilities found and blocked and intrusions detected and remediated (Figure 5). These priorities reflect both a strategic search for vulnerabilities that could lead to future intrusions—especially relevant at organizations employing DevOps methodologies—and a proactive approach to dealing with intrusion attempts when they happen.[16]

Figure 4. Top three success measurements for CIOs

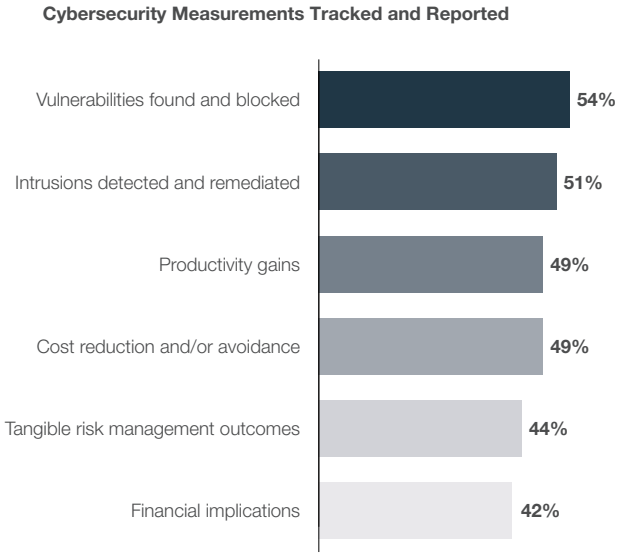


Figure 5. Cybersecurity measures tracked and reported

Trend: CIOs view their organizations as advanced regarding digital transformation (DX) and have high confidence in their security posture.

Respondents generally have a positive view of the status of their DX initiatives, with 61% asserting that their organizations were early movers in DX and have significant cloud, IoT, and mobile operations in place today. Similarly, these CIOs tend to have a high view of their organizations' security posture (Figure 6). Large majorities claim they are protected because they have full visibility and control (70%), can measure risk and align their security program accordingly (67%), and address risk proactively from detection to remediation (64%). A smaller majority (56%) is confident about their posture against unknown or zero-day threats.

Taken in isolation, the responses to this question seem to indicate that most CIOs have little to worry about regarding cybersecurity. However, responses to other questions about their organizations' security architecture and the frequency with which they experience intrusions are not so optimistic. This discrepancy points to significant overconfidence on the part of these CIOs.

Figure 6. CIOs' confidence in their organizations' cybersecurity

Trend: CIOs' organizations are still seeing significant intrusions, and they are having negative impacts.

Despite substantial efforts to plug security gaps, the vast majority of respondents are still seeing a significant number of security events (Figure 7). Only 17% of respondents experienced no intrusions in the past year. Over half (57%) had more than three intrusions, and 26% had more than six. Malware (57%), spyware (40%), and distributed denial-of-service (DDoS) (33%) attacks each impacted one-third or more of respondents. As intrusions employ a wide variety of attack vectors and methods, CIOs must ensure they develop and maintain a holistic security strategy that covers all of them.

The impact of these intrusions was significant. More than half of respondents (52%) saw at least one outage that impacted productivity, 43% experienced an impact on physical safety, and 40% felt an impact on revenue. The fact that physical safety impacts were felt by so many CIOs is a reminder that cybersecurity risk is broader than data loss and system downtime.

"The expanded attack surface] is resulting in a much more expensive security infrastructure, in terms of additional specialized software and hiring additional people." – Survey Respondent

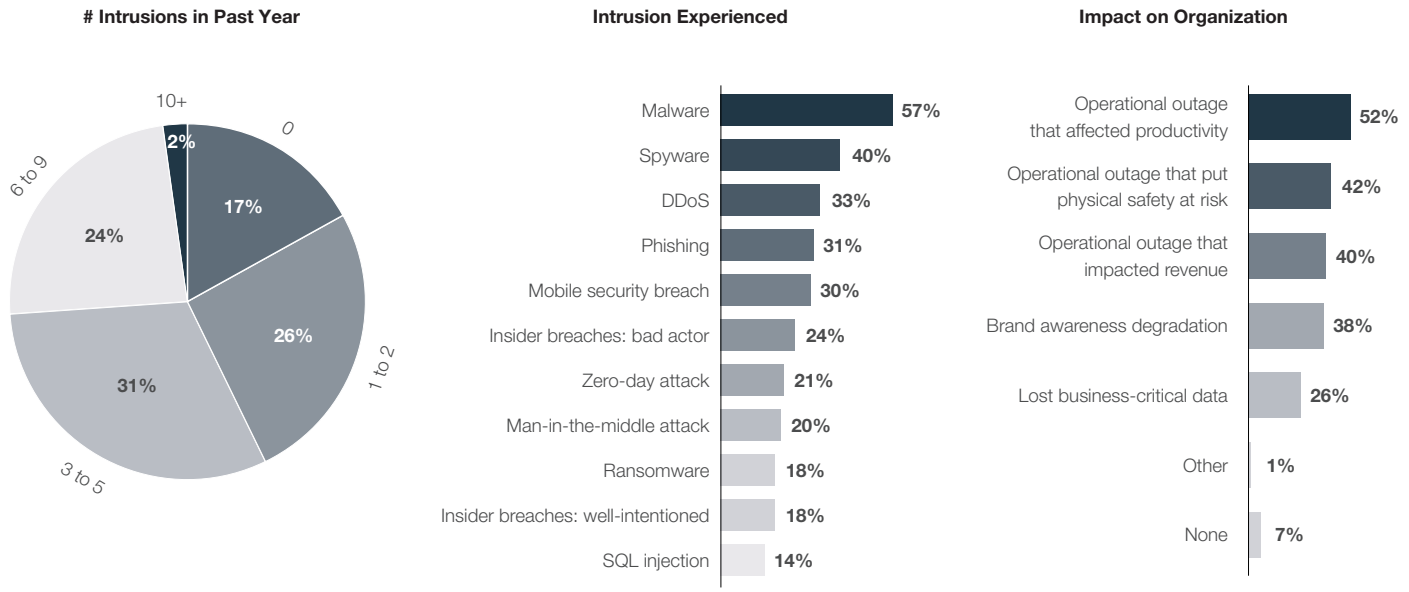


Figure 7. Intrusions at CIO organizations in the past 12 months

Trend: CIOs tend to use security point products to cover the attack surface, and many use MSSPs to supplement their security teams.

Respondents are taking a variety of approaches to deal with the expanded attack surface brought on by DX initiatives. Only 22% protect their systems with an end-to-end integrated security solution. A disaggregated security architecture is a pain point for many CIOs, with 39% in the process of fully integrating point products that they have purchased (Figure 8). How successful these integration efforts will prove to be remains to be seen.

While many CIOs are attempting to develop an integrated security architecture, respondents were clear-eyed about the problems with the point products they are using. When asked to name their top three security issues, the most common answers related to product shortcomings (Figure 9): false positives (35%), hard-to-manage solutions (34%), and issues with integration (32%).

The cybersecurity skills shortage exacerbates these problems at many organizations, and many organizations leverage MSSPs to fill gaps in their existing teams. A clear majority (59%) of respondents do significant business with an MSSP (Figure 10). 11% of respondents use MSSPs for a majority of their security functions, while 39% use them for implementation and management roles for specific security products. This suggests that many organizations put strategic thought into how best to leverage the scalability of MSSPs to supplement their team at specific points.

"It can be frustrating to always be reactive to the different threats that pop up on a too-regular basis."
– Survey Respondent

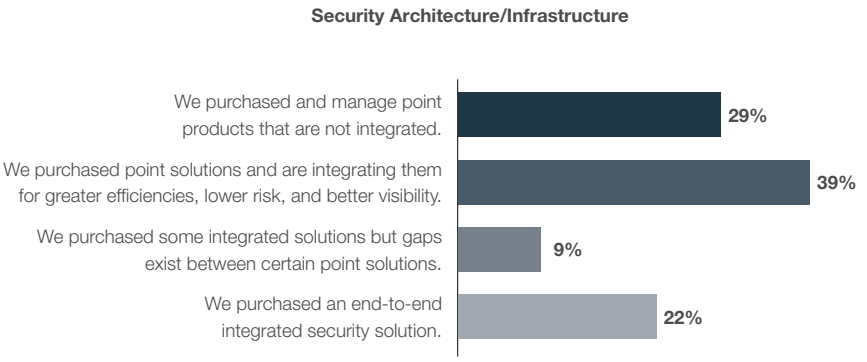


Figure 8. DX security architectures at CIOs' organizations

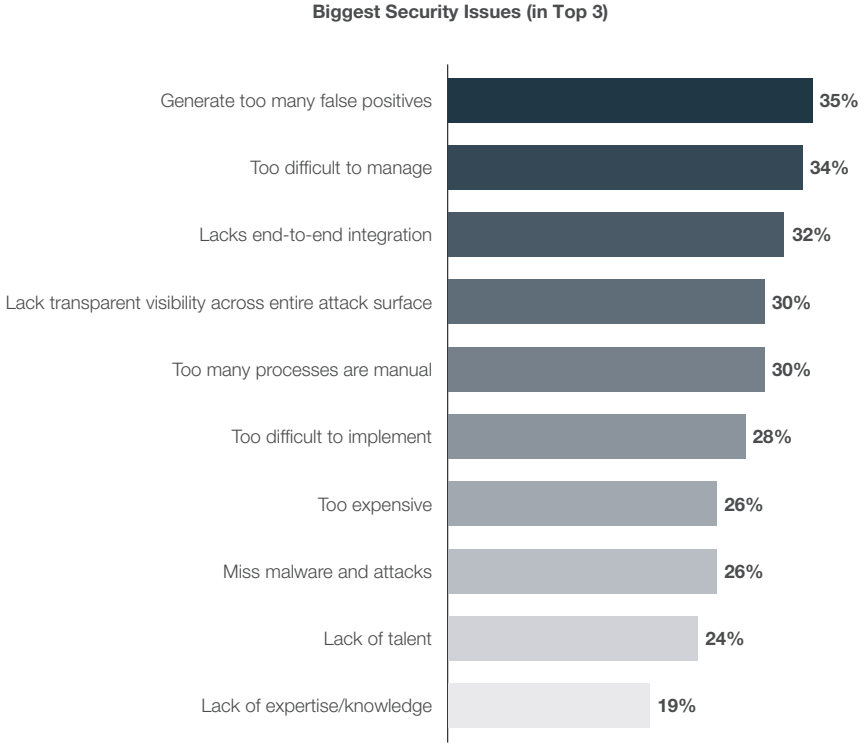


Figure 9. Security issues ranking in the top three for CIOs

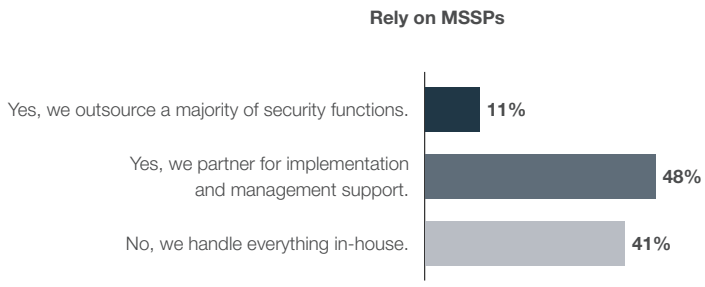


Figure 10. CIO engagement of MSSPs

Key Challenges for CIOs

Our survey asked respondents to answer several open-ended questions to provide a deeper understanding of the key challenges CIOs face in their daily work. While responses varied greatly, we categorized those answers to get a picture of what is top of mind for CIOs.

Challenge: Hackers and external attacks top the list of industry challenges.

When asked to name the top three challenges causing them to enhance or change their security posture, respondents gave a wide variety of answers (Figure 11). The issue of preventing hackers and external attacks is mentioned by three times as many respondents as any other category of answer—nearly half of those who provided an answer. This is not surprising given the increasingly dire threat landscape facing CIOs, as well as the media attention paid to major data breaches that have had an impact on the value of brands. This suggests that CIOs need to prioritize preventing intrusions from occurring in the first place—dealing proactively rather than reactively with threats.

Other industry challenges cited by significant numbers of CIOs include cybersecurity strategy, learning and development for the cybersecurity team, and increased complexity

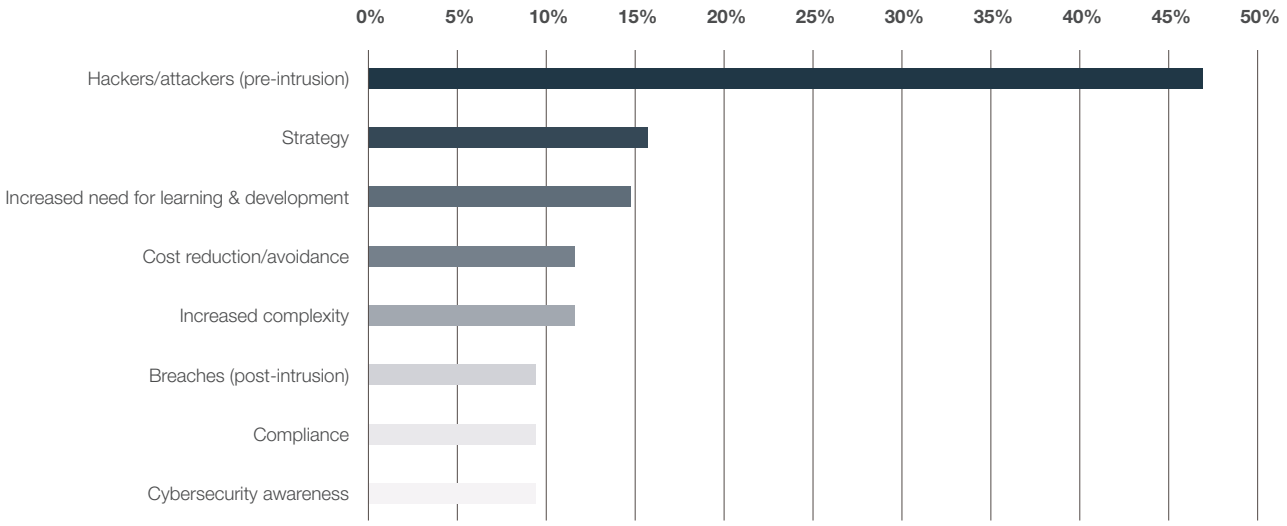


Figure 11. Industry challenges cited in the top three by CIOs

Challenge: Increased complexity is the biggest challenge of an expanding attack surface.

When asked how the expanding attack surface impacts their ability to do their jobs, one issue was predominant—increased complexity, mentioned by nearly half of respondents (Figure 12). Risk management is the second most frequently cited category, suggesting that CIOs recognize that these issues are best viewed in the context of the overall portfolio of organizational risk tolerance.

The problem of complexity tends to be exacerbated whenever a new attack surface element is introduced. These could include a new public or private cloud, a software-defined wide-area network (SD-WAN) deployment, a new DevOps or application container infrastructure, or new types of IoT devices connected to the network. When new security tools are deployed for each of these expansions of the attack surface, the security architecture can quickly balloon and become siloed and inefficient—plus, and most importantly, ineffective at providing comprehensive security.

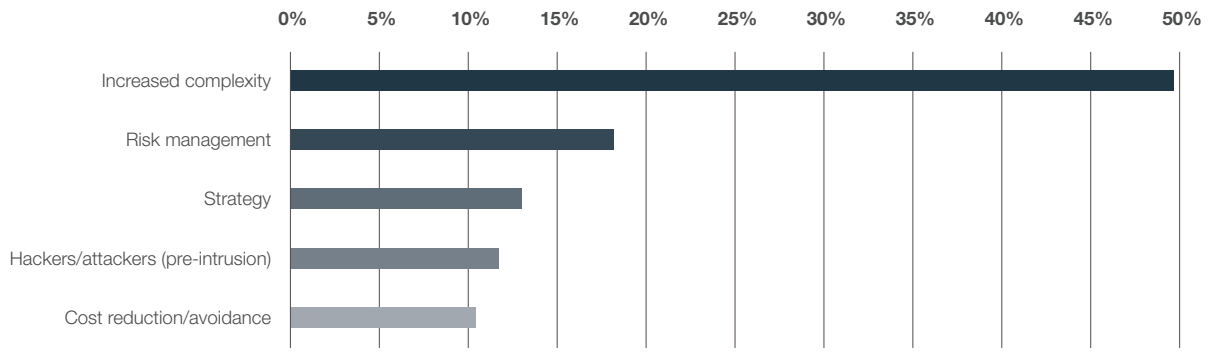


Figure 12. CIO challenges caused by the expanding attack surface

Challenge: Security complexity brings stress and impedes strategy.

When respondents were asked how the increasing complexity of cybersecurity impacts their work, their most common answer is that it increases challenge and stress in their jobs (Figure 13). Given the stakes involved, this is not surprising. New research pegs the cost of cyber crime in 2018 for the typical organization at $13 million—a 12% increase over 2017 and a 72% increase over five years.[17] Data breaches now command intense media scrutiny, and the face of IT for a company often receives negative scrutiny after a breach. This state of affairs can certainly bring anxiety for the CIO, and burnout is not uncommon.[18]

Learning and development was tied for a close second for this question, along with strategy. Since most CIOs come from a technical background and lack formal training in business administration, they can sometimes overlook this priority. Increasing complexity can mean that even cybersecurity experts on a CIO's team may not be able to keep up if they are not intentional about updating their skills. Likewise, strategy is impacted by complexity, and a strategic rather than tactical approach is required to keep systems secure these days.

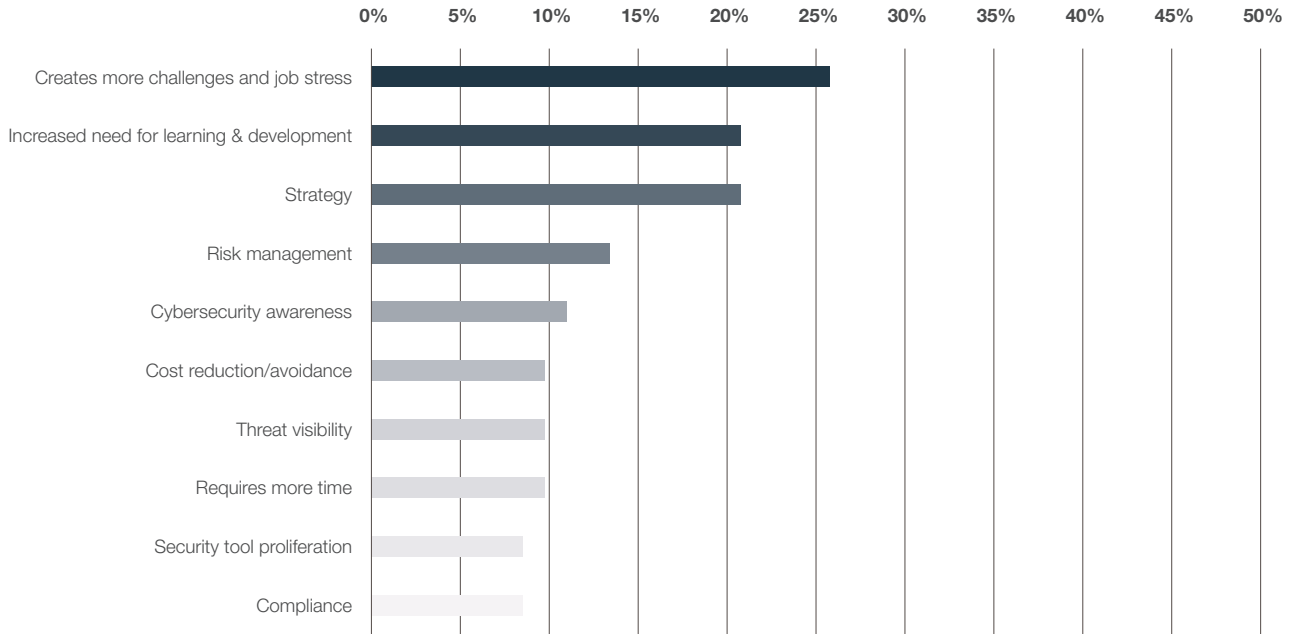


Figure 13. Effects of security complexity on the ability of CIOs to perform their jobs

Challenge: A complex threat landscape brings the need for full visibility.

When asked how a complex threat landscape affects their work, CIOs again emphasized two of the factors discussed above—strategy and training and development (Figure 14). But a third issue also predominated—the need for full visibility of threats.

In a world where threats are faster, more sophisticated, and harder to detect, siloed visibility across multiple security solutions is no longer adequate. When threat intelligence comes from multiple sources, it often has to be manually correlated across systems. Today's threats move at machine speed, meaning that this manual work may not be fast enough.

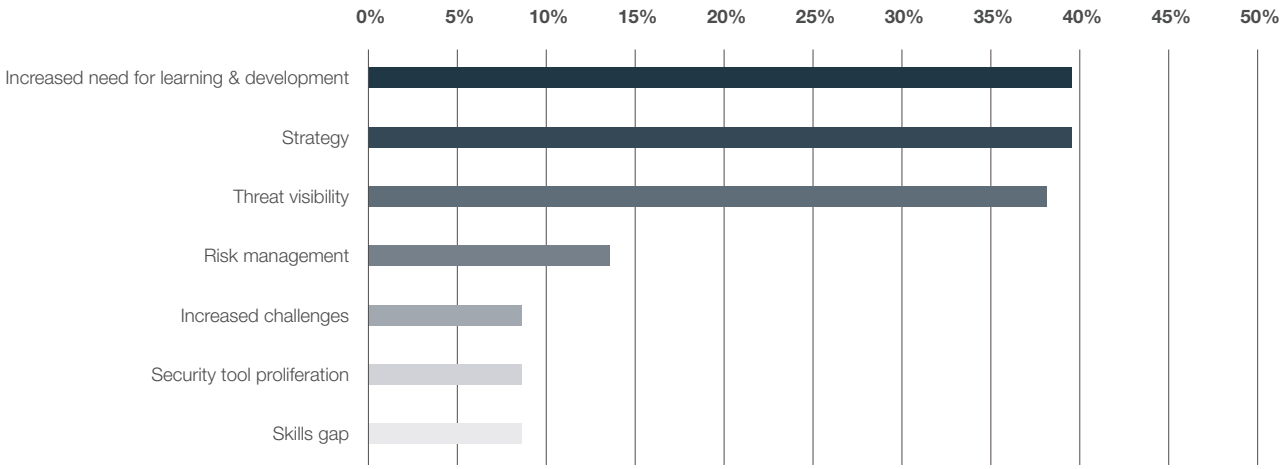


Figure 14. Effect of the threat landscape on the ability of the CIO to fulfill their responsibilities

"Cyber-threat landscapes are constantly changing. This can be detrimental to my position."
– Survey Respondent

Best Practices of Top-Tier CIOs

It is clear from our data that CIOs face significant challenges in protecting their organizations from increasingly sophisticated threats. However, some of the respondents have been more successful than others in combating cyberattacks and reducing risk for their organizations.

As noted above, 17% of respondents did not experience any intrusions in the past year, while 26% experienced six or more intrusions. We compared the cybersecurity practices of these subsets to identify the following best practices more commonly practiced by "top-tier" CIOs than by "bottom-tier" CIOs:

1. Top-tier CIOs are twice as likely to have purchased an end-to-end integrated security solution.

An integrated security architecture enables centralized visibility and control, automation of security policies, and threat-intelligence sharing across the infrastructure. This lays the foundation for achieving best practices with regard to cybersecurity—and reduced risk for the organization.

2. Top-tier CIOs are 71% more likely to meet regularly with the CEO to discuss cybersecurity.

Having a regular meeting at the executive level with a standing agenda keeps a topic at top of mind for an organization's leadership. This can potentially ensure that the CIO has the resources he or she needs to secure the network. Top-tier CIOs were also 43% more likely to have cybersecurity as a standing topic at every board meeting.

3. Top-tier CIOs are 4x as likely to outsource a majority of security functions to an MSSP.

The strategic decision to outsource a function can potentially make the difference in that function's success. When in-house expertise does not exist in a particular niche, partnering with an MSSP is an increasingly attractive option for CIOs. They offer in-house expertise, built-in scalability, and service-level agreements (SLAs) that help CIOs meet business objectives in a cost-effective way.

4. Top-tier CIOs are 134% more likely to track and report productivity gains from security solutions.

While cybersecurity is often viewed within an organization as a cost center rather than a business enabler, top-tier organizations are more than twice as likely to measure the business impact of their cybersecurity programs. Doing so helps the organization understand the value of the security team's work, potentially resulting in additional support in the form of monetary resources and internal goodwill. This is an area where top-tier CIOs have brought the business discipline of building total cost of ownership (TCO) and return on investment (ROI) models to technical teams that have not historically practiced them.[19]

5. Top-tier CIOs are 42% more likely to have full visibility and control across their attack surface.

Siloed visibility and control create increased risk on several fronts. Operational inefficiencies take staff time away from strategic work, manual correlation of security data leads to human error, and lack of automation enables fast-moving attacks to take place while manual work is in progress. Here, achieving full visibility and control is an important early step to an optimal security architecture.

6.Top-tier CIOs are 17% more likely to have automated proactive threat detection.

The ability to detect unknown threats by their behavior or other characteristics is no longer an option. Zero-day attacks are becoming more common, and 75% of unknown malware detected by FortiSandbox was not found on the VirusTotal tool—which aggregates information from 50 different antivirus vendors.[20] Cutting-edge threat-detection systems utilize artificial intelligence (AI) and machine learning (ML) to understand and detect the characteristics of malware and advanced threats.

7.Top-tier CIOs are 15% more likely to have automated critical security workflows.

Automation of all security processes is increasingly a key to beating threats that move at machine speed. When processes must wait for a human to move them from one step to the next, cyber criminals have time to make their move.

Conclusion

Our research shows that CIOs are intimately involved with cybersecurity at their organizations and have a stake in its success. But some organizations are realizing better results than others. Among the takeaways of our research are seven best practices more commonly practiced by top-tier CIOs. These best practices can fall into the following categories:

Clear communication of the security posture—and the business value of cybersecurity—to the board, the CEO, and the organization at large

A broad and integrated security architecture, covering the entire attack surface with centralized visibility and control, automation of processes, and comprehensive threat intelligence

A strategic approach to sourcing talent, partnering with MSSPs where it makes the most sense

As both IT systems and the threat landscape become immensely more complex, CIOs are increasingly called to take a proactive, strategic approach to security—eliminating silos rather than adding them, simplifying processes rather than complicating them, and being proactive rather than reactive.

"It is becoming harder to manage security within the budget. It takes a lot of analytics to improve efficiency in this area."
– Survey Respondent

References

[1] "Ascent Of The CIO," Forbes Insights, March 23, 2018.

[2] "Mastering the New Business Executive Job of the CIO: Insights From the 2018 CIO Agenda Report," Gartner Executive Programs, accessed March 6, 2019.

[3] "Manifesting legacy, looking beyond the digital era: 2018 global CIO survey," Deloitte Insights, accessed April 3, 2019.

[4] "Ascent Of The CIO," Forbes Insights, March 23, 2018.

[5] Ibid.

[6] "CIO Survey 2018: The Transformational CIO," Harvey Nash and KPMG, accessed March 6, 2019.

[7] Ibid.

[8] Rich Brennen, "The State of the CIO in 2018: A Three-Year Study of a Rapidly Changing Role," Spencer Stuart, February 2018.

[9] "The DNA of the CIO: Opening the Door to the C-Suite," EY, accessed March 6, 2019.

[10] Rich Brennen, "The State of the CIO in 2018: A Three-Year Study of a Rapidly Changing Role," Spencer Stuart, February 2018.

[11] Ibid.

[12] "1Q19 CIO Survey: Macro Beginning to Exert Some Pressure?" Morgan Stanley, April 3, 2019.

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

[14] Steve Vintz, "CFOs Don't Worry Enough About Cyber Risk," Harvard Business Review, December 1, 2017.

[15] E.g., "Anticipating the Unknowns: Chief Information Security Officer (CISO) Benchmark Survey," Cisco, March 2019; "The future of cyber survey 2019: Cyber everywhere. Succeed anywhere." Deloitte, accessed March 28, 2019.

[16] Patrick Spencer, "Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study," Scalar, February 20, 2019.

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

[18] John Edwards, "7 signs you're suffering from burnout—and what to do about it," CIO, October 25, 2018.

[19] Myles F. Suer, "The most important metrics to drive IT as a business," CIO, March 19, 2019.

[20] Based on internal data from FortiGuard Labs.

FORTINET®

www.fortinet.com

May 23, 2019 10:41 AM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2019:Report-The-CIO-And-Cybersecurity:report-cio-and-cybersecurity_DG Folder:report-cio-and-cybersecurity_DG

323524-0-0-EN