FORTINET

REPORT

The IT Infrastructure Leader 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

Cybersecurity Trends for the IT Infrastructure Leader 6

Key Challenges for the IT Infrastructure Leader. 13

Best Practices of Top-tier IT Infrastructure Leaders 16

Conclusion 17

References 18

Executive Summary

The IT Infrastructure Leader and Cybersecurity report from Fortinet demonstrates that cybersecurity is an increasingly important part of what their teams do. This is despite the fact that the CISO is usually a peer to the IT infrastructure leader and leads an adjacent team. The increasing complexity of IT networks, growing sophistication of threat actors, and the rising risks to the business stemming from security issues mean that security responsibilities are being distributed more broadly. Some key takeaways from the report include:

1. **IT infrastructure leaders have security among their top success measurements and have shared—and direct in some cases—responsibility for a variety of security functions.**

2. **IT infrastructure leaders have high confidence in their organizations' risk posture while acknowledging challenges with security tool integration, manual processes, and zero-day threats.**

3. **Ultimately, IT infrastructure leaders' high view of their organizations' security posture is exaggerated at best, as most organizations have experienced a significant number of intrusions, and these events have impacted the business significantly.**

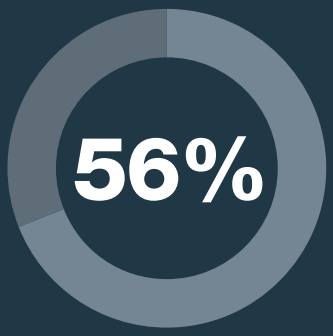
4. **Risk management is clearly the biggest challenge cited by IT infrastructure leaders that results from current cybersecurity trends.**

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. "Top-tier" IT infrastructure leaders are more likely to employ network and security best practices than their "bottom-tier" counterparts:

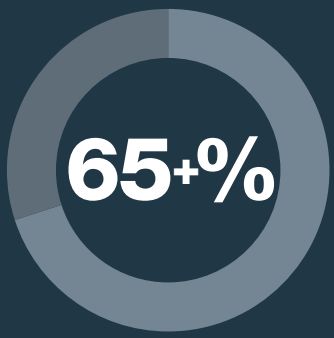
- Deploying an end-to-end, integrated security architecture
- Tracking and reporting basic cybersecurity metrics
- Discussing cybersecurity regularly at the board level
- Integrating SD-WAN networking with the rest of the network infrastructure
- Deploying protection against unknown threats
- Increasing financial investments in cybersecurity

These best practices reflect a holistic approach to cybersecurity that eliminates silos, enables automation, and provides the best protection against advanced threats.

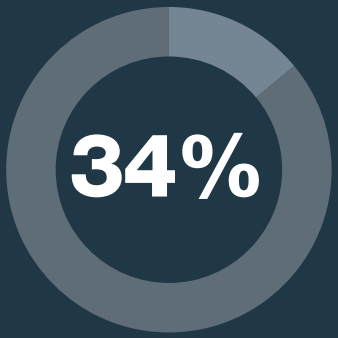
Infographic: Key Findings



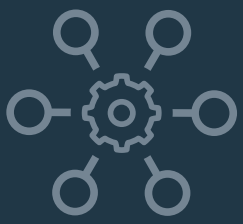
of IT infrastructure leaders **spend more than half of their time** dealing with security.



are directly responsible for **cloud security, SOC, DLP, IoT security, OT security.**



have **cybersecurity risk management** as one of their top three success measurements.



Only **9%** have purchased an **end-to-end, integrated security architecture.**



Yet, **77%+** say they practice ALL 15 security best practices listed.



54% did **NOT see** a cybersecurity **budget increase** in 2019; **23%** saw a **DECREASE.**

88% have **experienced intrusions** in the past 12 months.

26% have seen **6+ intrusions.**

57% had an intrusion that impacted **productivity.**

35% saw an impact on **physical safety.**

419% Top-tier IT infrastructure leaders were **419% more likely** to have an **end-to-end integrated security architecture** than bottom-tier ones, and

89% **more likely** to measure and report **intrusions detected and remediated.**

Introduction

The vice president or director of IT infrastructure is at the center of myriad stakeholders in the enterprise, and must juggle multiple priorities that come from many directions. Digital transformation (DX) is making their job more complex, and is also increasing the urgency of IT infrastructure improvements as organizations try to stay competitive in a rapidly evolving marketplace.[1]

Cybersecurity is an increasingly important part of fulfilling the needs of the business, as disruptions resulting from attacks by cyber actors impact the bottom line more quickly than ever. 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.[2]

While most of the operational side of security falls under the CISO, the IT infrastructure leader has a vested interest in that team's success and—in many cases—a charter to assist them.[3] In particular, security impacts on risk management, network performance, and operating costs are top priorities. Managing these factors is complicated by several trends:

1. ***An expanded attack surface.*** **DX initiatives in progress at most organizations have resulted in larger, more sprawling IT networks,[4] and securing them is increasingly 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 from Internet-of-Things (IoT) devices that often lack adequate security protection.[5] Scrambling to provide protection for these new technology elements, enterprises often find themselves deploying point products, resulting in fragmented visibility and more manual security processes. These trends work against the IT infrastructure leader's charter to improve operational efficiency.**

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,[6] and sensitive data is found in a variety of places and subject to more regulations and security standards. This complexity means that security increasingly needs to be an integral part of network design rather than an add-on. This adds another set of responsibilities to the IT infrastructure leader's already overburdened team.**

3. ***A rapidly changing threat landscape.*** **Cyber criminals are using highly sophisticated approaches[7] and unknown threats are increasing in frequency and scope.[8] And the speed of attacks is accelerating, with exfiltration of corporate data now happening in a matter of minutes.[9] IT infrastructure leaders recognize that automation is necessary to respond to threats that move at machine speed, but achieving full automation requires an integrated security architecture—which most organizations lack.**

As a result, IT infrastructure leaders can no longer afford to operate in a separate silo from the cybersecurity team, with infrequent coordination and communication.[10] They must collaborate with CISOs to build a strategic, comprehensive solution that provides a proactive stance toward an increasingly dire threat landscape.

Methodology for This Study

The IT Infrastructure Leader and Cybersecurity report is based on a survey conducted in March 2019. Respondents were all at the director and vice president job grades and had either IT infrastructure or IT operations in their job titles. Our respondents come from companies with more than 2,500 employees in a variety of industries, including technology, manufacturing, financial services, and retail.

This study utilizes data from the survey to identify several current trends around the IT infrastructure leader's role. Next, we analyze the freeform answers that respondents gave to several open-ended questions about their key challenges, to get a picture of what impacts their daily work. Finally, we 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 best practices more likely to be practiced by "top-tier" IT infrastructure leaders.

Cybersecurity Trends for the IT Infrastructure Leader

Trend: IT infrastructure leaders occupy senior positions in their organizations and have significant responsibility for cybersecurity.

Given their job grades and the importance of their function, it is not surprising that IT infrastructure leaders report primarily to senior executives—the CEO or CIO in nearly three-quarters (73%) of cases (Figure 1). 7% of IT infrastructure leaders report directly to the board of directors. Most are peers of the CISO, who also most commonly reports to the CEO, CIO, or board.

Despite the fact that the CISO typically leads a separate team, IT infrastructure leaders report that they spend a significant amount of time dealing with security (Figure 3). In all, 94% say they spend more than one-quarter of their time on security, while 56% relate that more than half of their time is spent on cybersecurity responsibilities.

At first glance, it might be surprising that a majority of respondents spend more than half their time on security considering that they lead a team adjacent to that of the CISO. But it is less surprising when one looks at the security responsibilities of their teams (Figure 4). Eight in 10 respondents are responsible for cybersecurity awareness training, and solid majorities (65% or more) are directly responsible for things like cloud security, the security operations center (SOC), data loss prevention, data privacy, IoT security, and operational technology (OT) security. While a closer look likely reveals that many of these responsibilities are shared between the IT infrastructure leader and the CISO, it is clear that security is an integral part of the infrastructure team's work.



Figure 1: IT infrastructure leaders' direct supervisor.

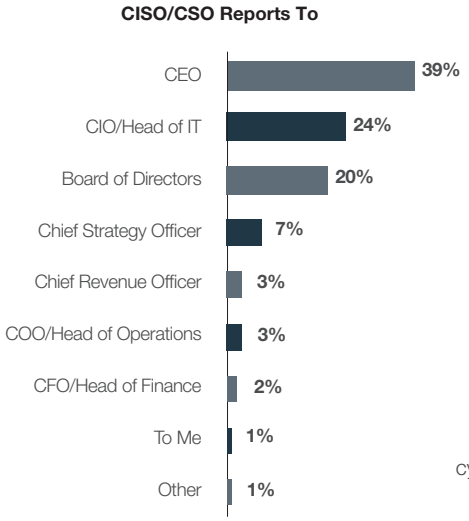


Figure 2: CISO's direct supervisor in IT infrastructure leaders' organizations.

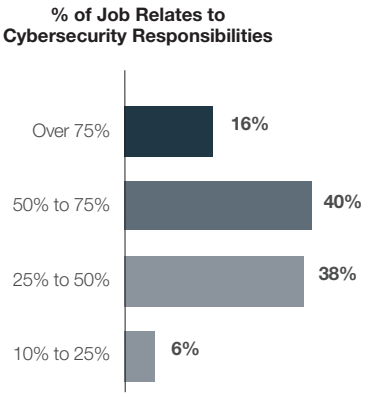


Figure 3: Percentage of job relating to cybersecurity responsibilities for IT infrastructure leaders.

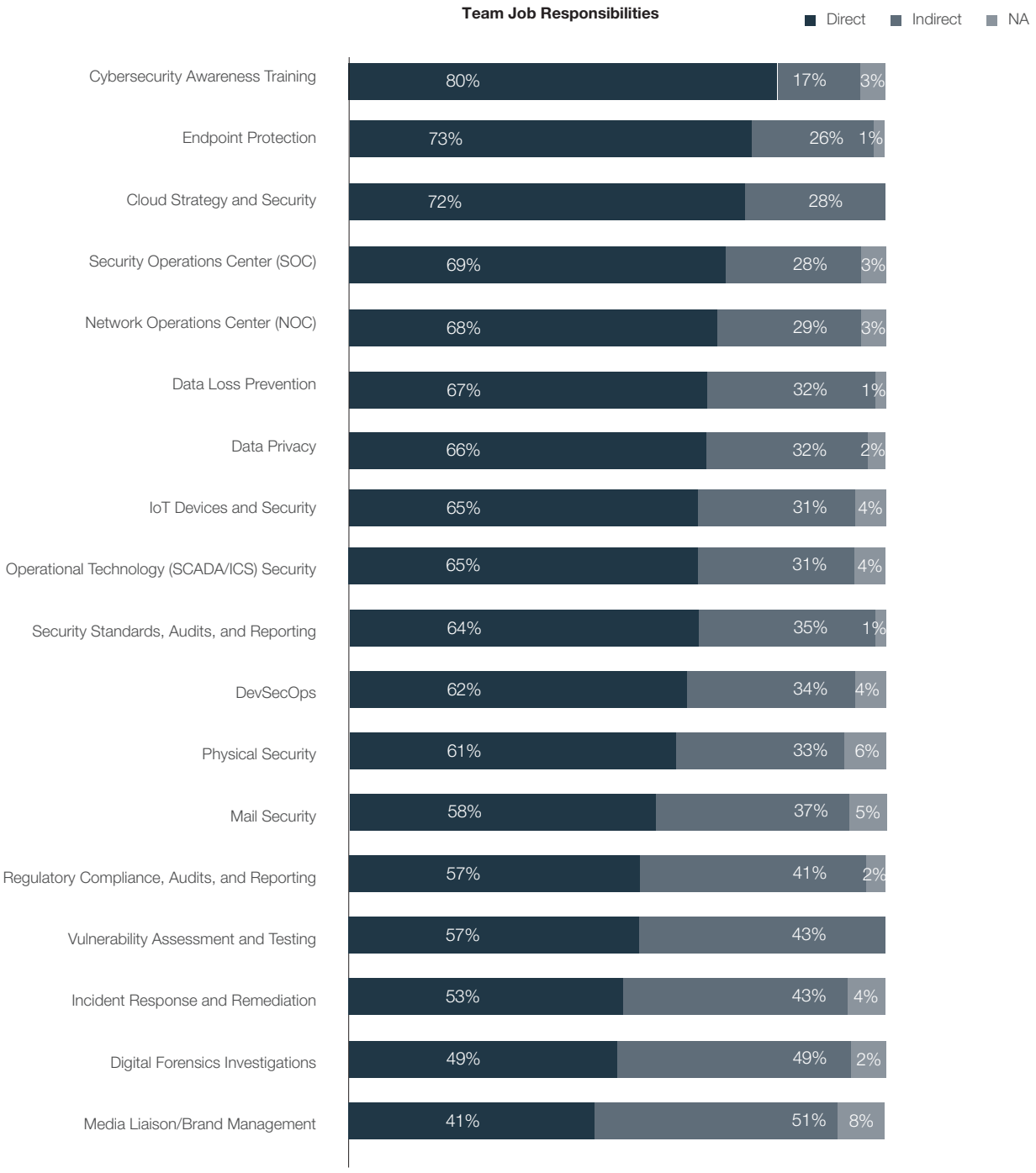


Figure 4: Security responsibilities of IT infrastructure leader's team.



"An expanded attack surface means that I am delegating more and have hired additional hourly IT tech workers."

– Survey Respondent

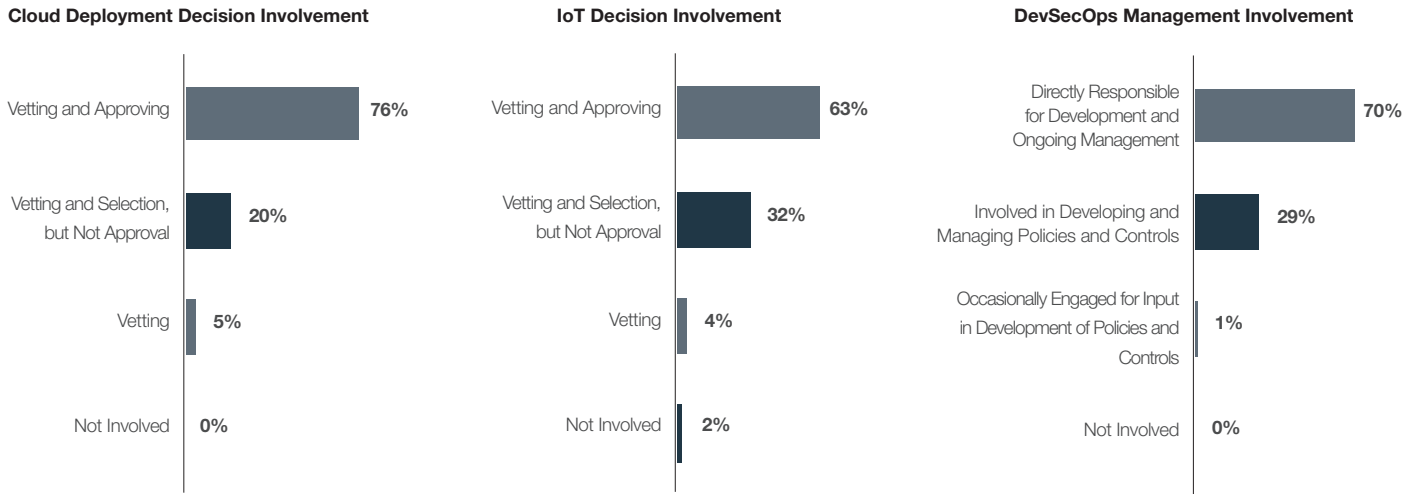


Figure 5: IT infrastructure leaders' responsibilities with cloud, IoT, and DevSecOps deployments.

Trend: Security is a significant part of IT infrastructure leaders' success measurements, but many do not track and report key security metrics.

When asked to list the top three success measurements used in their own performance reviews, IT infrastructure leaders named cybersecurity risk management more than any other metric (Figure 6). And cybersecurity cost and operational efficiencies was listed most often as the number one success measurement. In general, cybersecurity-related metrics were more commonly cited than other factors that might be seen as more infrastructure related, such as network uptime, speeding time to market with DevOps, and infrastructure consolidation. This is another indicator that security has become a front-of-mind topic in both the boardroom and the C-suite.

While the IT infrastructure leader's performance is tied heavily to cybersecurity, the organizations they work for are less likely to measure and report some basic cybersecurity metrics (Figure 7). Fewer than half measure tangible risk management outcomes, vulnerabilities found and blocked, and productivity gains from security measures. Half of respondents measure intrusions detected and remediated, and small majorities measure the cost and financial implications of security programs.

Trend: IT infrastructure leaders see their organizations as leaders in digital transformation, but struggle with security integration.

More than half of respondents (56%) see their organizations as early movers in DX, with extensive cloud, IoT, and mobile adoption (Figure 8). Another 38% say they are in the midst of DX, leaving just 6% who say they have not yet started the DX process. DX is defined in a variety of ways[11] and human nature is to exaggerate one's leadership status. However, it is clear that the three technologies listed in the question—cloud, IoT, and mobile—are widely adopted in today's enterprises.

However, IT infrastructure leaders are less confident when it comes to their security architecture. When asked to identify their top three security issues, it is not surprising that IT infrastructure leaders would most commonly cite performance degradations due to security issues (Figure 10). But tied for a close second is a lack of end-to-end integration.

In fact, when asked to describe their security architecture, only 9% of respondents report that they have purchased an end-to-end, integrated security solution (Figure 9). While a majority (56%) are trying to integrate the disparate security solutions they own or have already integrated some of them, it is unclear how successful these efforts will be at achieving full integration.

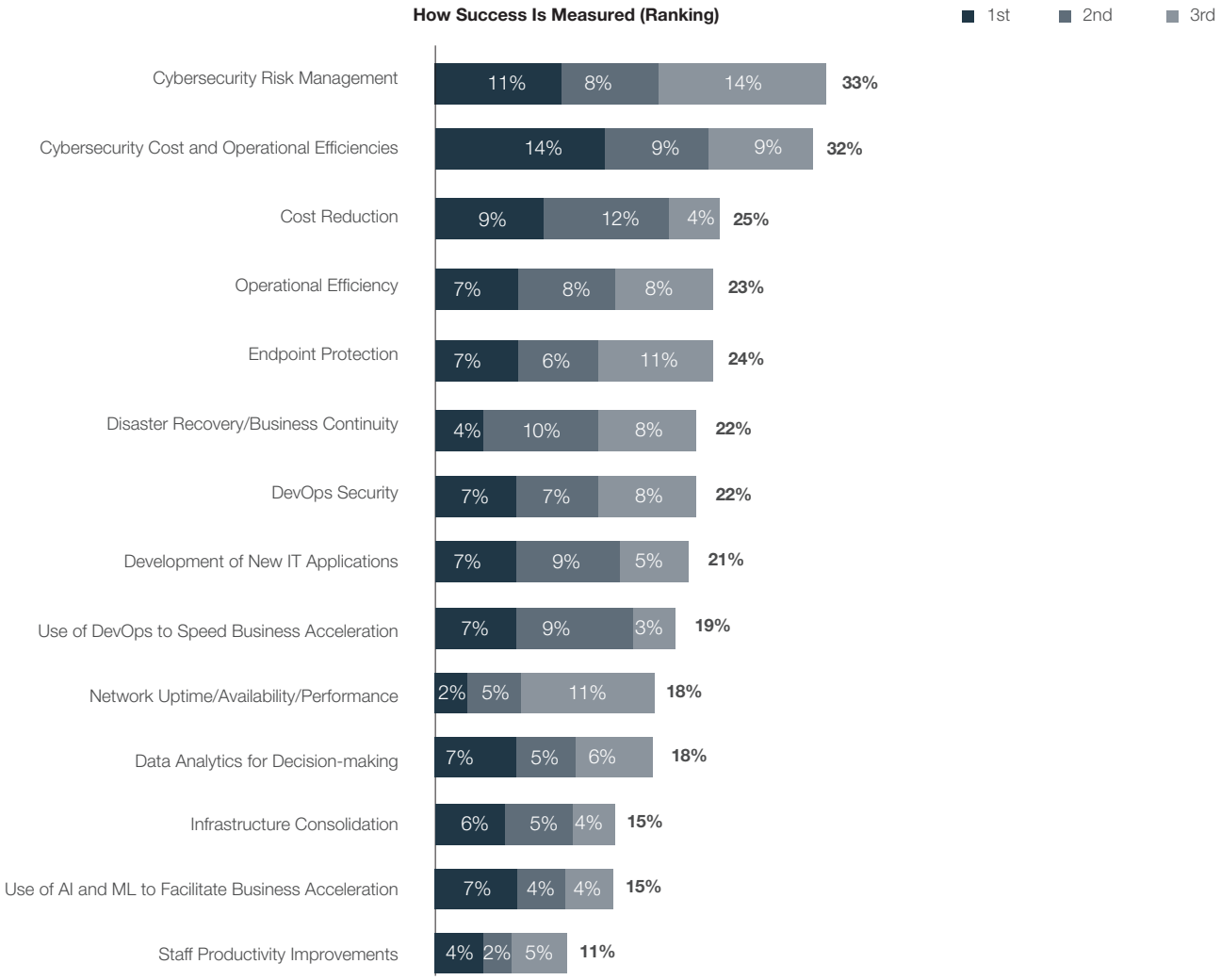


Figure 6: Top three success measurements for IT infrastructure leaders.

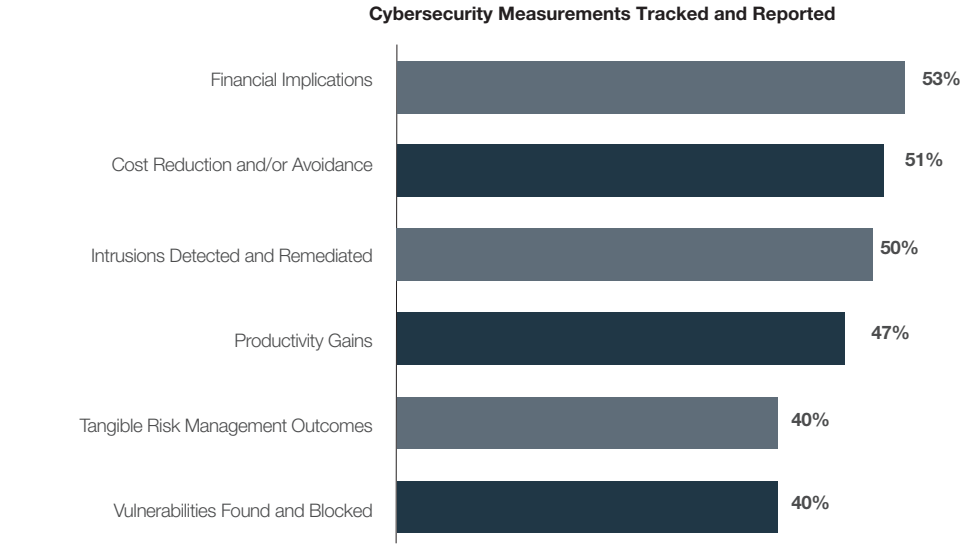


Figure 7: Cybersecurity measurements tracked and reported at IT infrastructure leaders' organizations.

Ultimately, more than one-third (35%) of respondents admit that their practice is to manage siloed point products—and apparently have no plans to integrate them. This not only creates more manual work for the security and infrastructure teams but also makes an organization vulnerable to sophisticated threats that move at machine speed.[12]

Insufficient funding to make major changes to security infrastructure may be one factor in this lack of progress with integration (Figure 11). More than half of respondents did not see a cybersecurity budget increase in 2019, and nearly one-quarter (23%) of respondents actually saw a budget reduction.

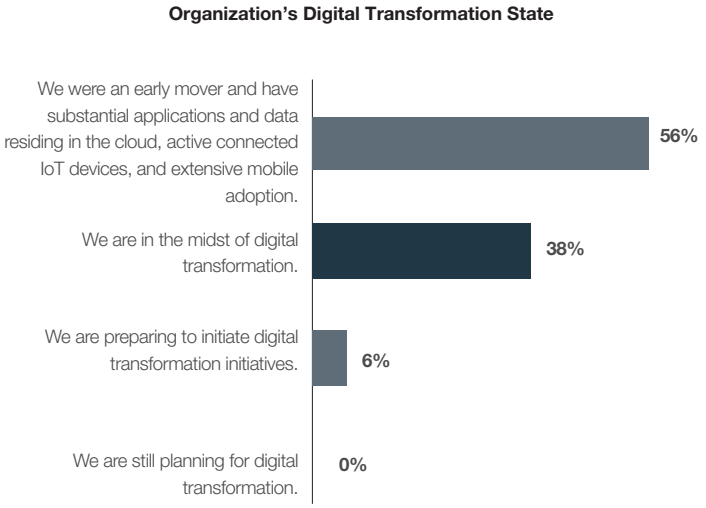


Figure 8: IT infrastructure leaders' digital transformation state.

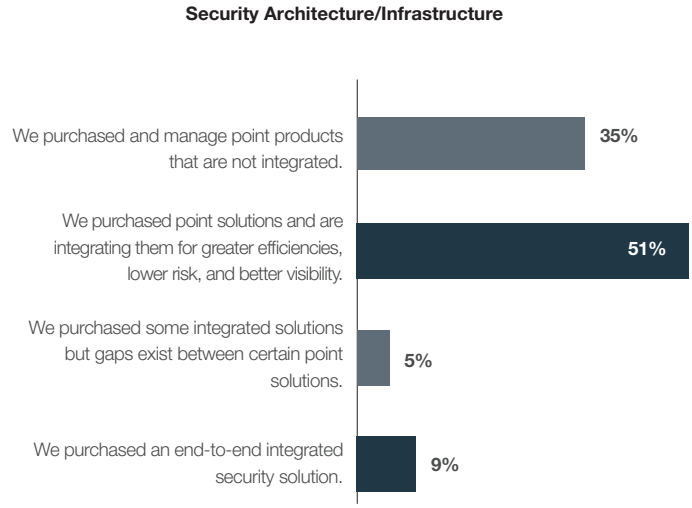


Figure 9: Security architecture at IT infrastructure leaders' organizations.

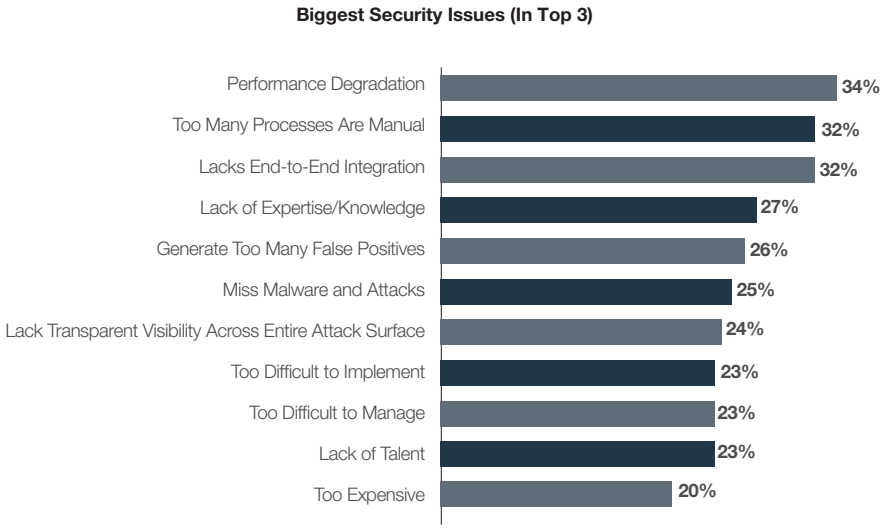


Figure 10: Security issues in the top three according to IT infrastructure leaders.

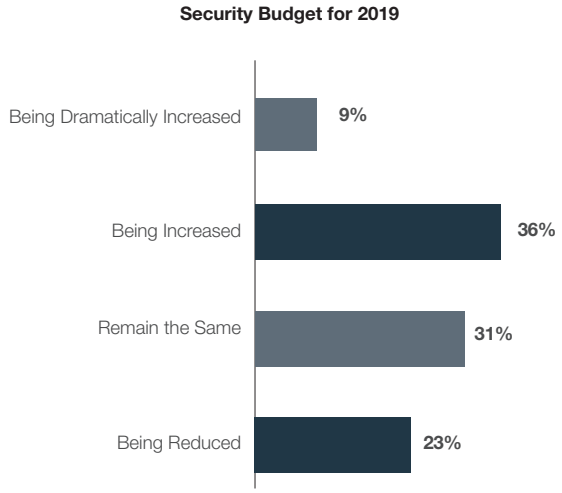


Figure 11: Security budget changes for 2019 at IT infrastructure leaders' organizations.

Trend: IT infrastructure leaders have an optimistic view of their security posture, but have too many manual security processes.

More than three-quarters of respondents claim they have full visibility and control and can measure risk and align it with security programs (Figure 12). And when asked about 15 different security best practices (Figure 13), more than three-quarters agreed or strongly agreed that they are following all of them. And 85% of respondents say they have an incident response and remediation plan in place.

Looking at these responses in isolation, it would appear that a large majority of organizations have "arrived," and that these companies do not need to make any further improvements to their security technology and processes. This is surprising given the aforementioned limited progress toward integration.

Respondents do admit that there is room for improvement in a handful of responses. For example, in Figure 12, only 43% feel comfortable about protecting against both known and unknown threats—an indication that they are concerned about their ability to thwart zero-day attacks. And in Figure 10, too many manual processes (32%) is another commonly cited security issue along with a lack of integration.

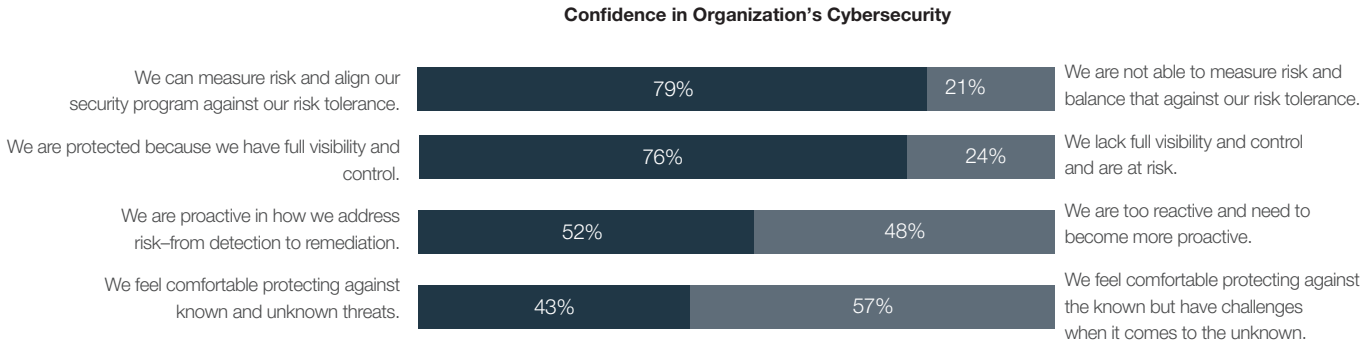


Figure 12: IT infrastructure leaders' confidence in their organization's cybersecurity posture.

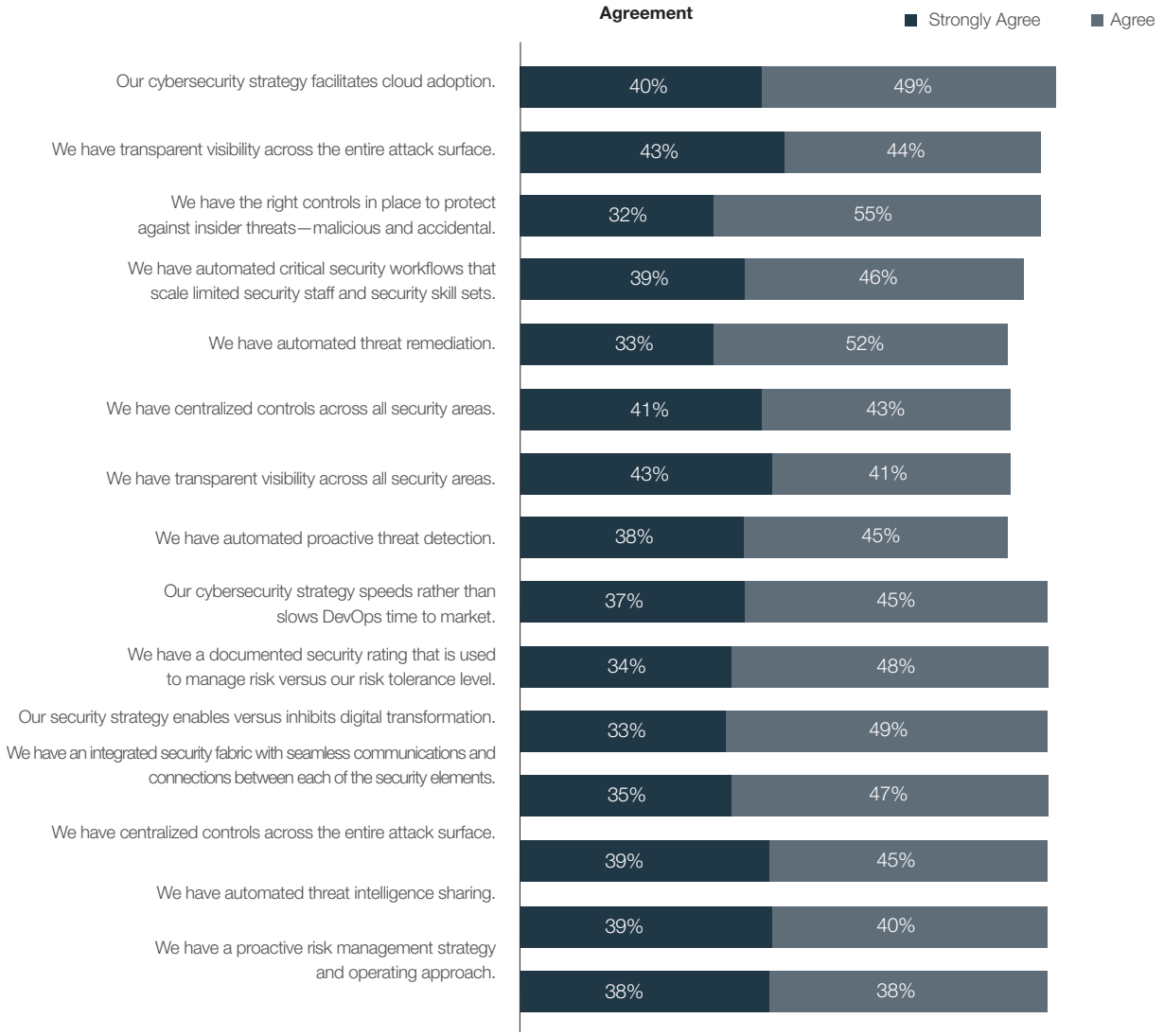


Figure 13: Adherence to security best practices at IT infrastructure leaders' organizations.

Trend: Most IT infrastructure leaders have experienced multiple intrusions in the past 12 months, and these have had a tangible impact on business.

The best measure of whether organizations need to make improvements to their security technology and practices is whether they are experiencing intrusions. Among the IT infrastructure leaders who responded to our survey, only 12% have not had any intrusions in the past 12 months (Figure 14). Another 19% experienced one or two intrusions, meaning that more than two-thirds of respondents have endured multiple security events. In fact, more than one-quarter (26%) had six or more intrusions in the past year.

The types of attacks varied widely, with a majority of respondents experiencing malware and more than 30% seeing spyware, phishing, ransomware, and breaches of mobile devices. The impact of these intrusions was not trivial. A solid majority of respondents (57%) reported that at least one intrusion impacted employee productivity, and more than one-third of respondents have seen intrusions that impacted brand awareness, data loss, revenue, and even physical safety.

These results make it clear that IT infrastructure leaders' optimistic view of their security posture and their adherence to best practices is unfounded—or at least exaggerated.

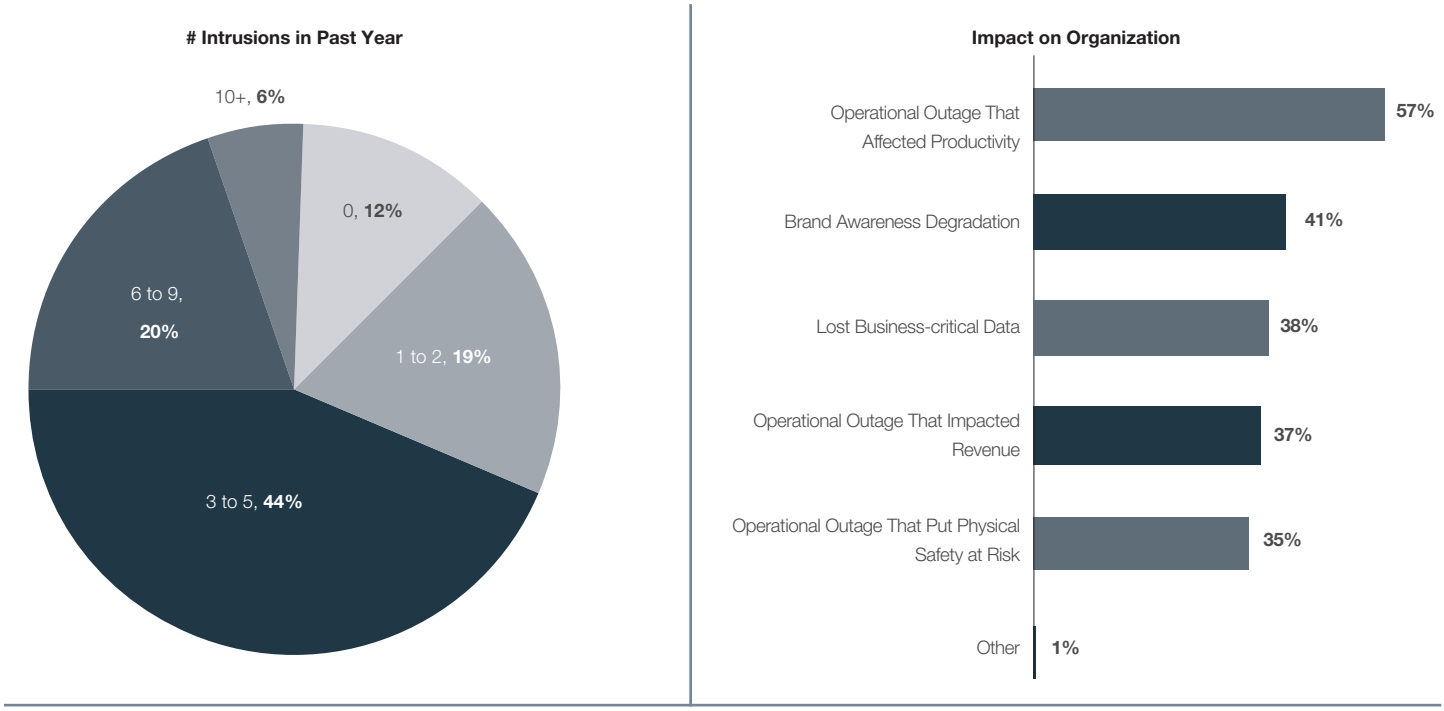


Figure 14: Number and type of intrusions in the past 12 months, and their impact on the organization.

Key Challenges for the IT Infrastructure Leader

Our survey 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 IT infrastructure leaders. The questions asked about challenges stemming from three high-level security trends: an expanding attack surface, increased complexity, and a more advanced threat landscape.

Challenge: Risk management is the biggest challenge of today's security landscape from the IT infrastructure leader's vantage point.

Risk management is by far the most-cited category of challenges for IT infrastructure leaders and is cited by a majority of respondents across all three security trends (Figures 15-17). It is interesting that risk management is also the most commonly cited success measurement for these professionals, and this is potentially a factor in the challenges they see. One positive aspect of these responses is that IT infrastructure leaders seem to view security from a more strategic, risk management lens rather than a more tactical, product-based view.

Challenge: The expanding attack surface increases complexity and opens new doors for hackers.

When asked about the impacts of an expanding attack surface (Figure 15), respondents most commonly cited complexity and the need to defend against hackers as the primary challenges. DX means that companies are adopting a variety of networking technologies, increasing their presence in multiple clouds, and adding many IoT devices to their networks. Securing these new technologies complicates the security architecture, and any gaps in that security invite intrusions.

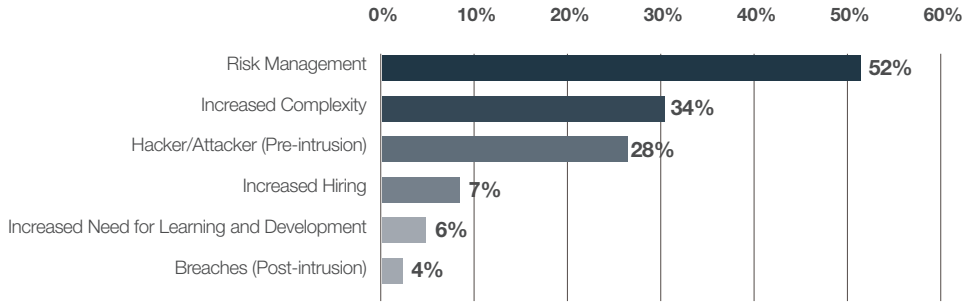


Figure 15: Challenges for IT infrastructure leaders from an increased attack surface.

Challenge: Security complexity challenges risk management capabilities or IT infrastructure leaders.

Security complexity is largely the result of siloed security tools that are not integrated. This results in manual security workflows that impact operational productivity, reduce visibility, and hamper security. For IT infrastructure leaders, the most-cited result besides risk management is the increased challenge in dealing with this complexity (Figure 16).

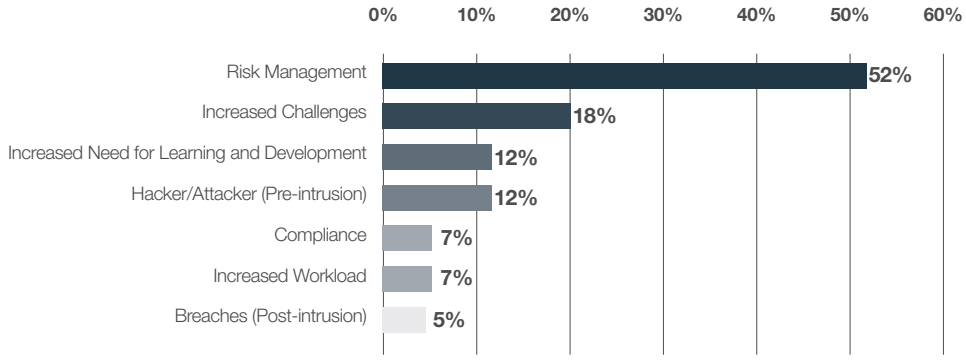


Figure 16: Challenges for IT infrastructure leaders from increased security complexity.



"The increasing complexity of security has forced me to rely more on good team members to help me make better decisions."

– Survey Respondent

Challenge: A more advanced threat landscape brings the need for more training and development.

In a world where threat actors are using the most advanced digital strategies—including artificial intelligence (AI), machine learning (ML), ad DevOps—to create ever-evolving attacks,[13] IT infrastructure leaders see a significant need for more learning and development—both for the IT team and for the full employee population. The cybersecurity and IT infrastructure teams must stay up to speed on the latest developments in the threat landscape, and employees must learn to practice the best security hygiene—and understand why doing so is important. This ratchets up pressure on IT infrastructure leaders; a majority struggle to protect against unknown threats.

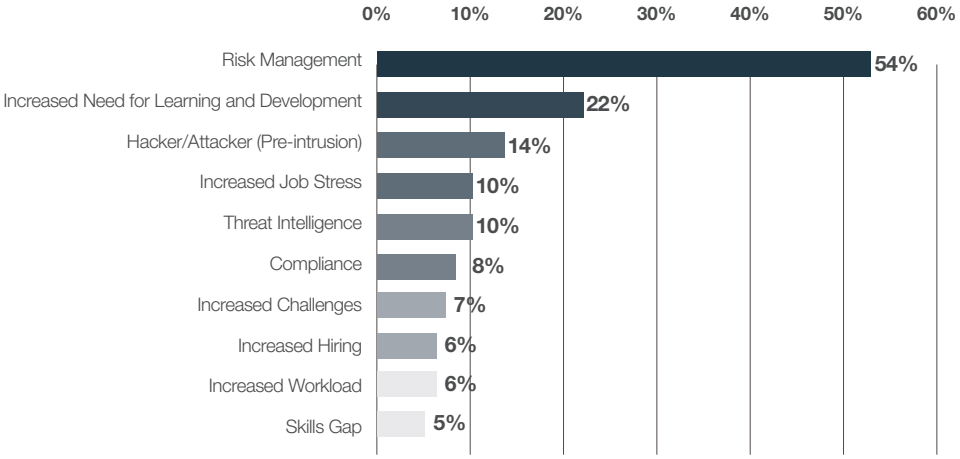


Figure 17: Challenges for IT infrastructure leaders from an increased advanced threat landscape.

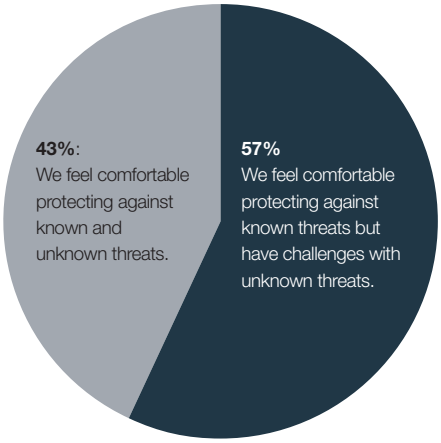


Figure 18: IT infrastructure leaders on protecting against known and unknown threats.



"I have more systems to monitor now than at any other time in the past 10 years."

– Survey Respondent

Best Practices of Top-tier IT Infrastructure Leaders

As discussed, only 12% of IT infrastructure leaders reported zero intrusions in the past year, while more than twice that number—26%—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 IT infrastructure leaders were more likely to employ:

1. Top-tier IT infrastructure leaders are more than five times as likely to have an end-to-end, integrated security solution.

While only 9% of respondents reported having a fully integrated architecture, most of those who do are in the "top tier," with no intrusions in the past year. Specifically, top-tier organizations are 419% more likely to have such an infrastructure than bottom-tier ones.

2. Top-tier IT infrastructure leaders are 89% more likely to do regular measurements on intrusions detected and remediated.

While measuring and reporting intrusions might seem obvious, only half of our respondents are doing so. Top-tier organizations are nearly twice as likely to adhere to this best practice.

3. Top-tier IT infrastructure leaders are 30% more likely to have DevOps security as one of their primary success measurements.

As the adage goes, what gets measured gets improved. IT infrastructure leaders with no intrusions in 12 months are 30% more likely to have DevSecOps among the top three metrics in their performance reviews.

4. Top-tier IT infrastructure leaders are 30% more likely to have cybersecurity as a standing topic at all board meetings.

The media has proclaimed that cybersecurity is now a boardroom topic, but some boards have gotten the message more fully than others. Top-tier IT infrastructure leaders are more likely to work at organizations where the board discusses the topic at every meeting.

5. Top-tier IT infrastructure leaders who have an SD-WAN network are 23% more likely to have it integrated into the broader network for full visibility.

Not all respondents have adopted SD-WAN, but for those who have, the best practice is for that part of the network to be integrated with existing network elements. Full, transparent visibility is key to providing optimal security.

6. Top-tier IT infrastructure leaders are 21% more likely to be confident in their protection against unknown threats.

Organizations that have access to threat-intelligence sources powered by AI and ML, and use technologies like sandboxing, are more likely to block zero-day threats. Blocking these threats reduces the likelihood that an adversary will successfully infiltrate the network.

7. Top-tier IT infrastructure leaders are 21% more likely to have seen a cybersecurity budget increase in the past year.

The fact that a majority of respondents did not see a cybersecurity budget increase for 2019 was something of a surprise. However, organizations that are increasing their investment in security this year are more likely to find themselves in the top tier.

Conclusion

While the IT infrastructure and cybersecurity teams worked in silos not too many years ago, our research shows that this is no longer the case. As security protection increases in importance to the functioning of the business, IT infrastructure leaders share distinct security responsibilities with the CISO's team at many organizations. This makes sense: today's advanced threats require a coordinated approach in which security is an integral part of IT infrastructure.

While respondents have a high view of where their organizations are regarding security, their frequent experience of damaging intrusions paints a different picture. IT infrastructure leaders will do well to learn from the best practices of organizations that have successfully avoided intrusions. These include:



Investing in an end-to-end, integrated security and networking architecture with full visibility and centralized control



Measuring and reporting basic cybersecurity metrics, enabling the development of strategies for improvement



Bolstering protection against unknown threats



Making cybersecurity a priority for the organization—including the board of directors

As IT infrastructure leaders share more and more responsibility for security, the best approach they can take is to simplify operations through integration and automation of security practices. This enables a proactive stance toward threats and a risk management-based strategy to protect an organization's most important assets.

References

[1] Clint Boulton, "What is digital transformation? A necessary disruption," CIO, May 31, 2019.

[2] Kelly Bissel, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, March 6, 2019.

[3] Arul Elumalai, et al., "Ten trends redefining enterprise IT Infrastructure," McKinsey & Company, November 2017.

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

[5] Saumitra Das, "IoT Security's Coming of Age Is Overdue," Dark Reading, February 4, 2019.

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

[7] 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.

[8] According to internal Fortinet 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.

[9] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[10] Sandra Gittlen, "How to boost collaboration between network and security teams," Network World, December 21, 2018.

[11] Clint Boulton, "What Is digital transformation? A necessary disruption," CIO, May 31, 2019.

[12] Dave Barton, "Automation: Moving Security from Human to Machine Speed, and All its Implications," Security Magazine, May 28, 2019.

[13] Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018.

FORTINET

www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

August 18, 2019 6:38 PM

Macintosh HD:Users:ckluck:Documents:FORTINET_ck:2019:report-VP-IT-Infrastructure:R2:Report-VP-IT-Infrastructure-R2

333437-0-0-EN