FORTINET

REPORT

Cybersecurity and the Network Engineering and Operations Leader

A Report on Current Priorities and Challenges

Table of Contents

Executive Summary

The "Cybersecurity and the Network Engineering and Operations Leader Report" looks closely at the role of network engineering and operations leaders from the standpoint of their core job responsibilities and measurements and security strategy and priorities. Following are some of the key takeaways from the analysis:

- **The network engineering and operations leader is highly visible within the organization, especially in larger enterprises.**
- **Network engineering and operations leaders are increasingly responsible for cybersecurity activities in addition to their other duties. However, their supervisors emphasize operational success metrics over cybersecurity metrics when evaluating them.**
- **The majority of network engineering and operations leaders lack fully integrated security solutions.**
- **Most network engineering and operations leaders use MSSPs to supplement their internal security resources.**

Given these trends and challenges, we analyzed the data more deeply and identified a subset of respondents who reported no intrusions in the past year that we deem top-tier security organizations. At the same time, we pinpointed another subset that had more than six intrusions in the same time frame and deemed them bottom-tier security organizations.

The differences in practice between these two groups are instructive in that they highlight the traits of top-tier network engineering and operations leaders versus those who struggle. In a nutshell, these best practices reflect a holistic, integrated approach to network security that eliminates silos, delivers highly available, resilient network performance, enables automation of security response, and provides the best protection against advanced threats.

Infographic: Key Findings

81%

are directly responsible for **cloud strategy and security.**

35%

report directly to the **CIO.**

34%

list **network performance/ uptime** as their #1 performance measure.

83% had at least one intrusion in the past 12 months.

59%

have had **3+** intrusions.

31%

have had **6+** intrusions.

52% find it more difficult to manage risk because of the expanding threat surface.

44% have challenges protecting against unknown threats.

90%

lack an end-to-end **integrated security system.**

74%

use **MSSPs** to supplement their security staff.

Best-in-class network engineering and operations leaders are:

- **4x** more likely to have purchased an **end-to-end integrated security solution**
- **3x** less likely to have **their budgets reduced**
- **88%** more likely to be **measured on network performance/uptime**
- **88%** more likely to be **measured on vulnerabilities remediated**
- **88%** more likely to be concerned about the operational inefficiencies of **false positives**
- **72%** more likely to **track and report vulnerabilities found and blocked**
- **67%** more likely to **report directly to the CIO**

Introduction

The network is a key enabler for the modern business. Even so, the network has often been overshadowed by high-profile disruptive technologies such as digital experiences, cognitive, and cloud. All too often, executives have taken the network infrastructure for granted in their strategic planning.[1]

That perception is changing. Thanks to the proliferation of mobile devices, Internet-of-Things (IoT) sensors, serverless computing, and exploding volumes of shared data, high-performance, reliable networking is becoming essential to drive organizational success and build brand equity. As a result, companies are investing heavily in the network. In a recent survey of IT leaders, 44% report that upgrading their networking foundation is a top priority for 2019.[2]

As the role of the network gains organizational visibility, so does the role of the network engineering and operations leader. A growing number of organizations now grade the network engineering and operations leader—typically a vice president or director—on cybersecurity metrics in addition to traditional network metrics such as performance, reliability, availability, and resiliency. This shift is consistent with the growing awareness at every level of the organization of the strategic importance of security.[3] More and more, the concept of a siloed security function is giving way to an "all-hands-on-deck" mentality in which security is everyone's job.

Beyond these internal expectations, the network engineering and operations leader also confronts a more virulent threat landscape that poses unique challenges. For one thing, cloud applications, IoT, mobility, and wireless connectivity are expanding the attack surface and thereby complicating security strategies. In addition, rapidly changing advanced threats ratchet up the pressure on network engineering and operations teams that are already struggling to keep up due to budgetary constraints and a lack of security skills. Finally, increased security complexity leaves gaps in protection and requires scarce staff time to configure, manage, and maintain the security infrastructure.

Methodology for This Study

This report is based on a survey of network engineering and operations leaders at organizations with more than 2,500 employees. Respondents come from a variety of industries, including technology, manufacturing, retail, and consumer goods.

The report has three primary sections. The **first** one identifies **current trends** that characterize the position, job duties, and attitudes of network leaders. The **second** one analyzes the **key challenges** network engineering and operations leaders are facing. The **final** one compares **top-tier network engineering and operations leaders** (i.e., those whose organizations reported no intrusions in the past year) **versus bottom-tier counterparts** (i.e., those with the most reported intrusions in the past year) and identifies the most **notable traits** of top-tier network leaders.

> **"Because of the advanced threat landscape, we need to deploy advanced security features faster than our team can handle and at greater cost than our budget can afford."**
> **– Survey Respondent**

Cybersecurity Trends Per the Network Engineering and Operations Leader

Trend: The network engineering and operations leader is highly visible within the organization, especially in larger enterprises.

All the network engineering and operations leaders in the survey report to C-level executives. However, only 38% report to a technical executive—namely, the CIO. The remaining 62% report to operational executives such as the CEO, COO, and CFO (Figure 1). (For CISOs, the network engineering and operations leader is typically a peer—either in an adjacent department or as an intradepartmental colleague when both report to the CIO.[4])

When organization size is considered, the reporting lines change significantly. Network engineering and operations leaders in enterprises with more than 10,000 employees are 50% more likely to report to the CEO as those in smaller companies (Figure 2). This finding suggests that the larger the enterprise, the more strategic value is placed on the network.[5] Thus, in these scenarios, network engineering and operations leaders are more likely to report to the CEO due to network performance and availability being tethered to business operations.

However, reporting to the CEO as opposed to the CIO may not be in the organization's best interest. A comparison between the top- and bottom-tier network leaders, as measured by the number of intrusions, shows that the most successful network engineering and operations leaders are 67% more likely to report to the CIO (see "Best Practices of Top-tier Network Engineering and Operations Leaders" below for a more complete discussion of this finding).

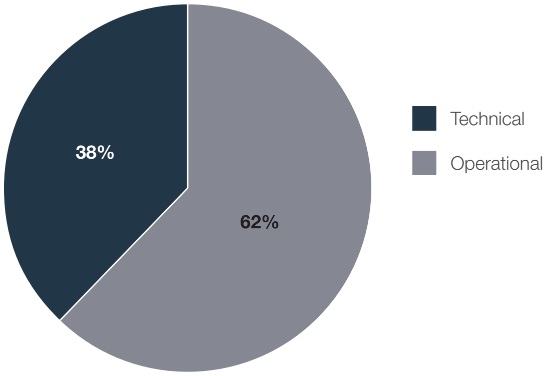

Figure 1: Reporting lines for network engineering and operations leaders across the full survey.

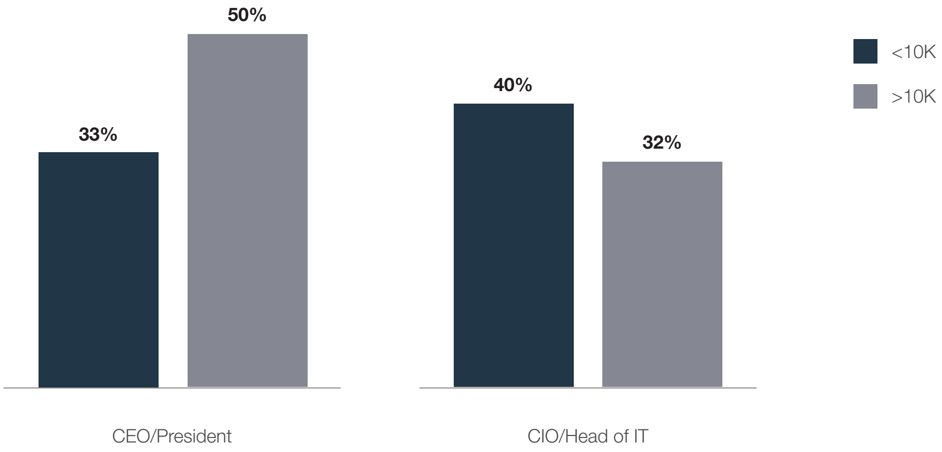

Figure 2: Reporting lines by number of employees in the organization.

Trend: Network engineering and operations leaders are increasingly responsible for cybersecurity.

Somewhat surprisingly, eight of the network leader's top 10 job responsibilities relate to security as opposed to network engineering and operations (Figure 3). Cloud strategy and security tops the list (81%), which is consistent with the widespread adoption of cloud (83% of enterprise workloads will be in the cloud by next year).[6] The next two most commonly cited responsibilities are operational technology (79%) and network operations center (75%), the only operational tasks in the top 10 skills. The remaining seven are security-related, including data privacy (75%), security operations center (72%), and data loss prevention (70%).

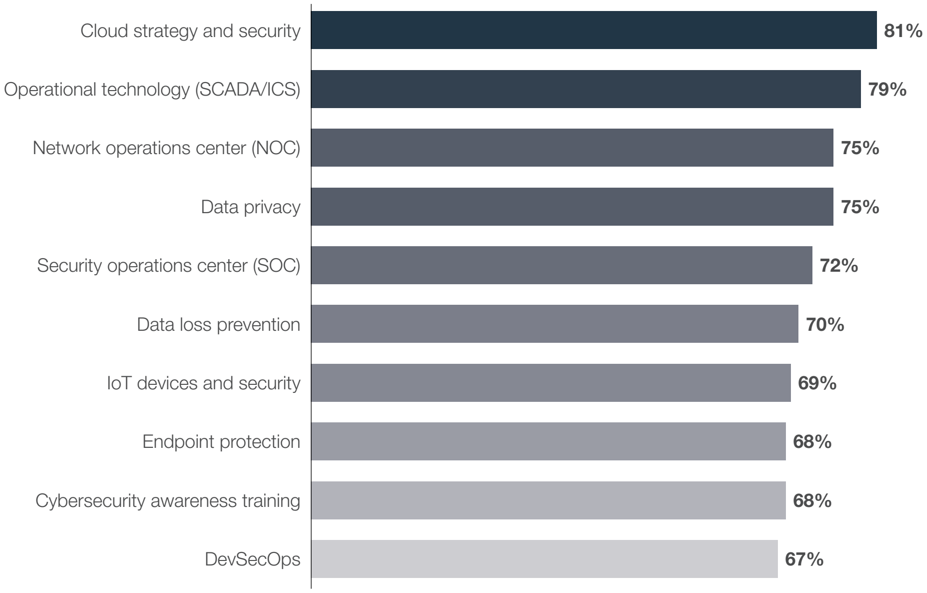

Figure 3: Top responsibilities for network engineering and operations leaders.

Trend: Organizations emphasize operational success metrics over cybersecurity metrics when evaluating network engineering and operations leaders.

In an interesting twist, the preponderance of cybersecurity responsibilities discussed above is not mirrored in the success metrics executives use to grade their network engineering and operations leaders. Three of the top five success metrics relate to network operations, including network performance/uptime (34%), cost reduction (32%), and staff productivity improvements (29%). The most commonly mentioned cybersecurity metrics are DevOps security (31%) and risk tolerance and reporting (29%) (Figure 4).

The discrepancy between areas of responsibility and success metrics lends itself to several interpretations. The **first** is organizational inertia. Executives may be slow to modify the traditional set of operational success metrics to reflect the organization's new emphasis on cybersecurity as an integral part of the network leader's charter. If this explanation is correct, then over time, these supervisors will likely balance the relative weighing of cybersecurity responsibilities and success metrics.

Depth of technical knowledge is a second possible explanation. To explore this **second possibility**, we can compare the success metrics of the network engineering and operations leader to those of the security architect.[7] Three of the network engineering and operations leader's top four metrics also appear in the security architect's list: DevOps security (37% for the security architect versus 31% for the network leader), vulnerabilities found (17% versus 24%), and intrusions stopped (14% versus 20%) (Figure 5).

At the same time, however, the success metrics for the network engineering and operations leader lack four of the top five success metrics in the security architect's list: integration of the security infrastructure (32%), centralized security controls (30%), automation of security workflows (29%), and full visibility across the security infrastructure (27%). The likely explanation here is that developing this fivefold set of evaluation criteria requires a deep understanding of cybersecurity architectures, something operational executives who supervise network engineering and operations leaders are unlikely to possess. In contrast, nearly two-thirds (66%) of security architects report to a security executive, individuals with the training and experience to understand and use more complex cybersecurity criteria to evaluate their direct reports.

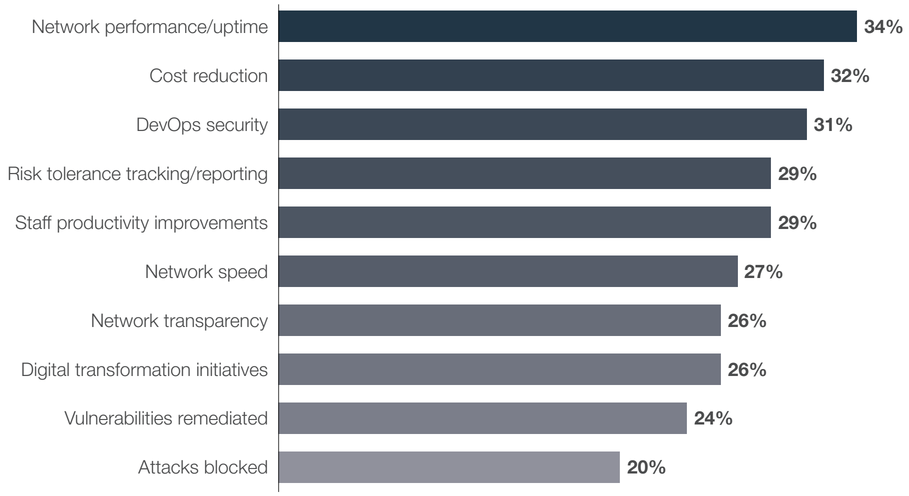

Figure 4: Success metrics for network engineering and operations leaders (blue = security-related).

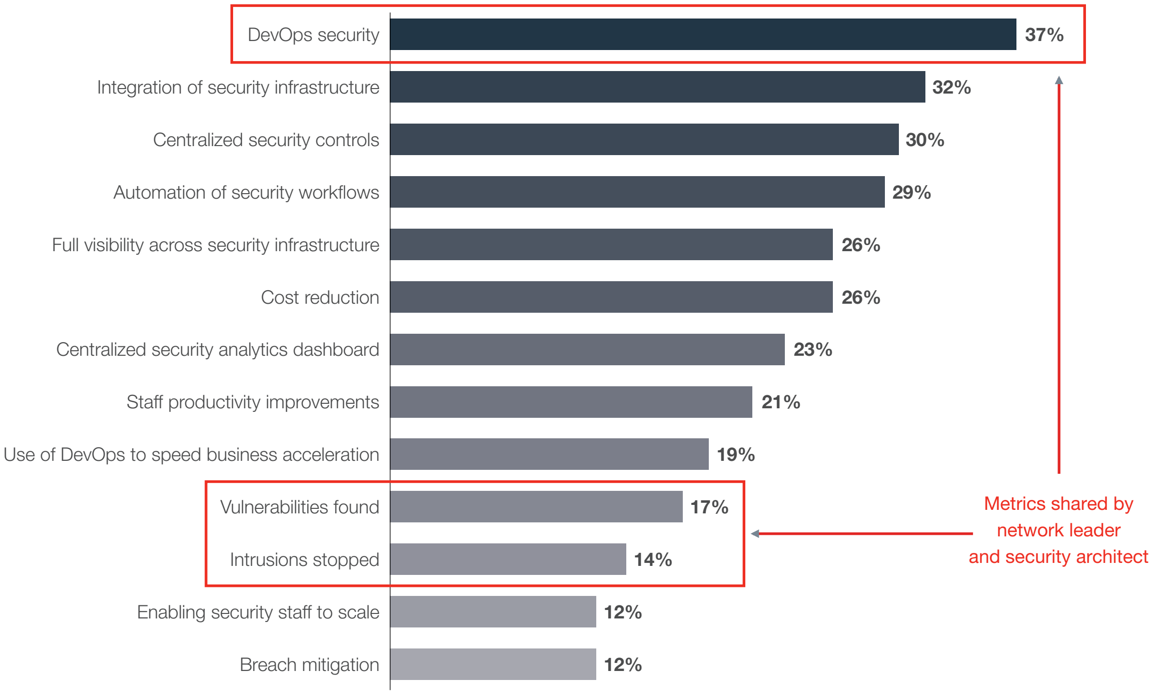

Figure 5: Success metrics for security architects that align with those listed by network engineering and operations leaders.

Trend: Network engineering and operations leaders are key decision-makers for cloud and IoT deployments.

Digital transformation (DX) is impacting more than 8 out of 10 enterprises: 53% were early movers in DX and an additional one-third (33%) are in the midst of transformation projects (Figure 6).

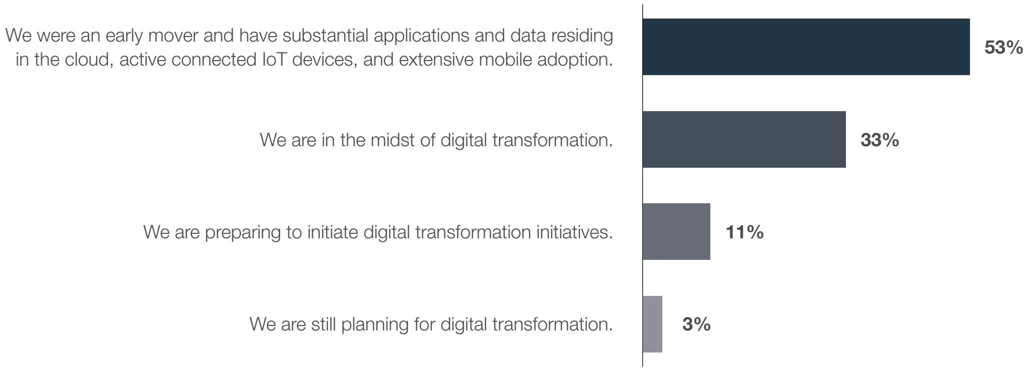

Figure 6: Network engineering and operations leaders' involvement in DX initiatives.

As a result of these DX activities, most of the organizations either now have or will soon have substantial applications residing in the cloud as well as IoT devices connected to their networks. Network engineering and operations leaders are involved in making decisions when it comes to DX-driven technology deployments: more than three-quarters (78%) vet and approve cloud initiatives (Figure 7), while almost 7 in 10 (68%) do so for IoT projects (Figure 8).

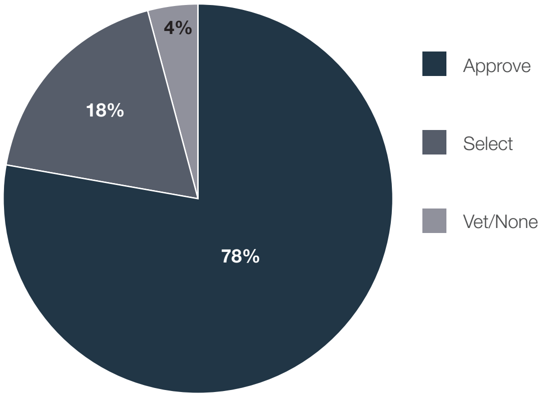

Figure 7: Network engineering and operations leaders' level of involvement in cloud deployments.

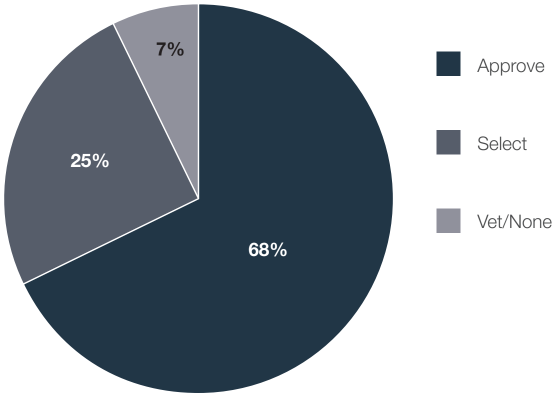

Figure 8: Network engineering and operations leaders' level of involvement in IoT deployments.

Trend: The majority of network engineering and operations leaders lack fully integrated security solutions.

Organizations are enthusiastically embracing DX, as witnessed by the finding that 86% have DX-related projects underway. These DX initiatives deliver significant benefits but also expand the attack surface. In response, network engineering and operations leaders are acquiring point security products to defend these additional attack points. This approach fragments the security architecture, resulting in just 1 in 10 indicating they have full security integration (Figure 9).

Organizations seem to recognize the problems that come with a fragmented security architecture. Nearly three-quarters (72%) of those that report gaps in the security infrastructure indicate they are actively working on integration projects. This finding suggests a growing awareness that point security solutions will not be adequate for securing applications in an era of expanding attack surfaces and advanced threats.

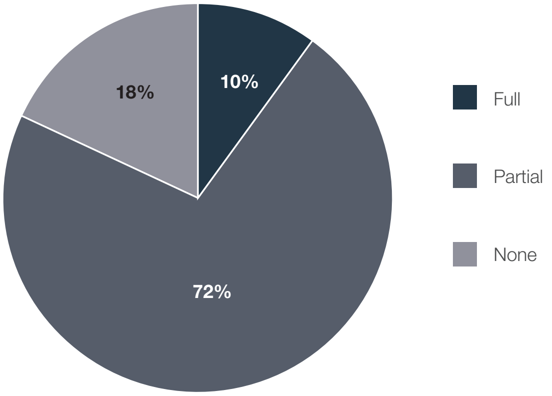

Figure 9: State of security integration.

Trend: Network engineering and operations leaders identify and block many vulnerabilities, but large gaps remain.

Despite significant investments in security infrastructure, the vast majority of respondents continue to see a large number of security events (Figure 10). Just 16% of respondents experienced no intrusions in the past year. Nearly 6 in 10 (59%) had at least three intrusions, while more than 3 in 10 (31%) had six or more. Malware (56%), spyware (44%), phishing attacks (41%), and distributed denial-of-service (DDoS) exploits (35%) each impacted more than one-third of respondents.

The impact of these intrusions was significant. Nearly half of respondents (46%) reported at least one outage that impacted productivity, almost 4 in 10 (38%) reported revenue impact due to an outage, and 3 in 10 (30%) suffered brand awareness degradation. In addition, intrusions put personal safety at risk (29%) and led to loss of business-critical data (29%) in more than one-quarter of organizations. These findings underline the dangers associated with a successful attack—and make clear the mandate for network engineering and operations leaders to put in place strong countermeasures.

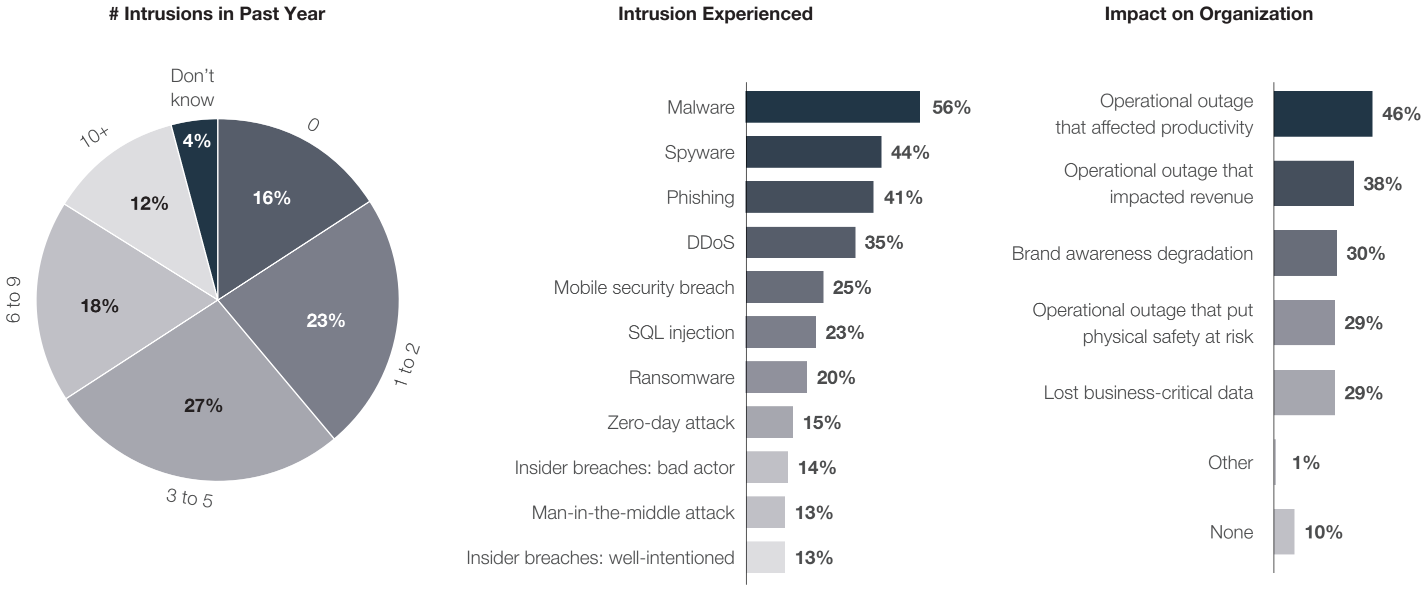

Figure 10: Intrusions at network leader organizations in the past 12 months.

Trend: Network engineering and operations leaders are concerned about operational inefficiencies.

Network engineering and operations leaders have a broad range of security issues but are particularly concerned about those that hinder operational efficiency: inefficient workflows (36%), false positives (32%), poor attack visibility (27%), and too many manual processes (26%) (Figure 11) top the list. Thus, it makes sense that almost three-quarters (72%) are working on integration initiatives. Collapsing fragmented point security solutions into a unified architecture provides network engineering and operations teams transparent visibility across the entire attack surface—whether cloud applications, IoT devices, wireless access points, or others. In addition to enhancing an organization's risk posture, an integrated architecture unlocks automation and enables organizations to eliminate manual processes tied to audits and report generation.

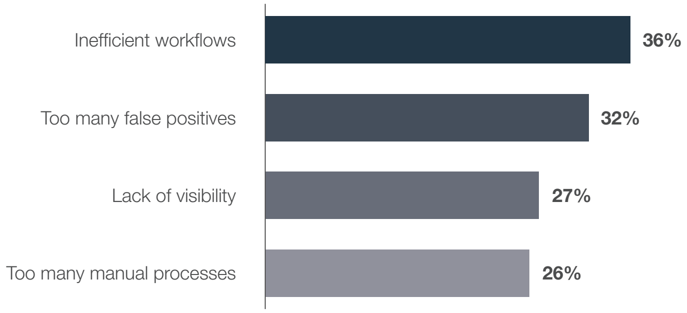

Figure 11: Top security issues that drain staff time.

Trend: Most network engineering and operations leaders use MSSPs to supplement their internal security resources.

Network engineering and operations leaders are increasingly turning to managed security service providers (MSSPs) to help manage or even assume full responsibility for the management of their networks and the security components attached to them. Nearly three-quarters choose to engage with MSSPs to either supplement their internal staff for selected functions (54%) or outsource security completely (20%) (Figure 12). Barely 1 in 4 choose to manage security entirely in-house.

This is hardly surprising, given the fact that organizations are tasking network engineering and operations leaders with more cybersecurity responsibilities for which they often have neither the training to manage nor the experience. Outsourcing portions or even all security to an MSSP with a proven track record is one way to mitigate risk and avoid taking management time away from traditional areas of focus such as network performance and application availability.

"The expanding threat landscape forces us to invest more into security solutions and hire qualified personnel to help us stay ahead of the threats."
– Survey Respondent

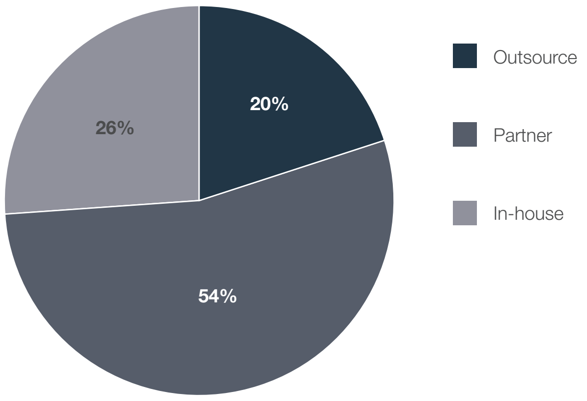

Figure 12: Reliance on managed security service providers.

Security Challenges on Network Engineering and Operations Leaders

The survey also included open-ended questions to provide a deeper understanding of the key challenges that network engineering and operations leaders face in their daily work. While responses vary, the answers were categorized to get a picture of what is top of mind.

Challenge: Risk management is the biggest challenge caused by the expanded attack surface.

In response to an open-ended question, more than half (52%) of network engineering and operations leaders reported that risk management is the job responsibility most impacted by the expanding attack surface (Figure 13). Organizations recognize this problem. According to a recent skills gap report, organizations are actively seeking network engineering and operations leaders who possess strategic risk management skills and experience.[8] Candidates with these qualifications are in short supply, so many organizations will not have the talent they need to effectively manage risks and improve efficiency.

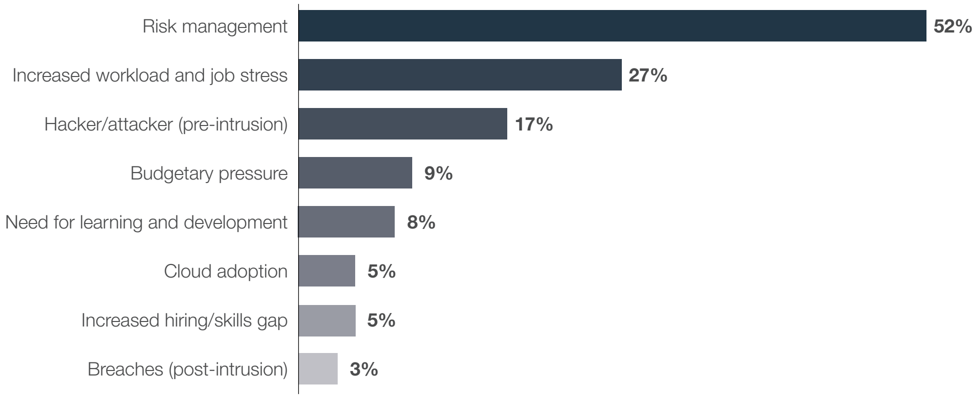

Figure 13: Impact of expanding attack surface on job responsibilities.

Challenge: Cybersecurity challenges increase the workload and create job stress.

As network engineering and operations leaders take on significant cybersecurity responsibilities, they are under more pressure to succeed, which is increasingly difficult due to constant changes in the threat landscape and attacks that increase in volume and velocity. Specifically, a significant percentage of network engineering and operations leaders cite job stress as the second most common outcome when posed in the context of the complexity of security management (36%), the advanced threat landscape (29%), and the expanded attack surface (27%) (Figure 14).

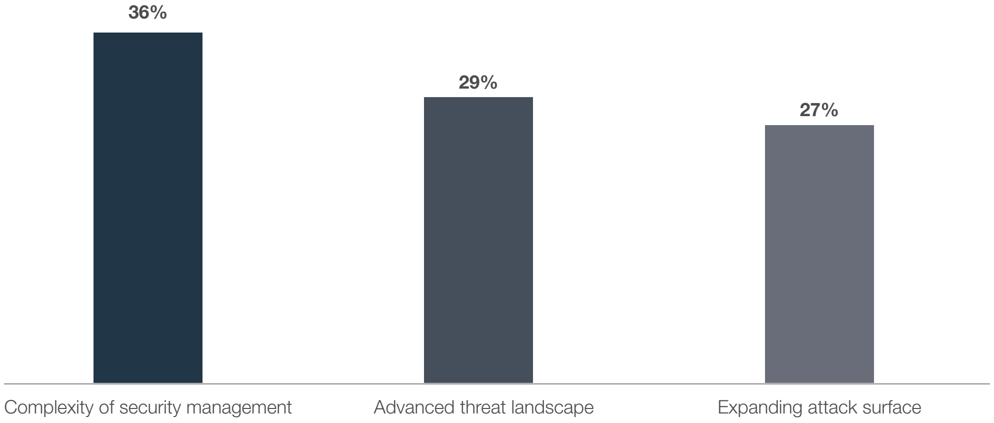

Figure 14: Percentage of network engineering and operations leaders citing job stress as impacted by specific cybersecurity factors in response to each of the three cybersecurity challenges cited.

Challenge: The cyber-threat landscape complicates pre-intrusion security much more than remediation activities.

Network engineering and operations leaders report that the evolving threat landscape affects their ability to stop attackers far more than their ability to remediate intrusions. As an example, 4x as many respondents believe the expanding attack surface impedes their pre-intrusion duties than the respondents who cite impact on post-intrusion activities (Figure 15). Similar percentages apply to the impact of the advanced threat landscape (6x) and security complexity (5x).

This finding make sense in light of the rapidly changing advanced threat landscape in which cyber criminals are unleashing previously unknown and highly sophisticated exploits at an increasingly rapid rate. Here, advanced threats challenge network engineering and operations leaders who may not have the training and experience to construct effective cybersecurity countermeasures.

Another plausible explanation for the lessened impact on post-intrusion responsibilities is preparation: 83% of network leaders have incident response and remediation plans in place and 72% include cross-functional responsibilities in their plans (Figure 16). Having remediation processes and personnel in place naturally would lessen the impact of intrusions on the network engineering and operations leader.

> "As our security system becomes more and more complex, I need to spend more money on training employees—and take the time to learn how to use it myself."
> – Survey Respondent

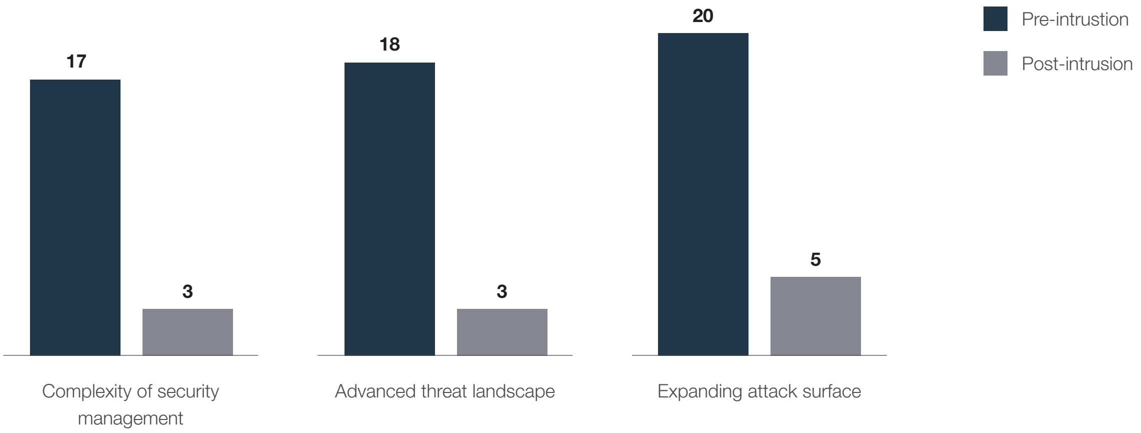

Figure 15: Percentage of network engineering and operations leaders citing pre-intrusion and post-intrusion as impacted by specific cybersecurity factors.

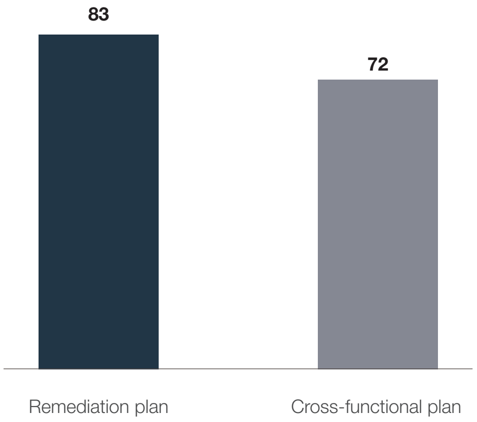

Figure 16: Percentage of organizations with remediation plans and remediation plans with cross-functional responsibilities in place.

Best Practices of Top-tier Network Engineering and Operations Leaders

1. Top-tier network engineering and operations leaders are nearly 4x more likely to have purchased an end-to-end integrated security solution.

A recurring theme in the survey is the increasingly important role that network engineering and operations leaders play in the organization's cybersecurity strategy. Notably, findings show a correlation between breach prevention and integrated security systems: top-tier network engineering and operations leaders are nearly 4x more likely to have purchased an end-to-end security system as compared to bottom-tier performers. For organizations that rely on point security products, the top-ranking leaders are 25% more likely to be in the process of integrating those solutions. Taken together, these findings show that security integration is a best practice for reducing the risk of intrusions.

2. Top-tier network leaders are 3x more successful at making the case against budget cuts.

The adage "Nothing succeeds like success" is undoubtedly true for cybersecurity. Network engineering and operations leaders who report no intrusions anticipate that their budgets will either increase (44%) or stay the same (50%) the following year—and only 6% expect a decrease. On the other hand, 20% of the bottom-tier leaders foresee a budget cut, 3x more likely than their more successful colleagues.

3. Top-tier network engineering and operations leaders are 88% more likely to be graded on a) network performance/uptime and b) number of vulnerabilities remediated.

Top-tier network leaders are 88% more likely to cite network performance as a key metric than the bottom-tier laggards. Interestingly, top-tier leaders are also 88% more likely to cite vulnerabilities remediated, reflecting their increased focus on cybersecurity concerns. Several other security metrics also carry more weight with top performers, including DevOps security (31% more likely), intrusion remediation (25% more likely), and attacks blocked (7% more likely).

4. Top-tier network engineering and operations leaders are 88% more likely to be concerned about operational efficiencies of false positives.

According to an earlier finding in this report, 32% of network engineering and operations leaders have concerns about the number of false positives and the implications they have on operational efficiencies. Top-tier network leaders seem to be more aware of this problem than the laggards, as demonstrated by the finding that top performers are 88% more likely than the laggards to list the operational inefficiencies of false positives as a top security issue.

5. Top-tier network engineering and operations practitioners are 72% more likely to measure vulnerabilities found and blocked.

It comes as no surprise that the top-tier leaders are 72% more likely to measure vulnerabilities found and blocked. In contrast, bottom-tier laggards are 60% more likely to focus on productivity gains—an important organizational metric to be sure, but one that is unlikely to lead directly to intrusion prevention.

6. Top-tier network engineering and operations leaders are 67% more likely to report directly to the CIO.

Most bottom-tier network engineering and operations leaders report to operational staff. In contrast, top-tier network engineering and operations leaders are 67% more likely to report directly to the CIO. Network engineering and operations leaders in the IT organization likely benefit from the technical expertise and experience of the CIO, even in cases when the security function does not report to the CIO.

Conclusion

Our research shows that network engineering and operations leaders are highly visible in the organization and, as a result, they face heightened expectations. In addition to their traditional charter of ensuring network performance, availability, resiliency, and reliability, they must execute on key cybersecurity responsibilities—for some, an unfamiliar and challenging assignment.

Network engineering and operations leaders who are still experiencing high levels of intrusions can learn from the best practices of those who have had no recent successful attacks. Some of these lessons include:

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

Evaluating security efficacy using cybersecurity metrics rather than operational considerations.

Focusing on activities that improve staff productivity and operational efficiencies.

Building a strong case for increased funding to combat advanced threats and defend the expanding attack surface.

Of course, beyond these technology elements, network engineering and operations leaders should maintain a concerted focus on recruiting, hiring, and retaining top talent.

References

[1] Dan Littmann, et al., "Connectivity of tomorrow: The spectrum and potential of advanced networking," Deloitte, January 16, 2019.

[2] Ibid.

[3] Patrick E. Spencer, "What CISOs Need to Know About Network Engineering and Operations Leaders," The CISO Collective, July 17, 2019.

[4] Ibid.

[5] Elaine Chen, "CTO vs VP Engineering: What's the Difference?" IvyExec, accessed July 15, 2019.

[6] Louis Columbus, "83% Of Enterprise Workloads Will Be In The Cloud By 2020," Forbes, January 7, 2018.

[7] "The Security Architect and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, June 29, 2019.

[8] Patrick E. Spencer, "What CISOs Need to Know About Network Engineering and Operations Leaders," The CISO Collective, July 17, 2019.

FORTINET

www.fortinet.com

September 4, 2019 10:34 AM

D:\Fortinet\Work\2019\September\report-network-engineering-operations-leader-cybersecurity

331129-0-0-EN