Research Insights Report

Navigating Network Security Complexity

By Jon Oltsik, ESG Senior Principal Analyst and ESG Fellow

June 2019

This ESG Research Insights Report was commissioned by Cisco Systems and is distributed under license from ESG.

Contents

Executive Summary

In April 2019, the Enterprise Strategy Group (ESG) completed a research survey of 200 cybersecurity, IT, and networking professionals with purchase process responsibility for networking and/or security technologies at their organizations. Further descriptions of the research methodology and survey demographics are presented in the appendix section of this report.

Based upon the research collected for this project, ESG concludes:

- **Network security is growing increasingly complex and challenging**. Most organizations claim that network security is more complex today than it was two years ago due to factors like a growing attack surface, an increased security workload, and pervasive threats and vulnerabilities. Additionally, organizations face many network security challenges, including misalignment with business/IT initiatives, staffing shortages, and lengthy timeframes needed for policy creation and network security controls deployment. Issues like these are a direct cause of security incidents at 29% of organizations.

- **Network security can't keep up with the business.** As organizations move toward digital transformation, IT initiatives must be supplemented with security controls and oversight for cyber-risk mitigation. Unfortunately, many organizations don't have the right network security policies, processes, or controls in place to keep up with the accelerating pace of business change. This leaves them vulnerable to devastating cyber-attacks and data breaches.

- **Changes are in the works.** To accommodate the business, organizations want new types of network security technologies offering agile and consistent policy management. ESG believes that these demands will drive network security technology consolidation and integrated architectures featuring central management, distributed enforcement, ease-of-use, and process automation.

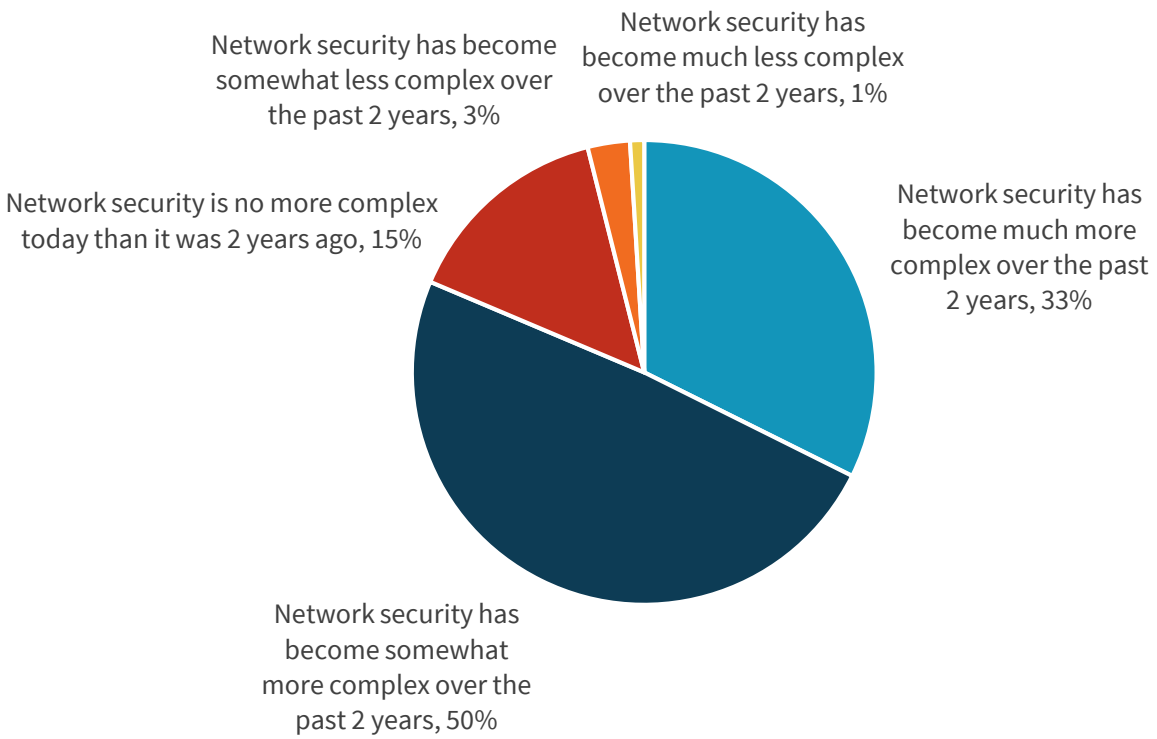
Overview

Network Security Complexity Is Bad and Getting Worse

Strong network security demands technical knowledge, security acumen, and process discipline. Mastering this combination can be difficult at any time, but ESG research indicates that network security is growing increasingly complex. In fact, 83% of respondents believe network security has become more complicated over the last two years (see Figure 1).

Figure 1. Opinion Regarding Network Security Complexity

Which of the following statements best characterizes your opinion about network security complexity? (Percent of respondents, N=200)

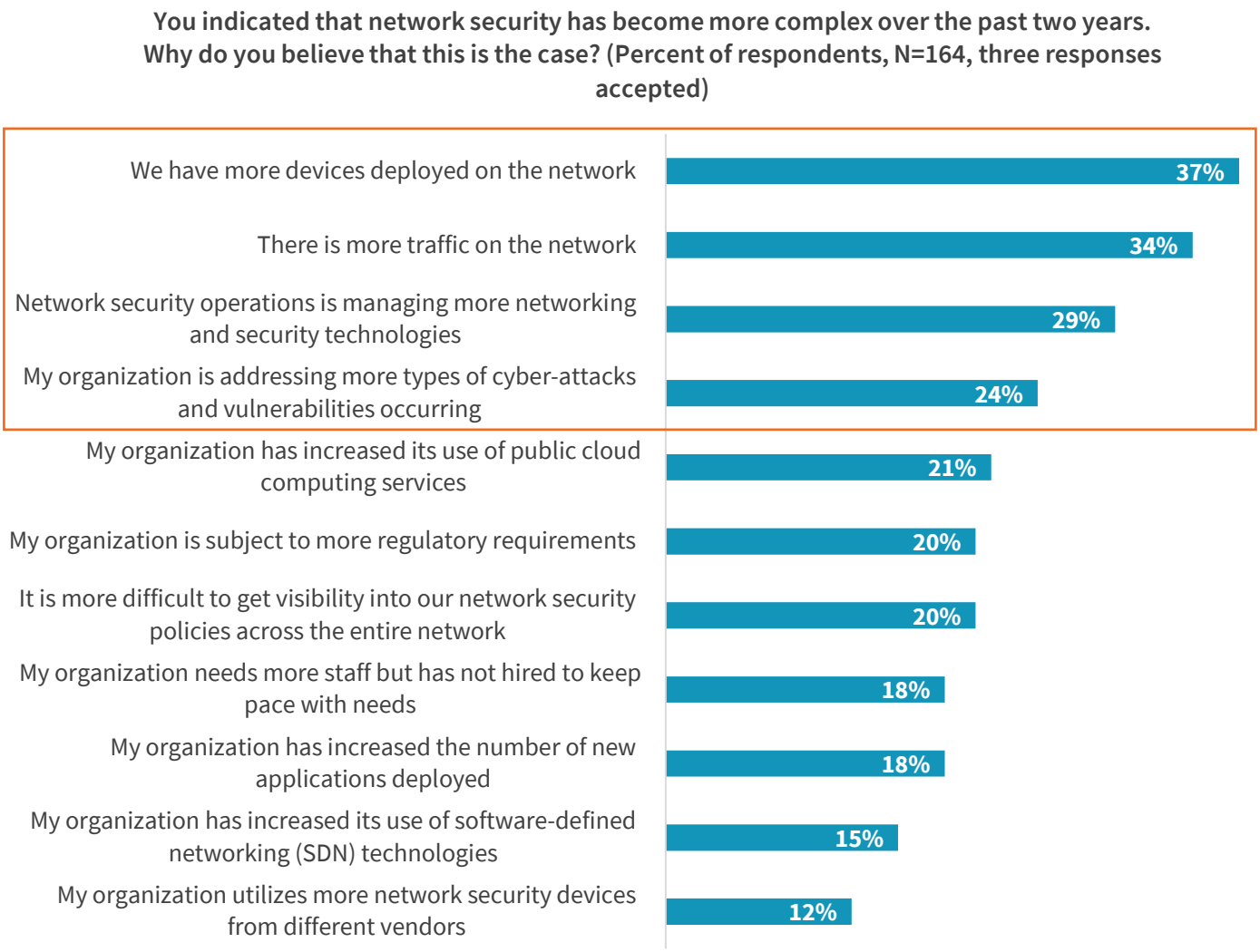


Source: Enterprise Strategy Group

To flesh this out further, ESG pressed respondents who claimed that network security has become more complex over the past two years and asked them why they believe this is the case. The research reveals that network security complexity is related to (see Figure 2):

- **A growing attack surface.** Thirty-seven percent of respondents claim that network security is more complex because they have more devices on their networks than they did two years ago while 34% point to more traffic on the network. Both situations suggest a growing attack surface where cybersecurity teams struggle to monitor network security and protect critical assets.
- **An increasing workload.** Twenty-nine percent of respondents believe that network security is more complex because network security operations teams are managing more networking and security technologies. Given the global cybersecurity skills shortage, many organizations don't have the right staff, skills, or time to procure, provision, configure, and operate a mounting mix of networking and security technologies.
- **Threats and vulnerabilities.** Twenty-four percent of respondents say that network security is more complex because their organization is addressing more types of cyber-attacks and vulnerabilities. This hits cybersecurity and networking teams with a one-two punch. As more devices are added to networks, security and IT operations teams are responsible for discovering and patching software vulnerabilities across a growing attack surface. At the same time, cyber-adversaries prey upon this complexity with a constant flood of probes, social engineering scams, exploits, and malware attacks. It's hard for security and networking teams to keep up with either case.

Figure 2. Reasons for Increase in Network Security Complexity



Source: Enterprise Strategy Group

Aside from increasing complexity, organizations also forecast impending network security challenges. For example (see Figure 3):

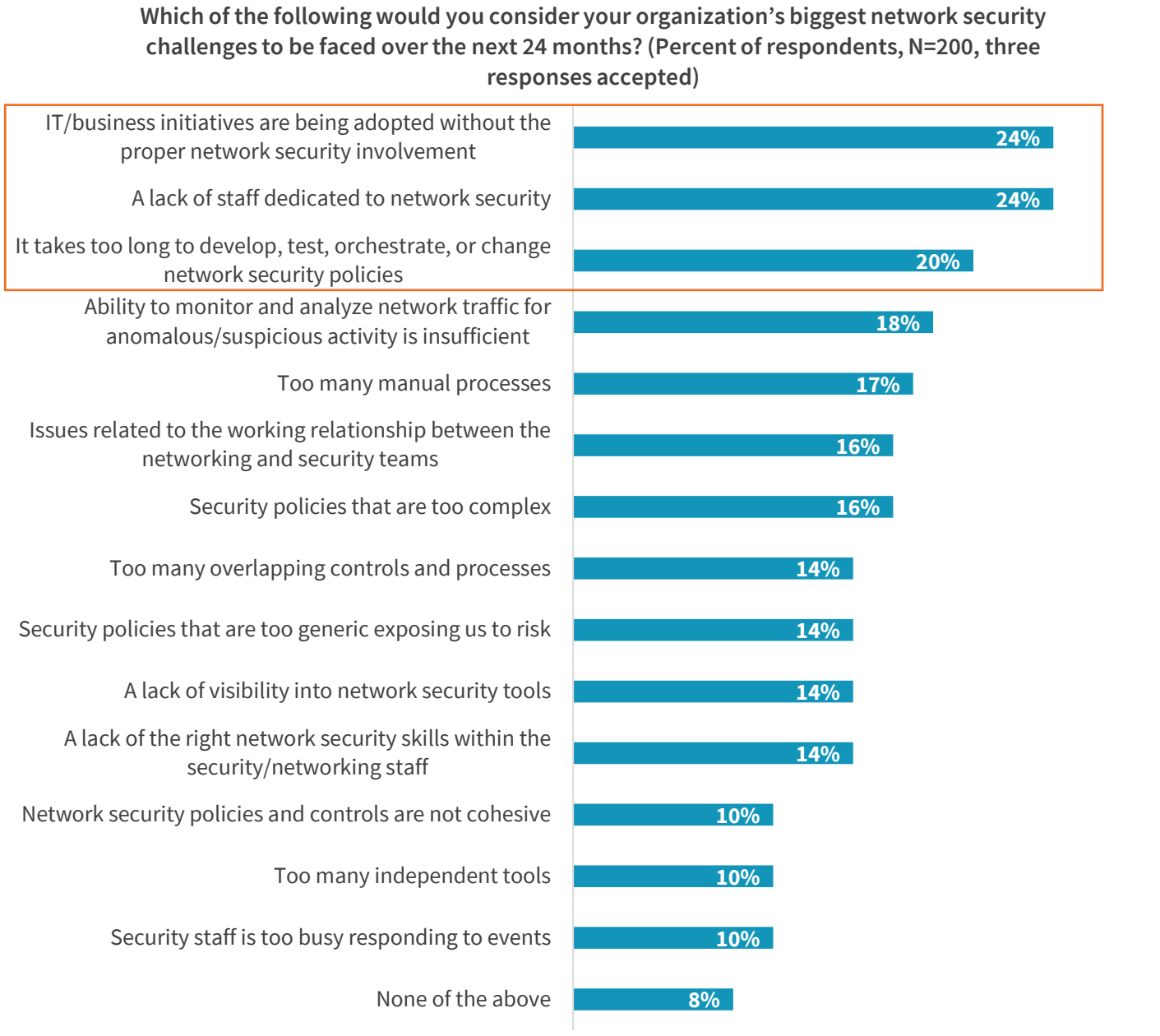
- Twenty-four percent of networking, IT, and security professionals claim that IT and business initiatives are being adopted without the proper network security involvement. This means that security is often ignored until after new business and IT initiatives are in a pilot or production phase. Security engineers are then forced to scramble to retrofit the right controls, while operations teams try and fast-track procurement, configuration, and deployment in order to catch up with ongoing projects. This leads to misconfigurations and human error.

- Twenty-four percent of networking, IT, and security professionals anticipate a lack of dedicated staff to network security. This isn't surprising. According to ESG research from earlier in 2019, 53% of organizations have a problematic shortage of cybersecurity skills.[1] Short-staffed organizations tend to have overwhelming workloads, making it difficult or impossible to keep up with business and security needs.

[1] Source: ESG Research Report, *2019 Technology Spending Intentions Survey*, March 2019.

- Twenty percent of networking, IT, and security professionals say that it takes too long to develop, test, orchestrate, or change network security policies. This is especially problematic because many organizations have adopted agile development and DevOps processes, so sluggish security controls management is getting in the way of business progress.

Figure 3. Biggest Network Security Challenges over the Next 24 Months



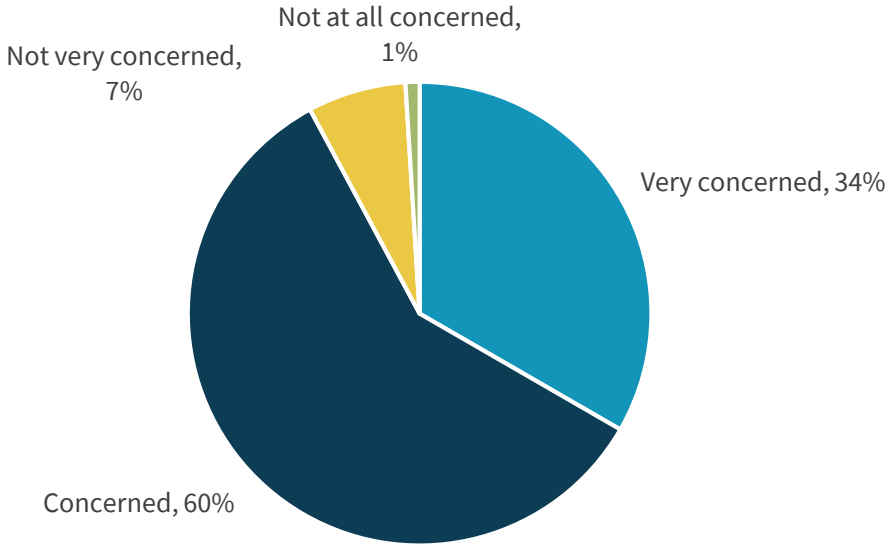
Source: Enterprise Strategy Group

Cyber-risks Have Consequences

Of course, threats and vulnerabilities equate to growing cyber-risk that could result in devastating ramifications for business operations. Clearly, cybersecurity and networking professionals are anxious about this situation—94% of survey respondents report that they are concerned the increased complexity in the network makes them more vulnerable (see Figure 4).

Figure 4. Concerns about Security Vulnerabilities Due to Network Security Complexity

How concerned is your organization about security vulnerabilities that may be introduced due to network security complexity (i.e., misconfigurations, conflicting policies, human error, etc.)? (Percent of respondents, N=200)

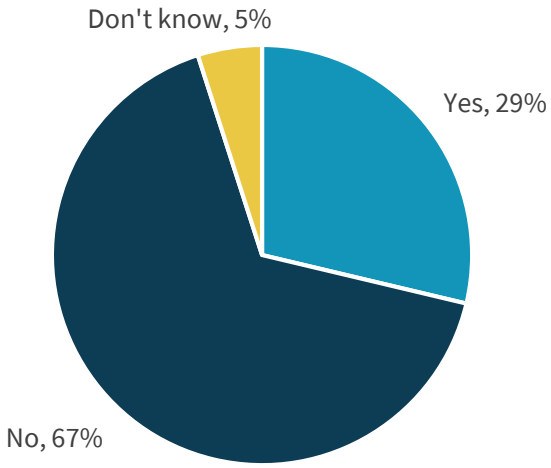


Source: Enterprise Strategy Group

Alarmingly, the research also indicates that these concerns are justified, as 29% of respondents claim that their organization experienced a security event in the past 12 months that was caused by a vulnerability tied to network security complexity (i.e., misconfigurations, conflicting policies, human error, etc., see Figure 5).

Figure 5. Security Incidents Due to Vulnerabilities from Network Security Complexity

Has your organization experienced a security event in the past 12 months that was caused by a vulnerability tied to network security complexity (i.e., misconfigurations, conflicting policies, human error, etc.)? (Percent of respondents, N=200)

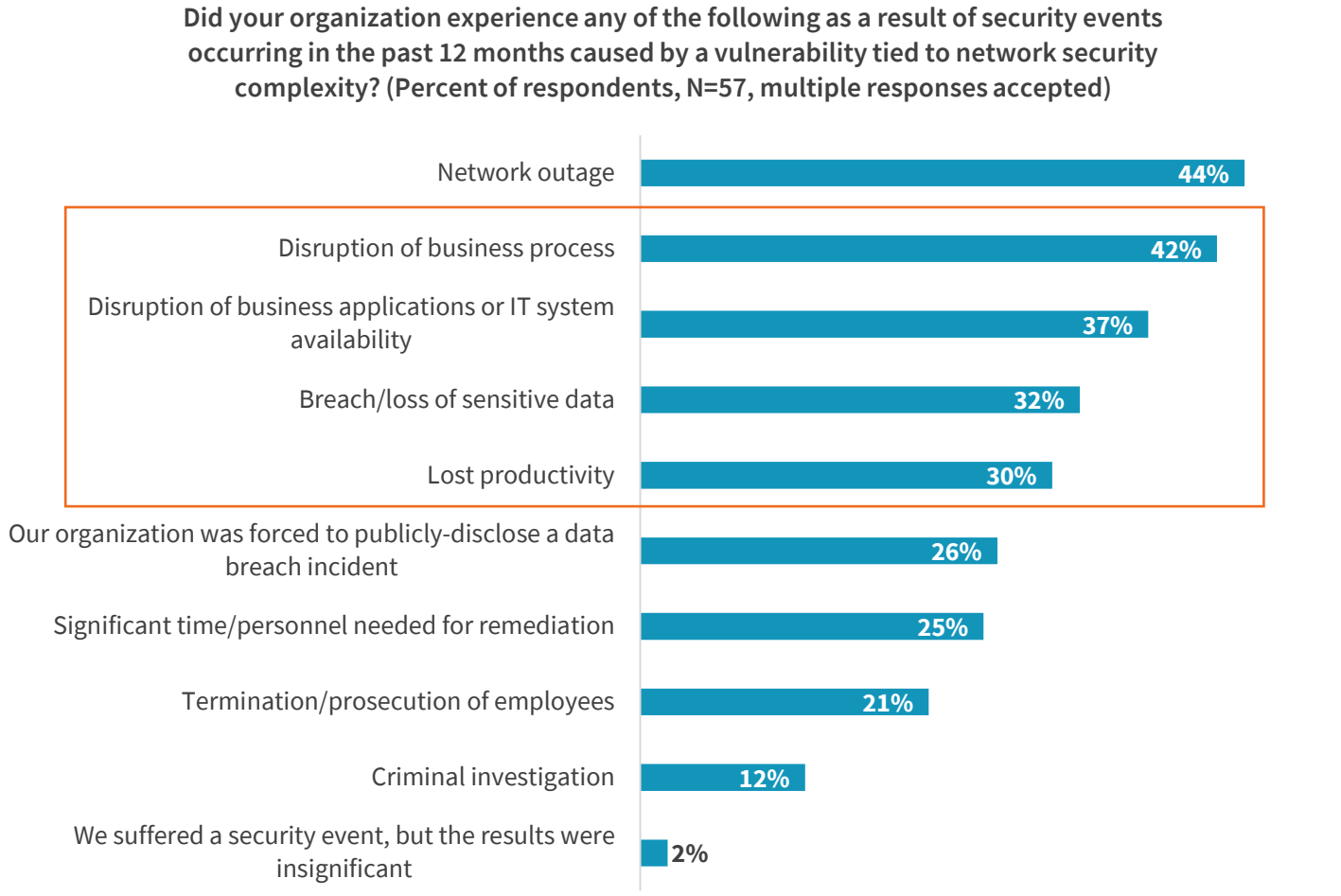


Source: Enterprise Strategy Group

The most common incident related to network security complexity is a network outage (44%), which could be a minor annoyance (i.e., an outage of a test or development network) or a major incident (i.e., an outage of a production network).

Beyond network outages, however, network security complexity incidents can have a direct impact on an organization's mission and operations. Respondents claim that network security complexity incidents often led to disruption of business processes (42%), disruption of a business application or IT system (37%), a breach or loss of sensitive data (which could also trigger a regulatory compliance violation, 32%) or lost productivity (30%, see Figure 6). Given these types of incidents, addressing network security complexity must be considered a business-critical cyber risk in need of attention and a sound risk mitigation strategy.

Figure 6. Types of Incidents Due to Network Security Complexity



Source: Enterprise Strategy Group

The Need for Change

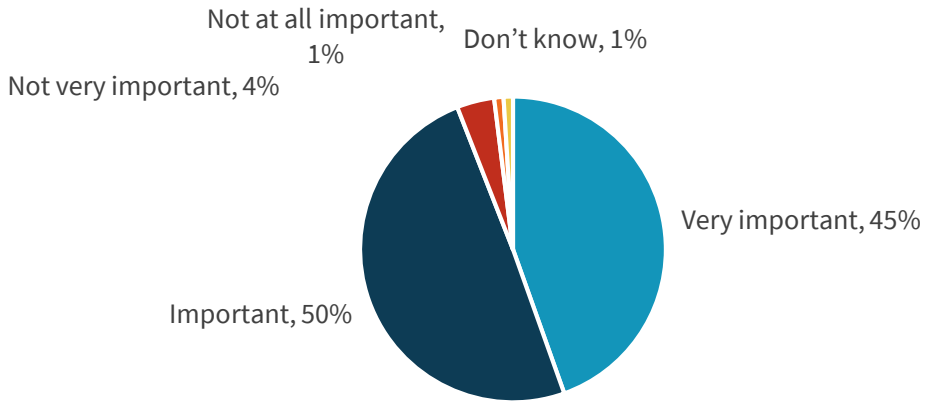
Organizations have clear priorities around network security. For example, the biggest factors driving network security include preventing/detecting malware threats (47%), regulatory compliance (42%), support for cloud computing initiatives (38%), and the need for network security to be more scalable to support dynamic business processes and new business initiatives (34%).

The data points to a strong intersection between business needs and network security, which ESG views as a positive development. As organizations embrace new technologies for digital transformation, business executives realize the need to balance technology initiatives with the right controls and oversight to mitigate cyber-risks and respond to cyber-attacks in a timely manner. These requirements demand more agility and consistency around network policies. This is certainly

why 95% of organizations believe it is very important or important to have consistent policies across all network security control points (e.g., spanning corporate network, branch networks, roaming users, and the cloud, see Figure 7).

Figure 7. Importance of Consistent Network Security Policies

How important is it for your organization to have consistent policies across all your network security control points (e.g., spanning corporate network, branch networks, roaming users, and in the cloud)? (Percent of respondents, N=200)

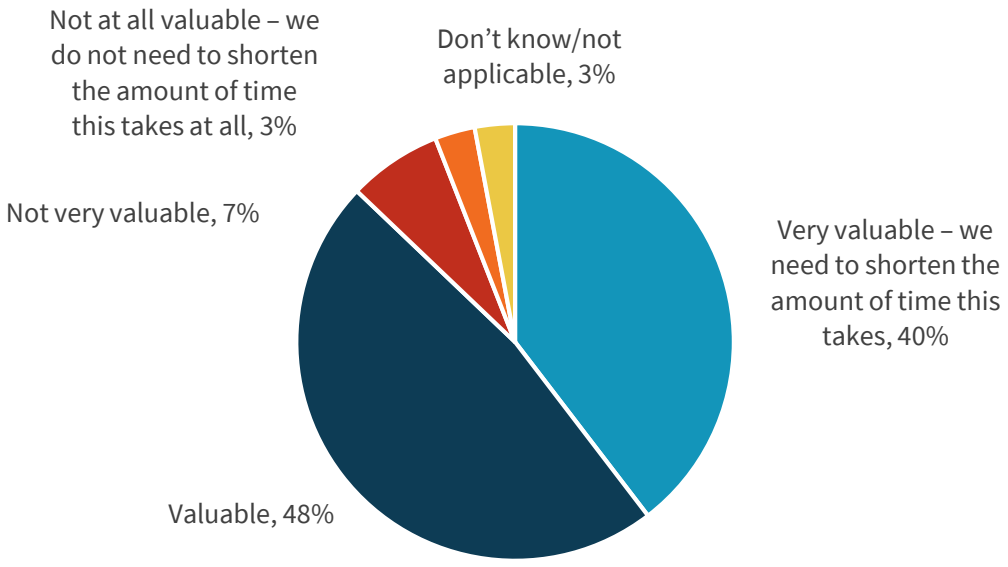


Source: Enterprise Strategy Group

As previously stated, consistency isn't the only network security policy requirement. A majority (88%) believe that reducing the time to create or change a network security policy would be considered very valuable or valuable to their organization. Obviously, these individuals understand the need to align technical controls with the increasing speed of digital business processes (see Figure 8).

Figure 8. Importance of Reducing Time Required to Create or Change Network Security Policy

How valuable would it be to your organization to shrink the amount of time it takes to create or change a network security policy? (Percent of respondents, N=200)



Source: Enterprise Strategy Group

The Bigger Truth

It's not a stretch to claim that network security policies and processes are prisoners of a bygone time when IT was managed in-house using an array of physical devices. Many organizations continue to rely on point tools, manual processes, and short-staffed networking and security teams to test, configure, deploy, and operate network security technologies that safeguard critical business assets. As the ESG research reveals, this strategy is broken and can no longer keep up with the unyielding pace of business/IT initiatives in areas like digital transformation.

To streamline operations, accelerate network policy creation/change, and achieve greater levels of policy consistency, CISOs must:

- Look toward technology consolidation and integration. Disparate point tools that require their own care and feeding introduce far too much operational overhead—especially when many organizations' security departments are short-staffed. CISOs must strive for more order by consolidating point tools into an integrated security technology architecture offering central management (i.e., configuration management, policy management, reporting, etc.) and distributed enforcement. The best architectures will have the ability to span physical, virtual, and cloud-based network security controls.

- Emphasize ease-of-use and time-to-value. As the saying goes, "complexity is the enemy of security," and based upon the research presented in this report, network security complexity leads to issues like misconfigurations, human error, and worst of all, data breaches. Addressing complexity requires a new generation of management tools offering simplicity, RBAC, profile-based dashboards, and end-to-end visibility. Many tools that meet this description are designed using a cloud-based interface for command-and-control.

- Push for process automation. Simply stated, there is too much network security work and not enough people or time to get everything done. To bridge this gap, CISOs should assess network security policies and processes, and strive for automation wherever possible. Policy management tools and network security controls should accommodate these needs with scripts, runbooks, and closed-looped responses to policy changes.

Appendix: Research Methodology and Respondent Demographics

To gather data for this report, ESG conducted a comprehensive online survey of IT decision makers responsible for their organizations' investments in networking and security technologies. Specifically, three-fifths of respondents held senior IT/security titles (i.e., CIO, CISO, VP of IT/networking/security, or equivalent) while the remainder held middle management and staff titles. All respondents were based in North America and employed at organizations with 100 or more employees. Specifically, 38% were employed at midmarket (i.e., those with 100 to 999 employees) organizations and 62% at enterprises (i.e., those with 1,000 or more employees). Respondents represented numerous industry and government segments, with the largest participation coming from information technology (19%), health care (14%), manufacturing (14%), financial services (13%), and government agencies (9%).

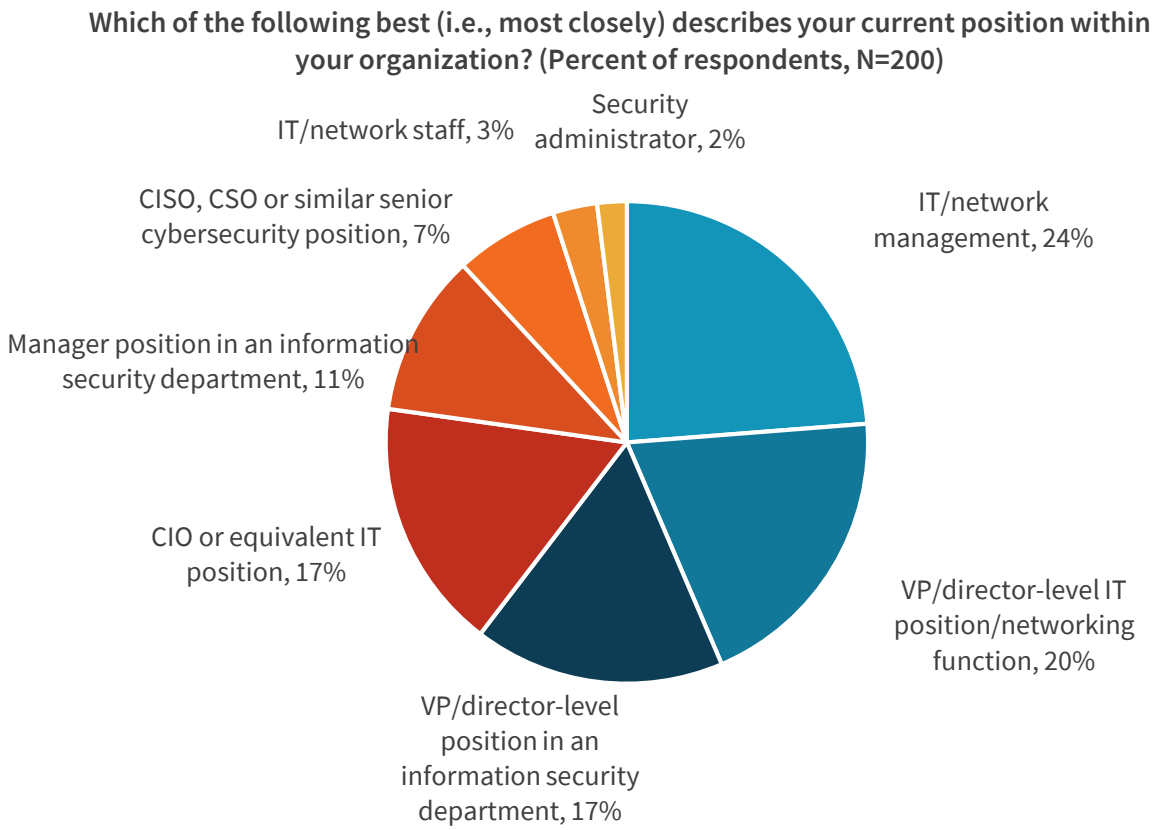
The survey was fielded between April 4, 2019 and April 20,2019.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 200 respondents remained.

All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

The figures below detail the full demographics of the respondent base: individual respondents' roles and areas of responsibility, as well as respondent organizations' total number of employees, primary industry, and annual revenue.

Figure 9. Survey Respondents, by Role

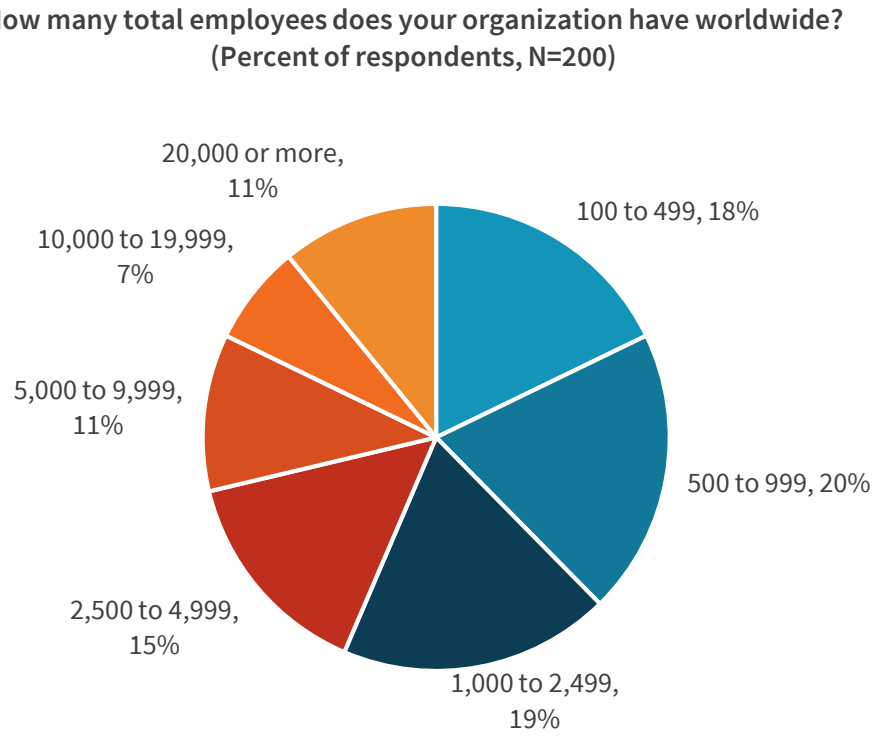


Source: Enterprise Strategy Group

Figure 10. Survey Respondents, by IT Security Responsibility

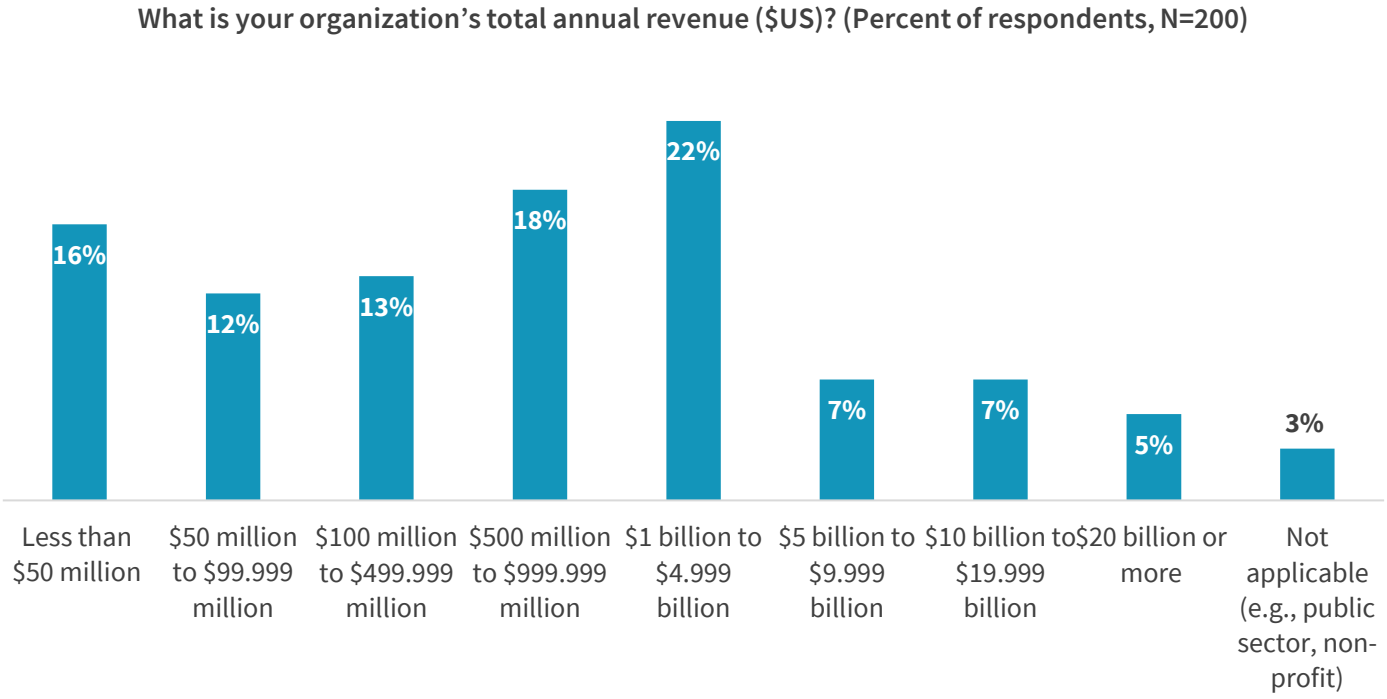
Source: Enterprise Strategy Group

Figure 11. Survey Respondents, by Company Size (Number of Employees)



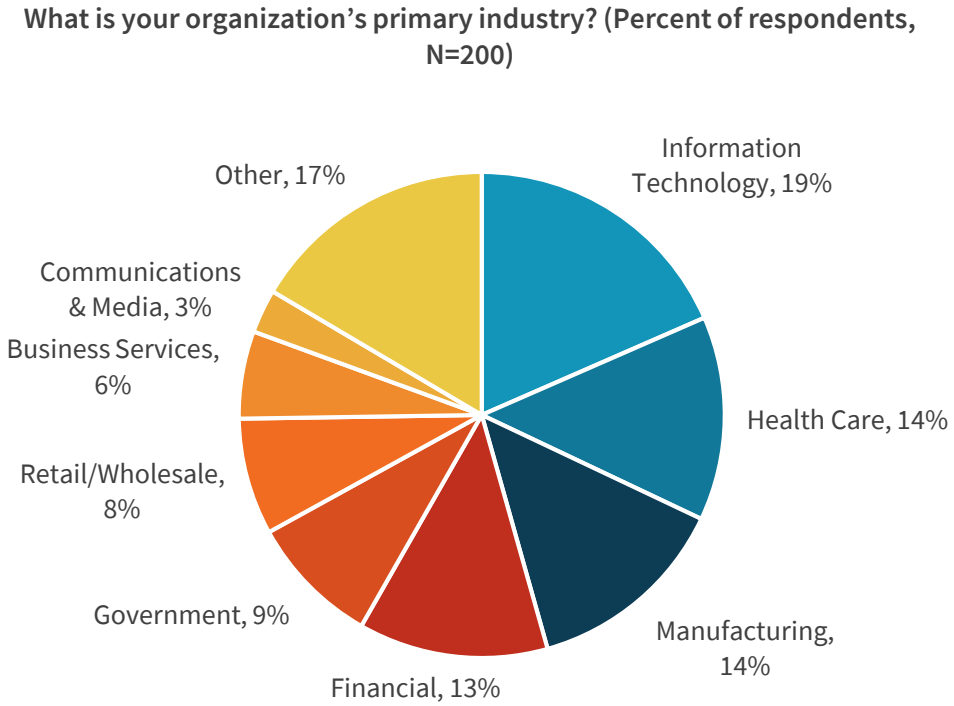
Source: Enterprise Strategy Group

Figure 12. Survey Respondents, by Company Size (Revenue)



Source: Enterprise Strategy Group

Figure 13. Survey Respondents, by Industry



Source: Enterprise Strategy Group

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188