ESG Research Insights Paper

Cybersecurity Realities and Priorities for 2018 and Beyond

By Jon Oltsik, Senior Principal Analyst; Adam DeMattia, Director, Customer Research; and Jennifer Gahm, Senior Project Manager, Market Research

August 2018

This ESG Research Insights Report was commissioned by Spirent Communications and is distributed under license from ESG.

Contents

Executive Summary

In late 2017 and early 2018, the Enterprise Strategy Group (ESG) completed a research survey of 413 IT and cybersecurity professionals with knowledge of, or responsibility for, the planning, implementation, and/or operations of their organization's security policies, processes, or technical safeguards. Survey respondents were in the United States, U.K., and Australia and worked at enterprise organizations (i.e., more than 1,000 employees). Respondents represented numerous industry and government segments, with the largest participation coming from financial services (i.e., banking, securities, insurance, 18%), manufacturing (16%), retail/wholesale (13%), health care (12%), and information technology (10%).[1]

Based upon the data collected as part of this research project, ESG concludes:

- **Overall, cybersecurity has become increasingly difficult.** Seventy-nine percent of security professionals believe that cybersecurity (i.e., knowledge, skills, operations, management, etc.) is more difficult today than it was two years ago. Why? Survey respondents point to increases in malware volume and sophistication, the number of new IT initiatives, the number of targeted cyber-attacks, and the number of devices connected to the network.

- **Organizations are impacted by the global cybersecurity skills shortage.** The data suggests that organizations don't have adequate security staff levels and skills, especially with regards to the intersection of networking and security. CISOs need help to bridge these skills gaps.

- **CISOs are moving closer to the business.** Security executives used to be the organization's most senior and experienced security technicians, but this profile is changing rapidly. CISOs are evolving into business executives responsible for protecting applications and business processes from end to end.

- **Cybersecurity budgets are on the rise.** Ninety-two percent of the organizations surveyed will increase their cybersecurity budgets in 2018. Areas in which organizations are most likely to increase spending include network security, cloud security, and application security.

- **Security testing should be a high priority.** The research indicates that cybersecurity professionals believe their organizations would benefit from more security testing as it could help them test controls and balance security with application and network performance. Furthermore, security testing should be part of IT projects from their genesis and should then be conducted on a continuous basis. Organizations appear to be getting this message, as security testing budgets are poised to increase. Nevertheless, CISOs should assess whether their organizations are doing comprehensive security testing and have the right skills and equipment to do so effectively.

Cybersecurity Is Becoming More Complex

According to over 80% of the respondents, cybersecurity is a difficult discipline that grows more complex annually. One-third of cybersecurity and IT professionals surveyed believe that cybersecurity (knowledge, skills, management, operations, etc.) has become significantly more difficult over the past two years while another 46% say that cybersecurity has grown somewhat more difficult during this period.

Why is cybersecurity becoming more difficult? Survey respondents point to numerous factors, including (see Figure 1):

- **An increase in the volume and sophistication of malware.** The AV-Test institute claims that it registers 250,000 new malware programs per day and recorded over 700 million malware variants in 2017. Of these, more than 120 million

[1] See Appendix: Research Methodology and Respondent Demographics for more information.

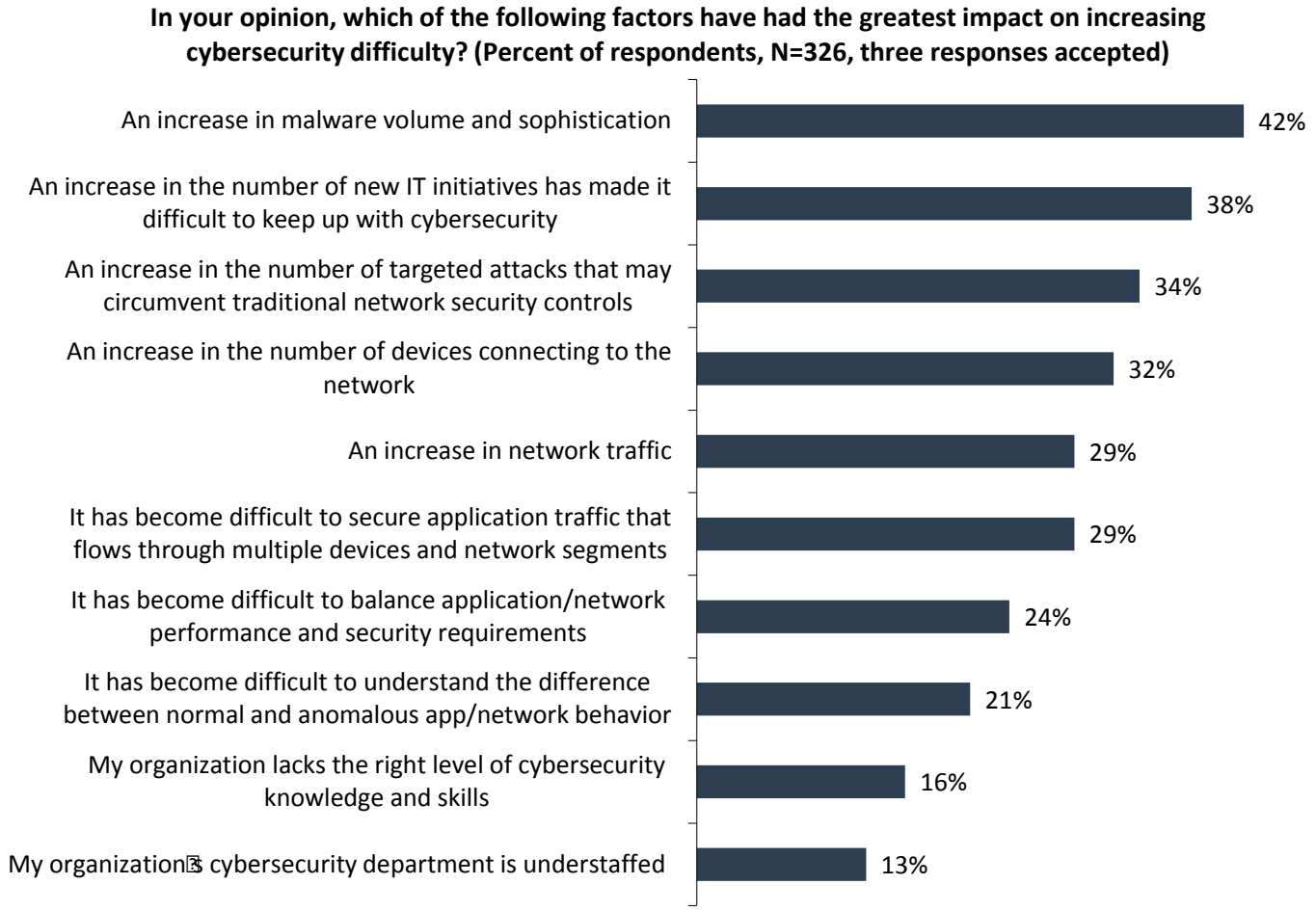
were classified as new malware. Not surprisingly, security professionals find it difficult to keep up with this barrage of activity emanating from the threat landscape.

- An increase in the number of IT initiatives. Enterprise organizations are embracing or increasing activities like cloud computing, digital transformation, and IoT applications at a rapid pace. Security teams find it difficult to learn the nuances of these technology initiatives, understand associated risks, and implement the right security safeguards to protect their organizations.

- An increase in the number of targeted attacks. Multiple security researchers also indicate that between 80% to 90% of malware attacks just one device and 50% to 60% of malicious web domains are active for one hour or less. These trends speak to the rise of targeted attacks designed to penetrate the network of a single organization. Targeted attacks act as small needles in a large haystack, making cybersecurity practices increasingly difficult.

Cybersecurity professionals also note that it can be difficult to prevent and detect cyber-attacks due to the high volume of encrypted network traffic, and the use of hybrid (i.e., public/private) cloud infrastructure. Furthermore, many respondents indicate that it is difficult to balance security with application and network performance requirements. Clearly, cybersecurity professionals face numerous and growing challenges just to do their jobs!

Figure 1. Reasons Why Cybersecurity Has Become More Difficult



Source: Enterprise Strategy Group

While cybersecurity continues to grow more difficult, many organizations must address these difficulties while lacking the right skills or adequate human resources. According to the 2018 ESG IT spending intentions research, 51% of organizations claim to have a problematic shortage of cybersecurity skills.[2]

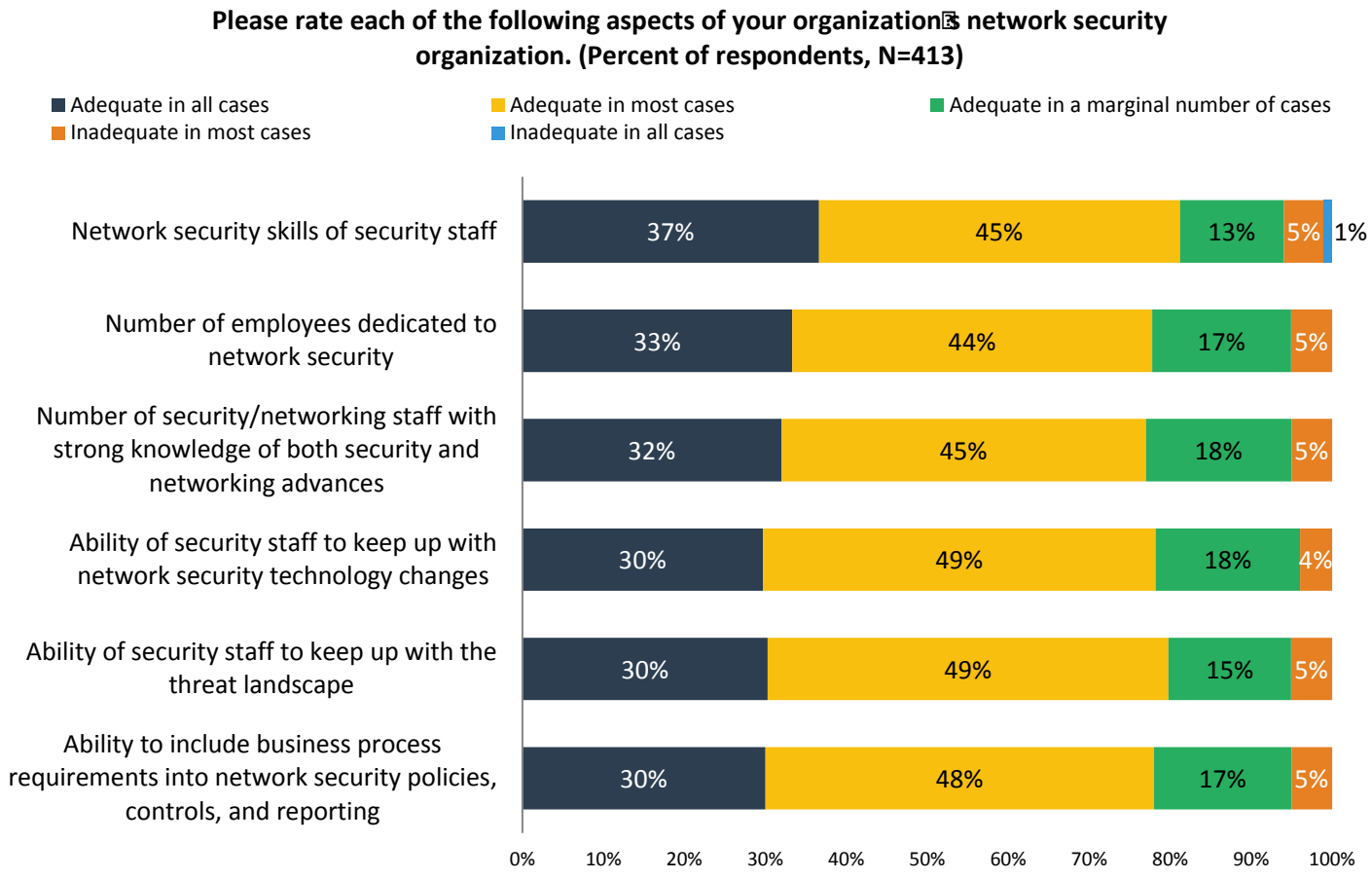
These skills gaps were also symptomatic in this research project (see Figure 2). For example:

- Only 37% of organizations believe that the network security skills of the security staff are adequate in all cases. This means that many organizations lack some foundational skills to keep up with network traffic and/or threats. Similarly, only 32% of organizations believe staff have a completely adequate level of knowledge of both networking and security.
- Only 33% of organizations say that the number of employees dedicated to network security is adequate in all cases. An understaffed cybersecurity team increases the workload of individuals, leading to long lead times, human error, and job fatigue. Similarly, only 30% of organizations can keep up with network changes or the threat landscape at an adequate pace.

Each of these deficiencies increases the potential for unknown vulnerabilities and increases risk.

Alarmingly, across all areas, 18% to 23% of respondents claim that their organization's cybersecurity skills and staffing levels are only adequate in a marginal number of cases or inadequate in most cases! Even the strongest internal teams cannot keep up with demands, making it difficult for them to dedicate time for training and further hone their skills.

Figure 2. Cybersecurity Skills and Staffing Gaps



Source: Enterprise Strategy Group

[2] Source: ESG Research Report, *2018 IT Spending Intentions Survey*, February 2018.

CISOs often turn to third-party service providers to bridge the skills and staffing gaps evidenced in the data presented in Figure 2. Security executives often call upon service providers to take over pedestrian security tasks (i.e., log management, email security filtering, system backup, etc.) that can be easily outsourced. Alternatively, many CISOs look for third-party experts to supplement the internal staff with tasks requiring advanced skills and training.

Cybersecurity Action Plan

Survey respondents were presented with several statements and asked whether they agree or disagree with each. The results can be seen as suggestions on how organizations can improve cybersecurity and address the challenges they face. For example (see Figure 3):

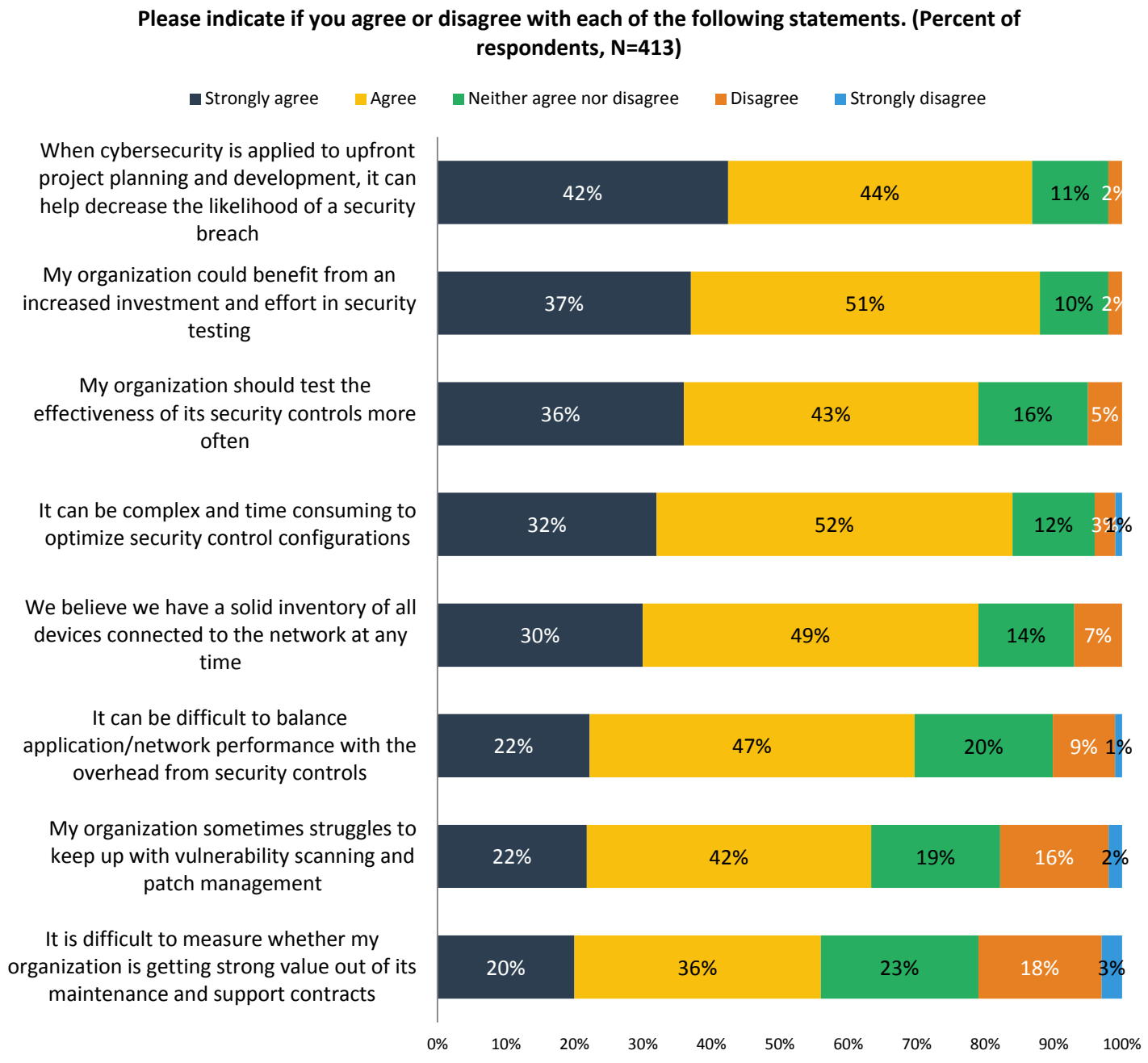
- Eighty-six percent of respondents strongly agree or agree with the statement: When cybersecurity is applied to upfront project planning and development, it can help decrease the likelihood of a security breach. This is the cybersecurity equivalent of the adage that an ounce of prevention is worth a pound of cure.

- Eighty-eight percent of respondents strongly agree or agree with the statement: My organization could benefit from an increased investment and effort in security testing. This should tell CISOs that the security staff believes that additional security testing should be viewed as a requirement rather than a discretionary option to improve security.

- Seventy-nine percent of respondents strongly agree or agree with the statement: My organization should test the effectiveness of its security controls more often. To ensure strong security, many infosec pros believe this testing should be done on a continuous rather than periodic basis.

It is also noteworthy that 84% of respondents believe it can be complex and time consuming to optimize security control configurations, while 69% believe it can be difficult to balance application/network performance with the overhead from security controls. Addressing each of these issues will take better planning, engineering, and testing of security controls across all technologies involved in application delivery from end to end.

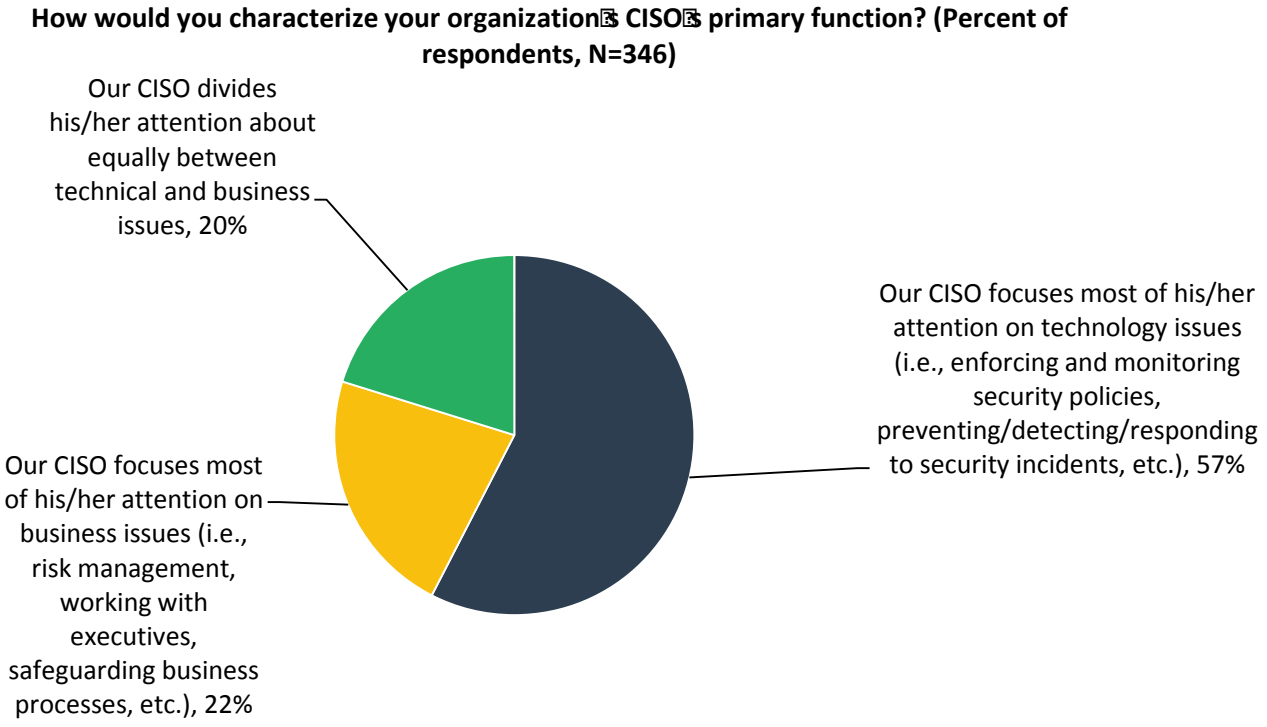
Figure 3. Cybersecurity Professionals Opinions



Source: Enterprise Strategy Group

Most (84%) of the cybersecurity professionals surveyed say that their organization currently employs a CISO (or someone with a similar role but different title). The research indicates that more than half (57%) of CISOs focus their attention on technical issues while others spend more of their time on business issues or maintain a balance between business and technical projects (see Figure 4).

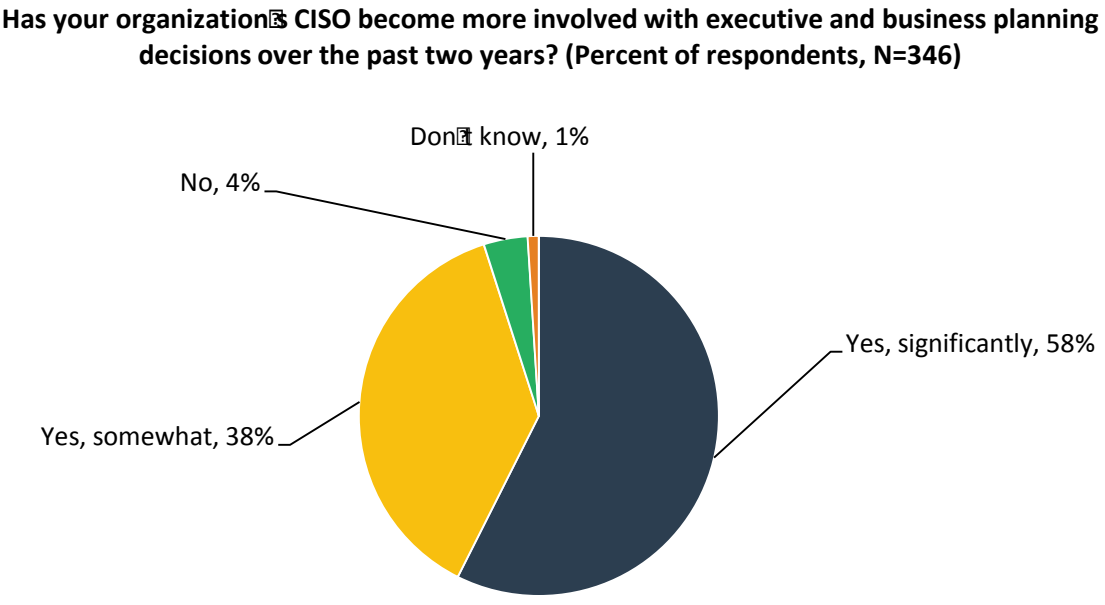
Figure 4. CISO Focus Areas



Source: Enterprise Strategy Group

While most CISOs continue to concentrate on technology issues, the research also points out that CISO concentration is in a state of evolution. More than half of respondents (58%) claim that their CISO has become significantly more involved with executive and business planning over the past two years while another 38% have become somewhat more involved with executive and business planning over the past two years (see Figure 5).

Figure 5. CISO Involvement with Executive and Business Planning



Source: Enterprise Strategy Group

As CISOs continue to get more involved with business planning, they tend to increase their focus on things like:

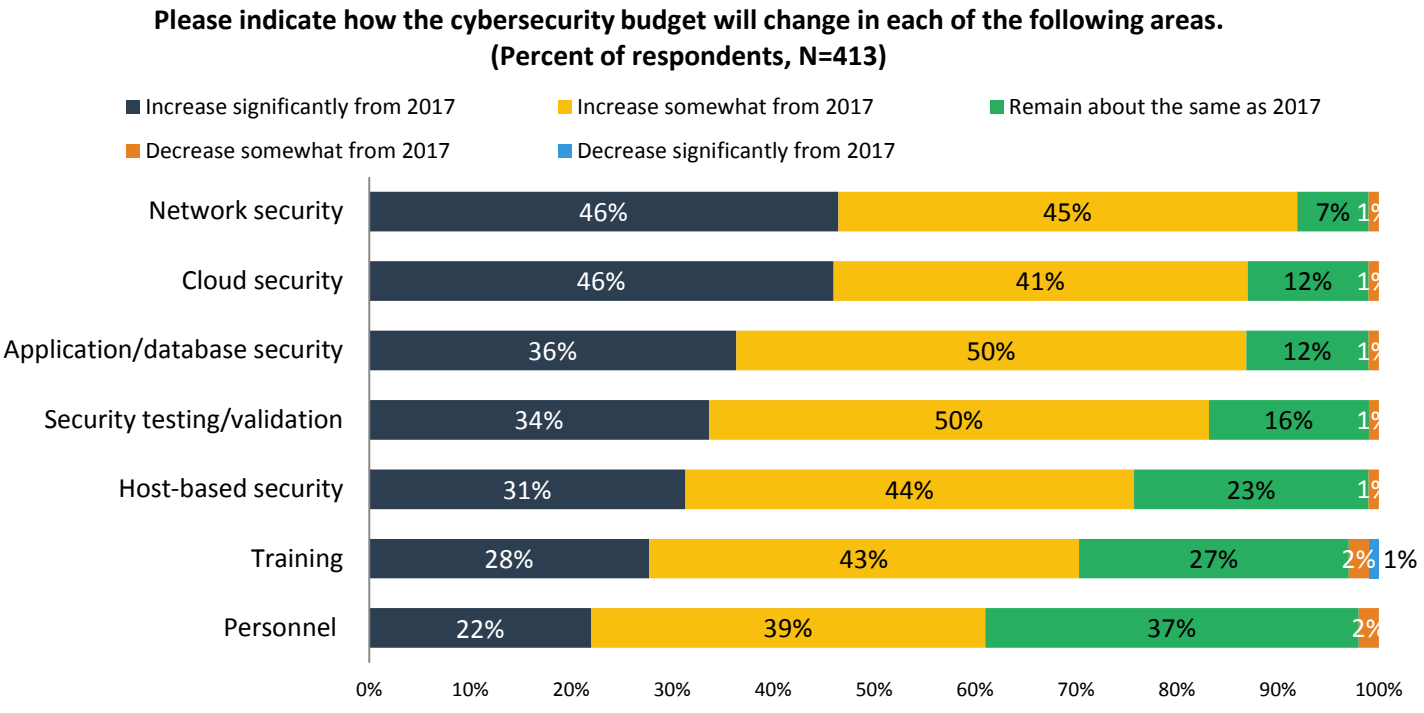
- **Risk to the business.** CISOs are being asked to understand and communicate business risks associated with targeted attacks. For example, when business managers read about the latest ransomware, they want to understand if their organization is vulnerable to this type of attack. Additionally, they want to know what risks come with new business applications associated with initiatives like cloud computing, digital transformation, and IoT.
- **Business resiliency.** CISOs are being asked how they can protect assets and respond to attacks while keeping critical business applications and services up and running.
- **IT planning and engineering.** Rather than layer security onto applications and infrastructure, CISOs are being asked to participate in projects at the business and technical planning phase. This provides an opportunity to design security into an end-to-end infrastructure that protects applications while maintaining peak performance.

With CISOs more engaged with the business, it is not surprising that most organizations (92%) plan to increase cybersecurity spending. In fact, over half (52%) say that their cybersecurity budget will increase significantly in 2018 while another 40% expect 2018 cybersecurity budgets to increase somewhat.

The research also points out that budget increases are targeted for specific areas. For example, 46% of organizations expect a significant increase in network and cloud security budgets while 36% are planning a significant increase in application security budgets (see Figure 6).

It is worth noting that 34% say that their security testing budget will increase significantly in 2018 while another 50% say that the security testing budget will increase somewhat. Based upon this data, it appears CISOs can articulate the importance of increasing the need for more security testing described in Figure 3 above to secure additional budget. Unfortunately, the data also shows that many organizations will not invest more in training and/or personnel in 2018. These spending deficits could exacerbate skills shortages and increase risk.

Figure 6. Cybersecurity Budget Changes for 2018 In Several Areas



Source: Enterprise Strategy Group

The Bigger Truth

The data presented in this ESG research insights report reveals that cybersecurity continues to grow more difficult annually, driven by dangerous external threats, changing IT initiatives, and a persistent shortage of cybersecurity talent.

Addressing these challenges can be difficult but a few patterns emerge from this data:

1. CISOs are working closer with business executives and managers to align security controls with business initiatives and processes. This requires an end-to-end view of security controls and continuous monitoring.

2. Organizations are increasing security budgets, especially in areas like network security, cloud security, application security, and security testing. Interestingly, these are the elements that *must* be included to attain an end-to-end security focus.

3. Cybersecurity professionals believe their organizations can benefit from including security as part of project planning and engaging in more thorough and frequent security testing. While the data suggests that organizations are moving in these directions, CISOs should carefully assess these security initiatives to make sure they are high priorities.

Throughout this report, the data also suggests that security should be balanced against application/network performance and resiliency. CISOs must work with IT teams to make sure they can achieve these goals to protect and enable the mission and objectives of their organizations.

Appendix: Research Methodology and Respondent Demographics

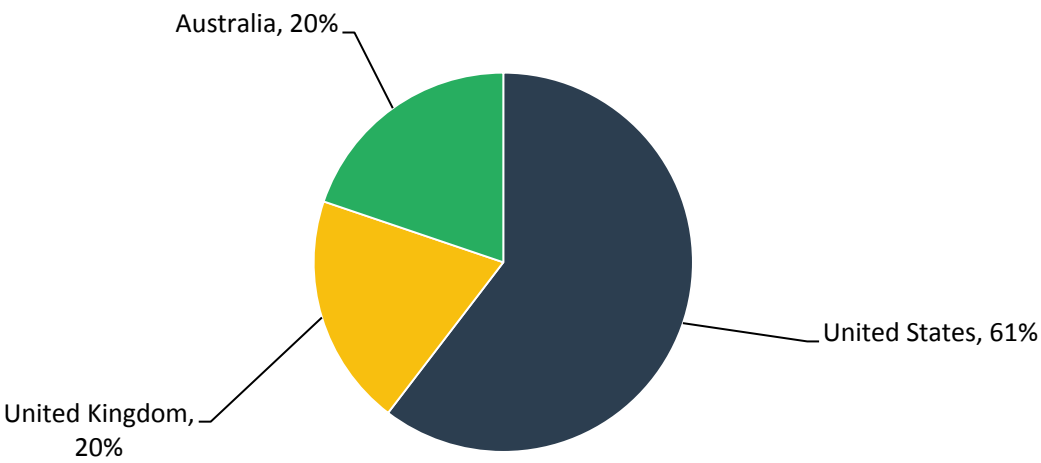
To gather the quantitative data for this report, ESG conducted a comprehensive online survey of security decision makers from private- and public-sector organizations in the United States, United Kingdom, and Australia between January 3, 2018 and January 22, 2018. To qualify for this survey, respondents were required to have reported a high level of knowledge for the planning, implementation, and operations of their organization's security processes and technical safeguards. Additionally, all respondents must have reported approval authority or influence in the purchase process for security technology products and services. Moreover, all respondents must have been employed at organizations with at least 1,000 employees worldwide. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 413 respondents remained.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

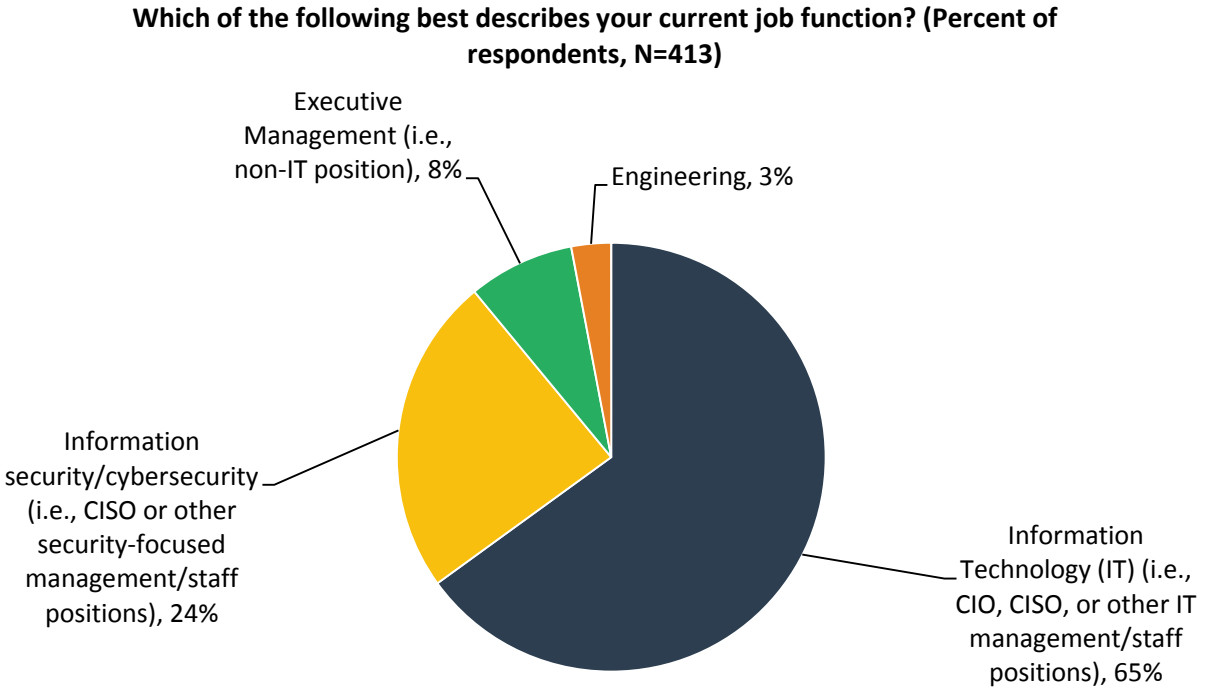
Figures 7-12 detail the demographics of the respondent base from the quantitative survey, including respondents' current role in the organization, respondent organizations' size, and primary industry.

Figure 7. Respondents by Country



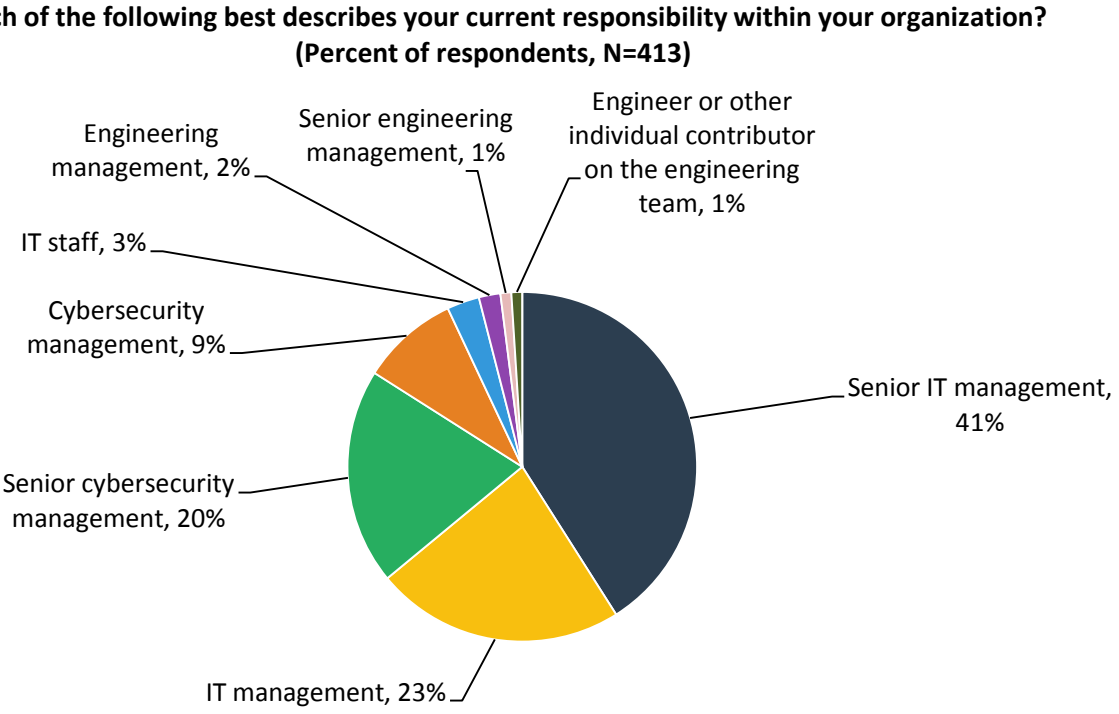
Source: Enterprise Strategy Group

Figure 8. Respondents by Job Function



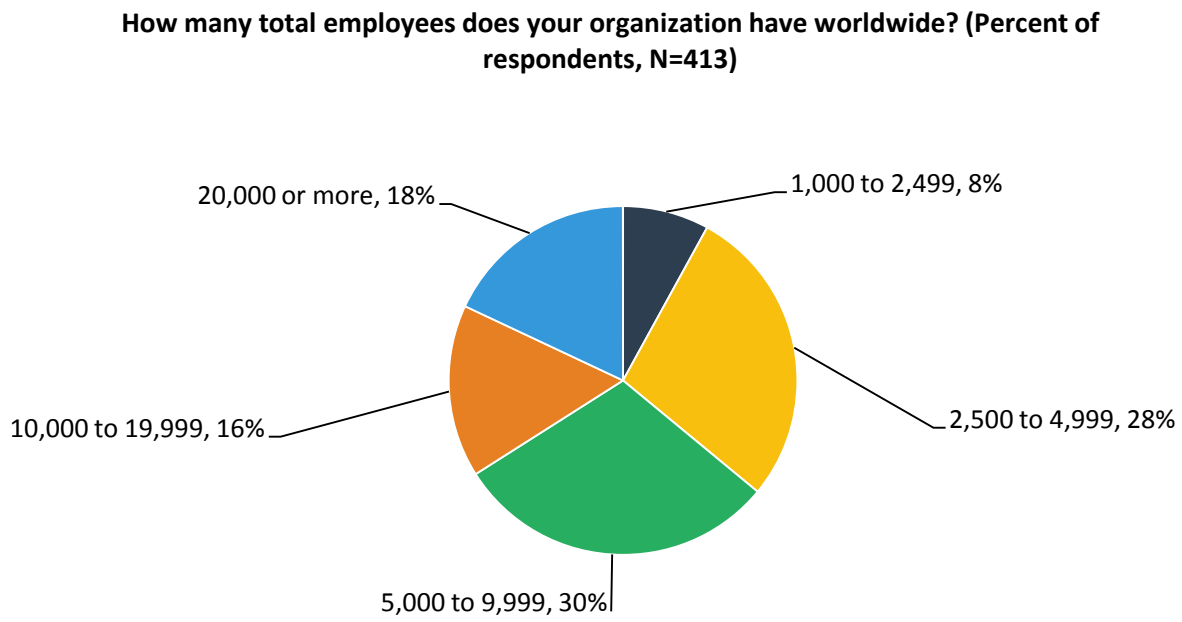
Source: Enterprise Strategy Group

Figure 9. Respondents by Responsibility Level



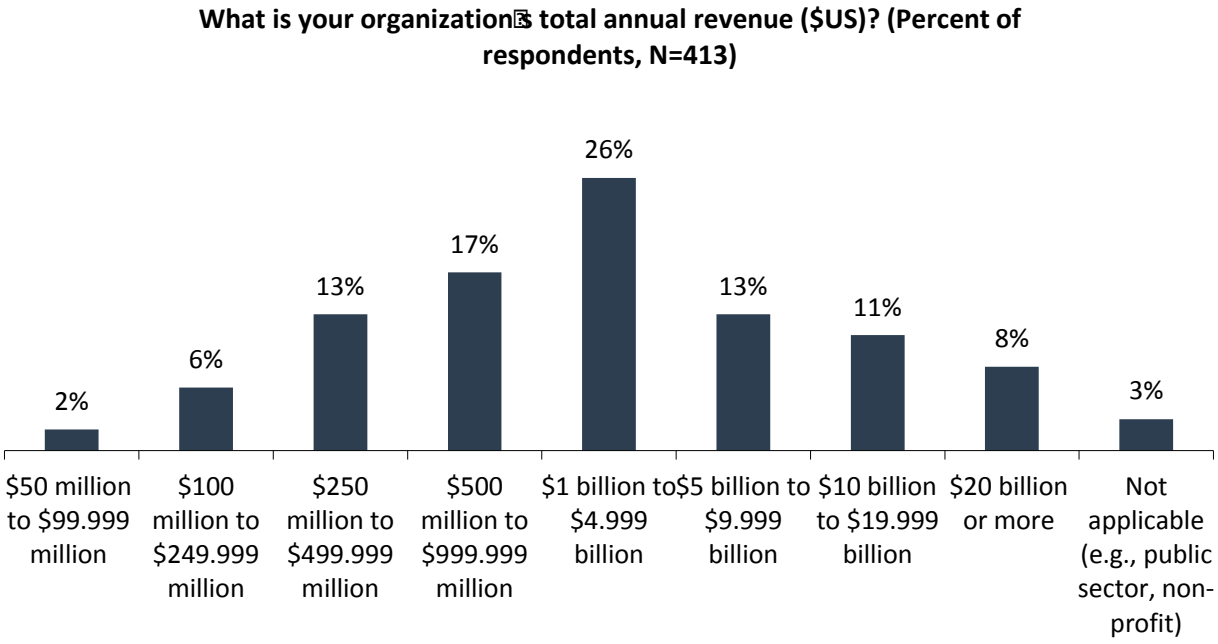
Source: Enterprise Strategy Group

Figure 10. Respondents by Number of Employees



Source: Enterprise Strategy Group

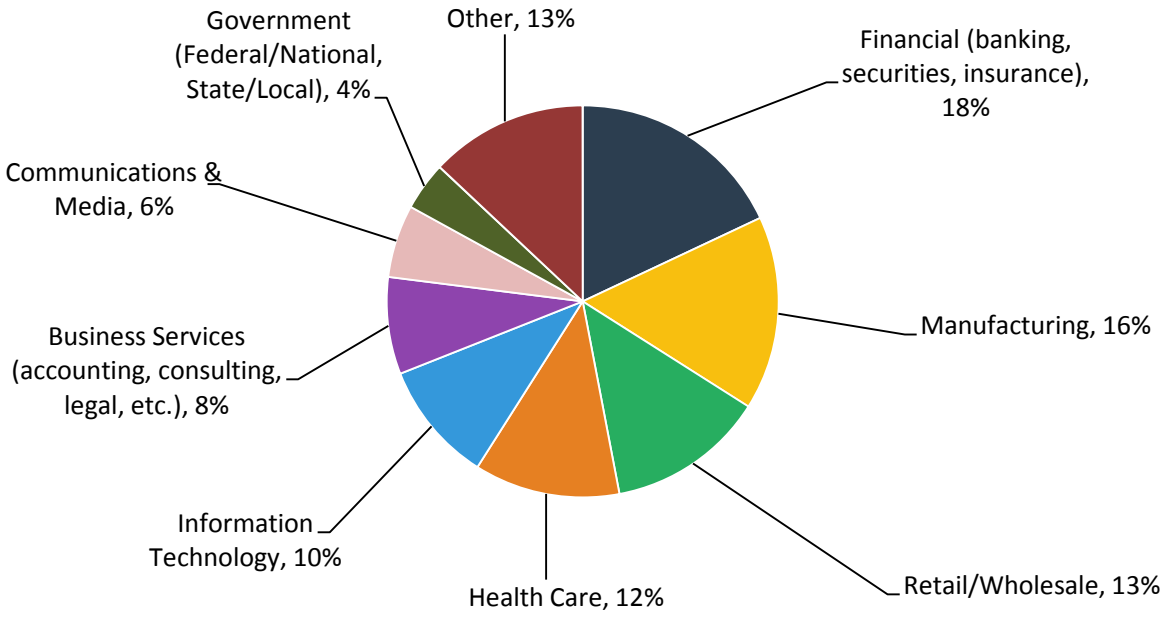
Figure 11. Respondents by Annual Revenue



Source: Enterprise Strategy Group

Figure 12. Respondents by Industry

What is your organization's primary industry? (Percent of respondents, N=413)



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