

RESEARCH REPORT

Through the Eyes of Cyber Security Professionals: Annual Research Report (Part II)



By Jon Oltsik, ESG Senior Principal Analyst
December 2016

A Cooperative Research Project by ESG and ISSA



Contents

| | |
|--|----|
| Contents | 2 |
| List of Figures | 3 |
| List of Tables | 3 |
| Executive Summary | 4 |
| Report Conclusions | 5 |
| Introduction | 8 |
| Research Objectives | 9 |
| Research Findings | 10 |
| The ISSA Survey Respondents | 11 |
| Are Organizations Vulnerable to Cyber-attacks? | 16 |
| The Cyber Security Skills Shortage | 18 |
| Bridging the Cyber Security Gap | 22 |
| Government and Cyber Security | 25 |
| Conclusion | 30 |
| The Bigger Truth | 31 |
| Top Five Research Implications and Recommendations | 31 |
| Research Methodology | 33 |
| Respondent Demographics | 34 |
| Respondents by Current Position | 35 |
| Respondents by Current Primary Responsibilities | 36 |
| Respondents by Region | 37 |
| Respondents by Number of Employees | 37 |
| Respondents by Industry | 38 |
| Respondents by Annual Revenue | 38 |

List of Figures

| | |
|---|----|
| Figure 1. Actions Taken Around Cyber Security Over the Past Two Years | 12 |
| Figure 2. Security Events Respondent Organizations Experienced Over the Last Year | 13 |
| Figure 3. Biggest Contributors to Security Events Experienced by Organizations | 15 |
| Figure 4. Vulnerability of Most Organizations to a Significant Cyber-attack or Data Breach | 16 |
| Figure 5. Vulnerability of Respondent Organizations to a Significant Cyber-attack or Data Breach Compared to Other Organizations..... | 17 |
| Figure 6. Impact of Cyber Security Skills Shortage..... | 19 |
| Figure 7. How Cyber Security Skills Shortage Has Impacted Organizations | 20 |
| Figure 8. Area(s) with Biggest Shortage of Cyber Security Skills | 21 |
| Figure 9. Actions That Would Provide the Most Cyber Security Benefits to Organization | 23 |
| Figure 10. Vulnerability of Respondents' Country to a Cyber-attack | 26 |
| Figure 11. Respondents' Sentiment on Cyber Security Strategy of Their Country's Government | 27 |
| Figure 12. How Active Government Should Be in Cyber Security | 27 |
| Figure 13. Actions Government Should Take If It Were to Become More Involved with Cyber Security | 28 |
| Figure 14. Respondents by Current Position | 35 |
| Figure 15. Respondents by Current Primary Responsibilities..... | 36 |
| Figure 16. Respondents by Region..... | 37 |
| Figure 17. Respondents by Total Number of Employees Worldwide | 37 |
| Figure 18. Respondents by Industry..... | 38 |
| Figure 19. Respondents by Annual Revenue | 38 |

List of Tables

| | |
|---|----|
| Table 1. Actions Taken Around Cyber Security Over the Past Two Years by Size of Organization | 13 |
| Table 2. Security Events Respondent Organizations Experienced Over the Last Year, by CISOs..... | 14 |
| Table 3. Actions That Would Provide the Most Cyber Security Benefits to Organization, by CISOs | 24 |
| Table 4. Actions Government Should Take If It Were to Become More Involved with Cyber Security, by CISOs..... | 29 |

Executive Summary



Report Conclusions

Today's cyber security professionals reside on the frontline of a perpetual battle, tasked with applying limited resources to outthink would be cyber-attackers and defend their organizations against everything from embarrassing website defacement through unseemly ransomware extortion to devastating data breaches. Alarming, cyber security professionals often accept this challenge knowing they are undermanned for the fight. According to ESG research, 46% of organizations claim to have a problematic shortage of cyber security skills.¹

Given this daunting responsibility, it's natural to wonder just how well cyber security professionals are holding up. Are they able to coordinate on cyber security strategies and tactics with their business and IT peers? Do they have the skills necessary for their jobs as cyber-adversaries develop new exploits? Are they overwhelmed and burnt out?

To answer questions like these, the [Enterprise Strategy Group](#) (ESG) and the [Information Systems Security Association](#) (ISSA) teamed up and initiated a primary research project in mid-2016 with the goal of capturing the voice and thoughts of cyber security professionals on the state of their profession, and gaining a perspective on situational analysis from those closest to the fight. In pursuit of this goal, ESG and ISSA surveyed 437 information security professionals (and ISSA members). Survey respondents represented organizations of all sizes and included professionals located in all parts of the world.

The cyber security professionals participating in this project were asked a series of questions on a variety of cyber security topics. The previously published report, [The State of Cyber Security Professional Careers](#), focused on the lifecycle of cyber security professional careers.

This second research report builds upon these conclusions by examining cyber security professionals' observations and opinions on the state of cyber security today within the organizations they work for. Furthermore, cyber security professionals express their opinions on the role that national governments should play as part of a comprehensive cyber security ecosystem.

This final report of the two-part series concludes:



- **Organizations have experienced a multitude of cyber security incidents.** For example, 39% of cyber security professionals say that their organization has experienced one or more incidents resulting in the need to reimage one or more endpoint or server, 27% have experienced a ransomware incident, 20% have experienced at least one security incident that disrupted a business application, and 19% have experienced at least one security incident that disrupted a business process.



- **A multitude of issues contributes to the onslaught of security incidents.** Altogether, 54% of organizations have experienced at least one type of security incident. What security issues contributed to these incidents? Nearly one-third (31%) of cyber security professionals say that the cyber security team is not large enough for the size of their organization, 26% point to a lack of training for non-technical employees, and 21% say that business and executive management tend to treat cyber security as a low priority. This data is especially troubling as it suggests that many organizations continue to lack a proportional commitment to cyber security.



- **Cyber security professionals believe that most organizations are vulnerable to cyber-attacks.** Nearly half (45%) of the cyber security professionals surveyed believe that most organizations are significantly vulnerable to a major cyber-attack or data breach while another 47% say that most organizations are somewhat vulnerable to a significant cyber-attack or data breach.
- **Most organizations are feeling the effect of the global cyber security skills shortage.** Sixty-nine percent of cyber security professionals say that the global cyber security skills shortage has had an impact on the organization they

¹ Source: ESG Research Report, [2016 IT Spending Intentions Survey](#), February 2016. All outside ESG research references in this report come from this research report.



work for. What type of impact? More than half (54%) say the cyber security skills shortage has resulted in an increasing workload on existing staff, 35% say it has forced them to hire and train junior employees rather than bring on more experienced cyber security professionals, and 35% say that the cyber security skills shortage has led to the inability to learn or fully utilize some of their security technologies.



- **Organizations have acute cyber security skills deficiencies in several areas.** Aside from day-to-day operational issues, many organizations have severe skills shortage in particular areas. For example, one-third of organizations say they have a shortage of security analysis and investigation skills, 32% report skills shortages with application security, 22% claim to have a shortage of cloud security skills, and 21% are deficient in security engineering. It is worth noting that these skills may require years of practical experience or knowledge in both security and other technology areas. This means that firms will need to compete heavily to acquire these skills.



- **Cyber security professionals have several suggestions to help improve the current situation.** Cyber security professionals were asked what type of cyber security actions would be most helpful to their organizations. Forty-one percent suggested increasing the cyber security budget, 40% proposed adding cyber security goals and metrics to business and IT managers' objectives, 39% recommended increasing cyber security training for non-technical employees, and 39% advised hiring more cyber security professionals.



- **Critical infrastructure is very vulnerable to cyber-attacks.** A majority (62%) of cyber security professionals believe that their country's critical infrastructure services like electric power, telecommunications, and water are very vulnerable to some type of significant cyber-attack.



- **Government cyber security tends to be incoherent and incomplete.** More than one-fourth (26%) of cyber security professionals surveyed say that their country's cyber security strategy is extremely unclear and not at all thorough while another 37% claim that their country's cyber security strategy is somewhat unclear and not very thorough. This leads to an obvious conclusion: If cyber security professionals don't understand their country's cyber security strategy, who does?







- **Cyber security professionals want more help from their governments.** More than half (57%) of cyber security professionals believe that their government should be significantly more active with cyber security strategy and defense while another 32% say that their government should be somewhat more active with cyber security strategy and defense. What types of programs would they like to see? Fifty-four percent suggest that their government create better ways to share security information with the private sector, 44% want the government to provide incentives to organizations that improve cyber security, and 43% would like their government to provide funding for cyber security training and education.

This report builds upon the conclusions of the previously published report, [*The State of Cyber Security Professional Careers*](#), focused on the lifecycle of cyber security professional careers. As a review, the first report also revealed some alarming conclusions:



- **Most cyber security professionals struggle to define their career paths.** Nearly two-thirds (65%) of respondents do not have a clearly defined career path or plans to take their careers to the next level. This is likely due to the diversity of cyber security focus areas, the lack of a well-defined professional career development standard and map, and the rapid changes in the cyber security field itself. Business, IT, and cyber security managers, academics, and public policy leaders should take note of today's cyber security career morass and develop and promote more formal cyber security guidelines and frameworks that can guide cyber security professionals in their career development in the future. Independent organizations such as the ISSA with its Cyber Security Career Lifecycle are taking the lead on such initiatives.

- **Cyber security professionals have solid ideas for skills advancement.** When asked how they improve their knowledge, skills, and abilities (KSAs), cyber security professionals pointed to activities like attending specific cyber security training courses (58%), participating in professional organizations (53%), and engaging in on-the-job mentoring from more experienced cyber security professionals (37%). Responses varied by seniority with experienced cyber security managers (i.e., CISOs, VPs, Directors, etc.) leaning toward professional organizations while cyber security staff members favored on-the-job mentoring.
- **Cyber security certifications are a mixed bag.** Over half (56%) of survey respondents had received a CISSP and felt it was a valuable certification for getting a job and gaining useful cyber security knowledge. Other than the CISSP certification, however, cyber security professionals appear lukewarm on other types of industry certifications. Based upon this data, it appears that security certifications should be encouraged for specific roles and responsibilities, but downplayed as part of a cyber security professional's overall career and skills development.
- **Continuous cyber security training is lacking.** When asked if their current employer provides the cyber security team with the right level of training to keep up with business and IT risk, more than half (56%) of survey respondents answered "no," suggesting that their organizations needed to provide more or significantly more training for the cyber security staff. This represents one of the "red flags" uncovered in this research project. Organizations that don't provide continuous training to cyber security staff will fall further behind cyber-adversaries while increasing business and IT risk. This should be an unacceptable situation for all business and technology managers.
- **Cyber security professionals are in extremely high demand.** This is another critical data point exposed in this research project, as 46% of cyber security professionals are solicited to consider other cyber security jobs (i.e., at other organizations) at least once per week. In other words, cyber security skills are "a seller's market" where experienced professionals can easily find lucrative offers to leave one employer for another. Turnover in the cyber security ranks could represent an existential risk to organizations in lower-paying industries like academia, health care, the public sector, and retail.
- **Many CISOs are not getting enough face time in the boardroom.** While industry rhetoric claims that "cyber security is a boardroom issue," 44% of respondents believe that CISO participation with executive management is not at the right level today and should increase somewhat or significantly in the future. Alarming, this perspective is more common with more experienced cyber security managers (who should be working with the business) than cyber security staff members.
- **Internal relationships need work.** While many organizations consider the relationship between cyber security, business, and IT teams to be good, it is concerning that 20% of cyber security professionals say the relationship between cyber security and IT is fair or poor, and 27% of survey respondents claim the relationship between cyber security and the business is fair or poor. The biggest cyber security/IT relationship issue selected relates to prioritizing tasks between the two groups while the biggest cyber security/business relationship challenge is aligning goals. The report data reveals that cyber security and IT teams are taking steps to improve collaboration but also uncovers that more work is necessary to bridge the gap between cyber security and business management.
- **CISO turnover has business and economic roots.** When asked why CISOs tend to seek new jobs after a few short years, cyber security professionals responded that CISOs tend to move on when their organizations lack a serious cyber security culture (31%), when CISOs are not active participants with executives (30%), or when CISOs are offered higher compensation elsewhere (27%). To retain strong CISOs, organizations must not only provide competitive compensation but also make a serious commitment to cyber security executives and comprehensive programs.

Introduction

The background of the slide features a complex geometric pattern. It consists of a grid of squares in various shades of blue, with some squares being white. Overlaid on this grid are several thin, white diagonal lines that create a sense of movement and depth. The pattern is most prominent in the lower half of the slide, where it appears to recede into the distance.

Research Objectives

In order to assess the experiences, careers, and opinions of cyber security professionals, ESG and ISSA surveyed 437 cyber security professionals representing organizations of all sizes and across all industries and geographic locations. Survey respondents were also ISSA members.

The first report titled, *The State of Cyber Security Professional Careers*, examines topics such as:

- **Cyber security careers**
- **Cyber security skills development**
- **Cyber security organizational considerations**

This second report in this two-part series focuses on:

- **Security incidents and vulnerabilities**
 - Have organizations suffered security incidents? If so, which types of security incidents?
 - What factors contributed to these incidents?
 - Do cyber security professionals believe that organizations are vulnerable to cyber-attacks?
 - Do cyber security professionals believe that their employers are vulnerable to cyber-attacks?
 - Do cyber security professionals believe that critical infrastructure services in their countries are vulnerable to significant cyber-attacks?
- **The cyber security skills shortage**
 - Do cyber security professionals believe that their organizations have been impacted by the global cyber security skills shortage? If so, in what way?
 - In which areas do their organizations have the biggest cyber security skills deficits?
- **Cyber security activities**
 - What types of cyber security actions have organizations taken over the past few years?
 - What additional actions should organizations take to help improve cyber security overall?
- **Cyber security and government strategy**
 - Are government cyber security strategies clear and/or thorough?
 - Is the government providing the right level of cyber security help?
 - What further actions, if any, should governments be taking with regards cyber security incentives, investments, and programs?



Survey participants represented a wide range of industries including financial services, manufacturing, business services, communications and media, and government. For more details, please see the *Research Methodology* and *Respondent Demographics* sections of this report.



Research Findings



The ISSA Survey Respondents

According to previously published ESG research, 70% of organizations planned to increase cyber security spending in 2016 while 59% claimed that cyber security budgets would rise in 2015. Just what types of infosec activities were they focused on in this two-year timeframe? Respondents to the ESG/ISSA survey said that their organizations have taken actions like engaging in new cyber security initiatives, increasing security oversight for privileged users, and adding headcount to the cyber security team (see Figure 1).

It is worth noting how tightly grouped the top ten responses are, ranging from 35% to 49%. This indicates that many organizations have taken numerous actions simultaneously to address changing cyber security requirements.

When it comes to cyber security, the largest and smallest organizations in the survey population have some common and opposing behavior. For example, about one-third of large and small organizations have increased cyber security training for non-technical employees and IT staff, prepared to adhere to one or several regulatory compliance requirements, and implemented stronger access controls for sensitive applications and data. Beyond these similarities, however, large enterprise organizations were much more active in several areas (see Table 1). While these results are not surprising, smaller organizations should review the behavior of large enterprises and assess whether they need to move forward in some of these areas as they develop cyber security plans for the future.

Why are organizations taking a multitude of cyber security actions? Clearly many want to address business and IT risk or bolster security controls as countermeasures to the increasingly dangerous threat landscape. Nevertheless, the ESG/ISSA data also points to another issue as many organizations are simply responding to a wave of cyber-attacks they've experienced over the past year (see Figure 2).

It should be noted that between 23% and 30% of the survey population responded "don't know" or "prefer not to say" in each of the responses in Figure 2. Upon further review, ESG/ISSA believes that these responses were dominated by junior cyber security respondents who may not have been comfortable or knowledgeable enough to answer these questions. For example, the percentage of CISOs acknowledging each type of security incident was higher than those of the overall survey population (see Table 2). This may indicate that security events are more prevalent than many junior security professionals realize.

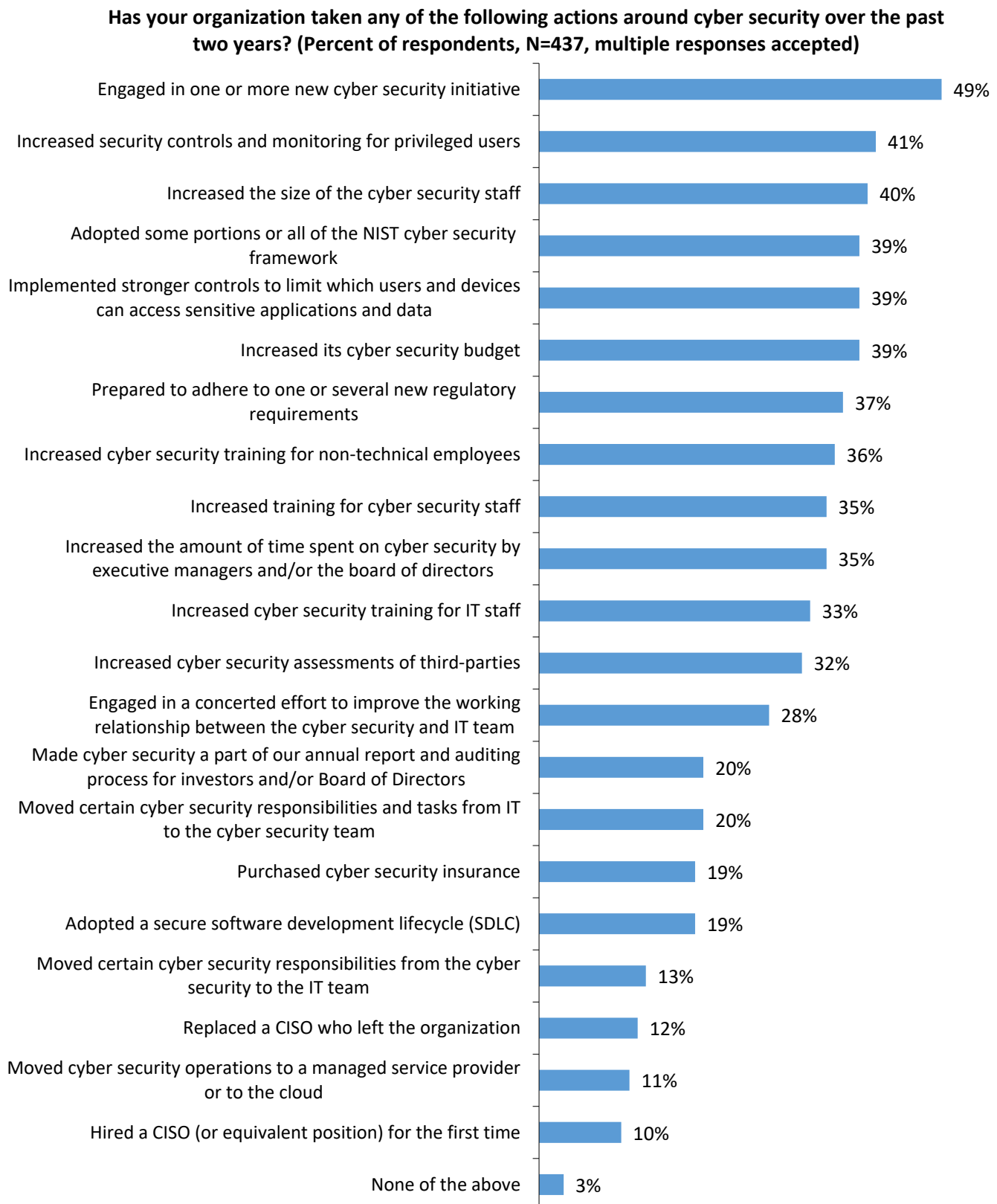
In aggregate, 54% of the cyber security professionals surveyed for this project admitted that their organization experienced at least one type of security event over the past year. Given this frightening reality, survey respondents were also asked to voice their opinion on the factors that may have led to these events. It is noteworthy that none of the top issues cited are related to cyber security technology. Rather, infosec professionals point to resource constraints such as the size of the cyber security organization, a lack of cyber security training for non-technical employees, and an inadequate cyber security budget (see Figure 3).

A few points stand out in this data:

- Nearly one-third (31%) of respondents say that their cyber security organization isn't large enough for their organizations. The problem here is that many of these organizations will not be able to hire their way out of this problem due to the global cyber security skills shortage. CISOs at these organizations will likely have to turn to other options like enhanced cyber security automation and orchestration or a greater reliance on managed security services. Additionally, many organizations believe that they are too small to have a cyber security program, or that they are not a big enough company to really have to worry about cyber security. This only compounds the issues.
- In spite of a constant barrage of data breaches and cyber security headlines or industry hype proclaiming cyber security is a "boardroom-level" issue, 21% of respondents indicate that business and executive management tend to treat cyber security as a low priority. Organizations that continue to ignore cyber security do so at their own

peril. These firms will likely experience a multitude of security events, alienate the cyber security staff, and be held accountable for lapses by angry shareholders, business partners, and others.

Figure 1. Actions Taken Around Cyber Security Over the Past Two Years



Source: Enterprise Strategy Group and ISSA, 2016

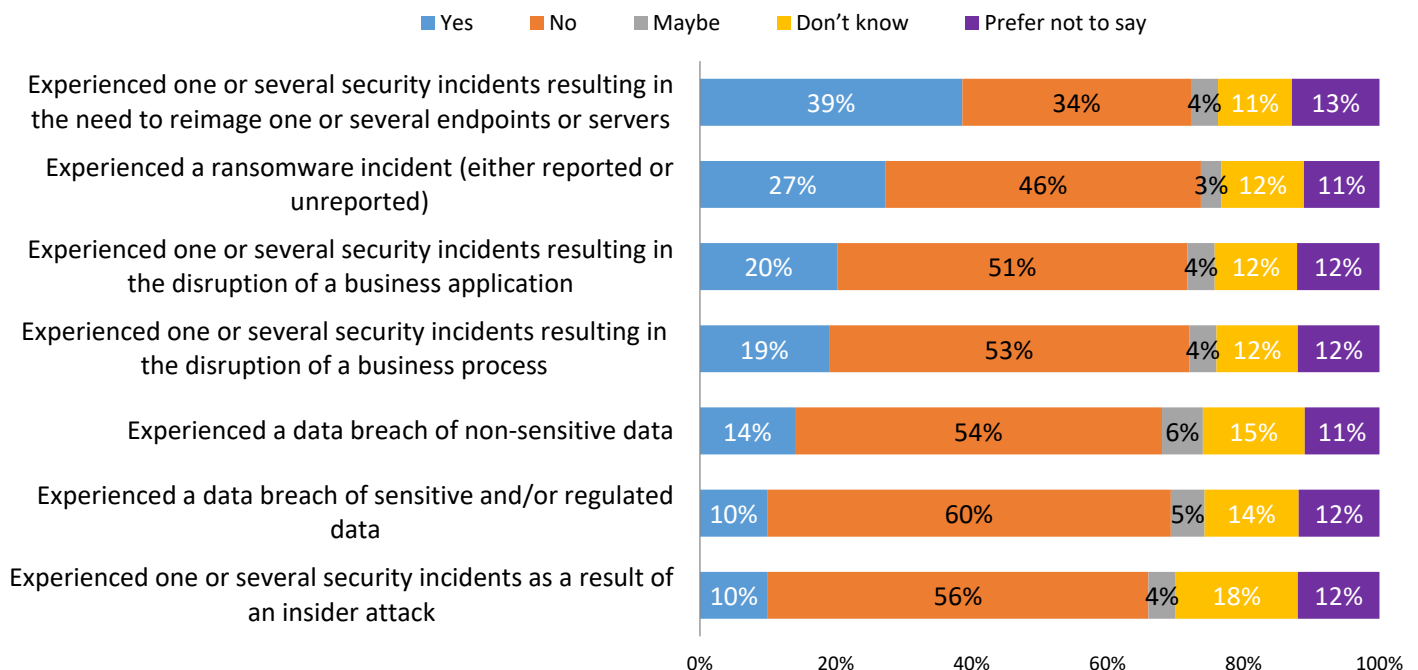
Table 1. Actions Taken Around Cyber Security Over the Past Two Years by Size of Organization

| | Organizations with fewer than 1,000 employees (N=173) | Organizations with more than 20,000 employees (N=96) |
|---|---|--|
| Increased cyber security training for non-technical employees | 32% | 31% |
| Increased cyber security training for IT staff | 33% | 36% |
| Prepared to adhere to one or several new regulatory compliance requirements | 34% | 35% |
| Implemented stronger controls to limit which users and devices can access sensitive applications and data | 35% | 39% |
| Increased cyber security budget | 27% | 49% |
| Increased the size of the cyber security staff | 21% | 57% |
| Increased training for the cyber security staff | 26% | 44% |
| Engaged in one or more new cyber security initiative (i.e., deploying new types of cyber security technologies) | 38% | 55% |
| Adopted some portions or all of the NIST cyber security framework | 33% | 47% |
| Increased security controls and monitoring for privileged users (i.e., IT administrators, etc.) | 32% | 52% |
| Increased cyber security assessments of third-parties | 25% | 42% |

Source: Enterprise Strategy Group and ISSA, 2016

Figure 2. Security Events Respondent Organizations Experienced Over the Last Year

**Over the past year, has your organization experienced any of the following security events?
(Percent of respondents, N=437)**



Source: Enterprise Strategy Group and ISSA, 2016

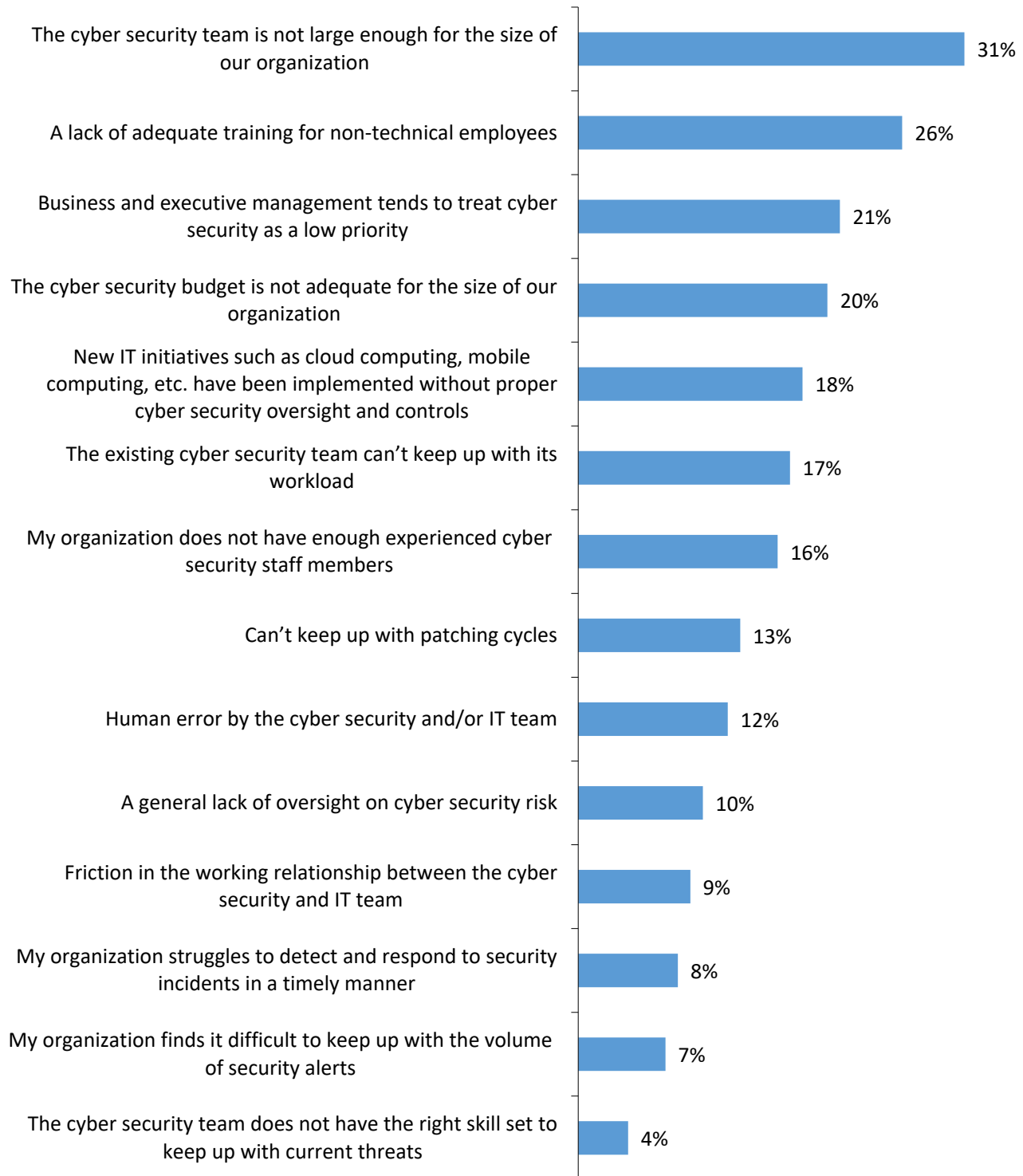
Table 2. Security Events Respondent Organizations Experienced Over the Last Year, by CISOs

| | CISOs acknowledging various types of security incidents (N=61) | Overall survey population acknowledging various types of security incidents (N=437) |
|--|--|---|
| One or several security incidents resulting in the disruption of a business application | 25% | 20% |
| One or several security incidents resulting in the disruption of a business process | 23% | 19% |
| One or several security incidents resulting in the need to reimage one or several endpoints or servers | 43% | 39% |
| One or several security incidents as a result of an insider attack | 16% | 10% |
| Experienced a data breach of non-sensitive data | 18% | 14% |
| Experienced a data breach of sensitive and/or regulated data | 20% | 10% |
| Experienced a ransomware incident | 33% | 27% |

Source: Enterprise Strategy Group and ISSA, 2016

Figure 3. Biggest Contributors to Security Events Experienced by Organizations

Which of the following factors were the biggest contributors to the security events your organization experienced in the last year? (Percent of respondents, N=234, three responses accepted)



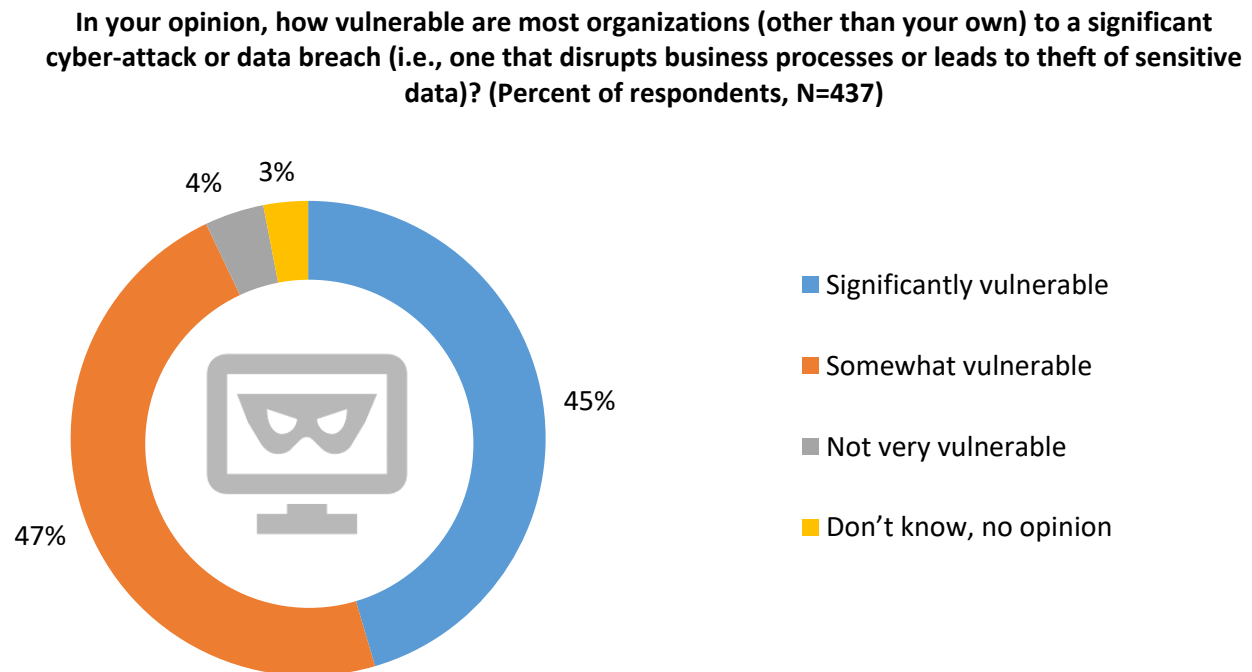
Source: Enterprise Strategy Group and ISSA, 2016

Are Organizations Vulnerable to Cyber-attacks?

Cyber security professionals were asked a few questions about the overall state of the cyber security threat and just how vulnerable organizations are to a cyber-attack and potential data breach. Once again the results are troubling—45% of survey respondents believe that most organizations are significantly vulnerable to a cyber-attack or data breach while another 47% say that most organizations are somewhat vulnerable to a cyber-attack or data breach (see Figure 4).

The clear majority (92%) of cyber security professionals believe that an average organization is vulnerable to some type of cyber-attack or data breach. Alarming, 44% also think that their own organization is as vulnerable or even more vulnerable to these kinds of cyber security incidents (see Figure 5). Why are cyber security professionals so pessimistic? Because they have extensive situational awareness of today's cyber security landscape. They understand that cyber-adversaries are more numerous and sophisticated, making the threat landscape increasingly dangerous. Unfortunately, as the ESG/ISSA research reveals, they also know that they are currently understaffed, receive inadequate levels of training, are under-resourced, and lack the right level of support and cooperation from their organizations in some cases. This data should set off alarm bells for not only CISOs but also business managers, consumers, and government officials.

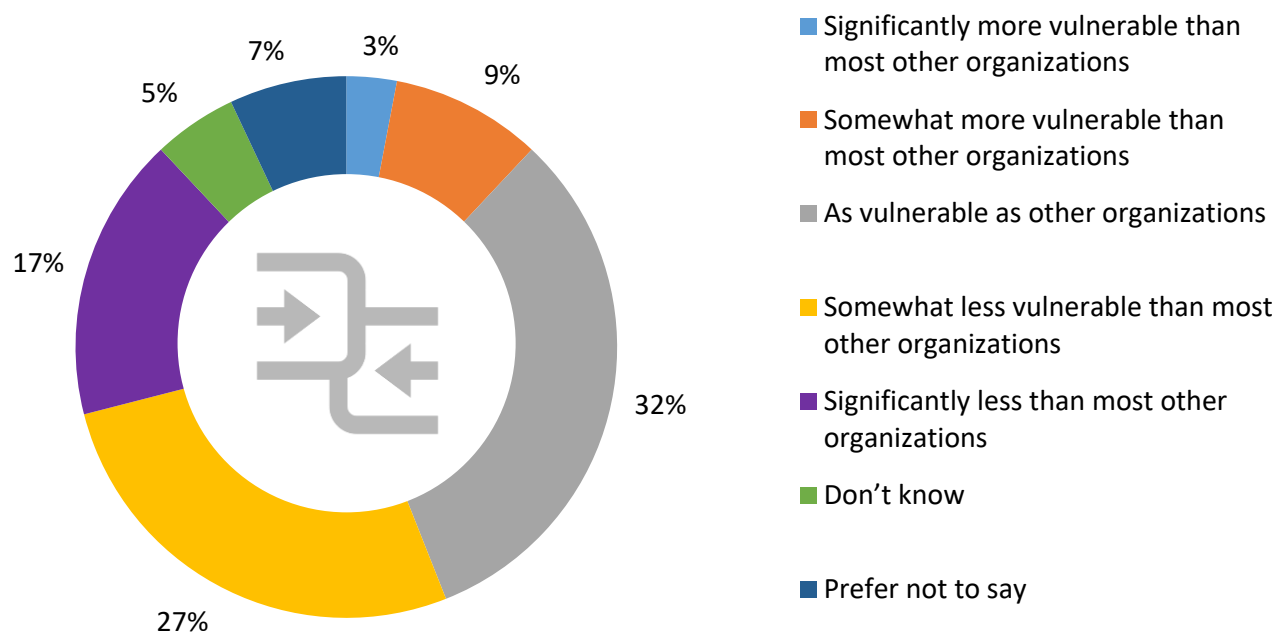
Figure 4. Vulnerability of Most Organizations to a Significant Cyber-attack or Data Breach



Source: Enterprise Strategy Group and ISSA, 2016

Figure 5. Vulnerability of Respondent Organizations to a Significant Cyber-attack or Data Breach Compared to Other Organizations

How vulnerable would you say your organization is to a significant cyber-attack or data breach (i.e., one that disrupts business processes or leads to theft of sensitive data) compared to other organizations in your industry? (Percent of respondents, N=437)



Source: Enterprise Strategy Group and ISSA, 2016

The Cyber Security Skills Shortage

ESG has written extensively about the cyber security skills shortage over the past several years. As previously stated, early 2016 research revealed that 46% of organizations claim they have a problematic shortage of cyber security skills at present, an 18% increase from 2015.

Other industry research also recognizes the cyber security skills shortage problem. For example:



- Job market analytics vendor [Burning Glass](#) states that cyber security job postings grew 74% from 2007 to 2013, more than *twice the growth rate* of all IT jobs.



- In 2015, prospective employers posted more than 50 thousand jobs requesting Certified Information Systems Security Professional (CISSP) certification. Unfortunately, there are only about 105 thousand CISSPs in the world, and many are gainfully employed.



- [ISC2](#), the organization that certifies CISSPs, believes that there will be a deficit of 1.5 million cyber security professionals by 2020. The UK House of Lords is even more bearish, predicting a shortage of two million cyber security professionals by 2017.

While the industry at large has come to recognize a cyber security skills shortage, ESG and ISSA wanted to understand how this issue is impacting organizations today. As it turns out, 29% of cyber security professionals say that the cyber security skills shortage has had a significant impact on their organizations, while 40% claim that their organizations have been impacted somewhat by the global cyber security skills shortage (see Figure 6).

It is also worth noting that the global cyber security skills shortage has impacted organizations of all sizes. In other words, smaller organizations (i.e., fewer than 1,000 employees) and large enterprises (i.e., more than 20,000 employees) are all impacted by the lack of available cyber security talent.

Previous ESG research reveals one implication of the global cyber security skills shortage. When asked to characterize how difficult it is to recruit and hire cyber security professionals, 13% of respondents said very difficult, 29% said difficult, and 44% said somewhat difficult. Beyond recruiting and hiring, however, the cyber security skills shortage is also creating day-to-day ramifications for existing cyber security teams. For example:



- More than half (54%) of the cyber security professionals surveyed indicate that the cyber security skills shortage leads to an increasing workload on existing staff. This excess workload may contribute to the fact that 32% claim that the cyber security skills shortage has driven high attrition rates and turnover, while 25% of respondents say that the cyber security skills shortage has created a high burnout rate for cyber security staff.



- More than one-third (35%) of respondents say that their organizations have had to hire and train junior employees rather than seasoned cyber security professionals. While this strategy may be necessary, it also means that many organizations suffer from a cyber security skills gap while they educate and train junior staff.



- More than one-third (35%) of respondents say that the cyber security skills shortage causes an inability to fully learn or utilize some of their security technologies to their full potential. In other words, time is a limiting factor as the cyber security team is spending an inordinate amount of time putting out fires and not enough time configuring and operating their security controls as effectively as possible.

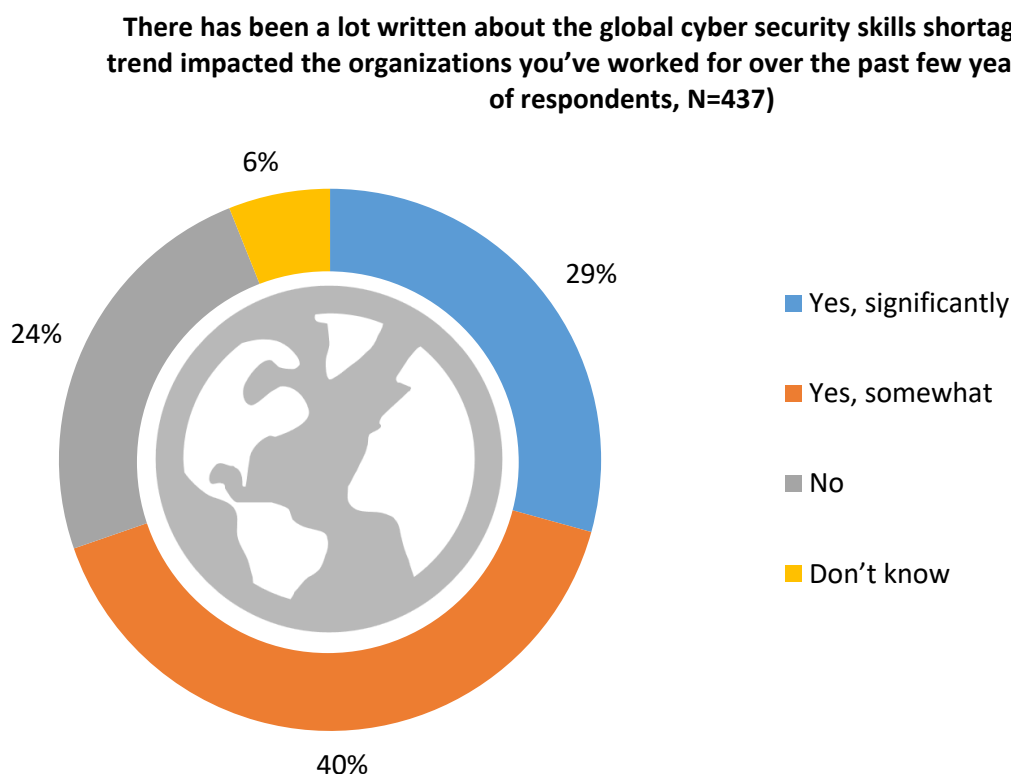
On a similar note, nearly one-third (32%) of cyber security professionals say that they have limited time for training since the cyber security team is too busy keeping up with day-to-day responsibilities. Like medicine, cyber security knowledge is

in a constant state of progress. Therefore, when cyber security professionals can't keep up with training, the organizations they work for face a steady state of increasing risk (see Figure 7).

Survey respondents were also asked to identify the specific cyber security areas where their organizations had the biggest shortage. The data indicates that:

- One-third claim a shortage of security analysis and investigations skills. This is a real problem as security analysts and investigators tend to have many years of hands-on experience. Since this role can't be filled by junior personnel, CISOs have no choice but to steal individuals from other organizations or delegate some or all security analysis and investigation tasks to third-party service providers.
- Just less than one-third (32%) report a skills deficit with regard to application security. This creates an especially difficult situation as application security specialists are often called upon to work with developers on the front-end of software development projects, and application testers are tasked on the back-end. In this case, CISOs and CIOs may want to invest in secure software development programs and automated tools to try to alleviate the burden on the infosec team.
- Twenty-two percent point to a shortfall of cloud security specialists. This is likely to increase as organizations move more workloads to the cloud. Unfortunately, these skills will continue to be scarce as they depend upon rare individuals with strong cyber security *and* cloud knowledge (see Figure 8).

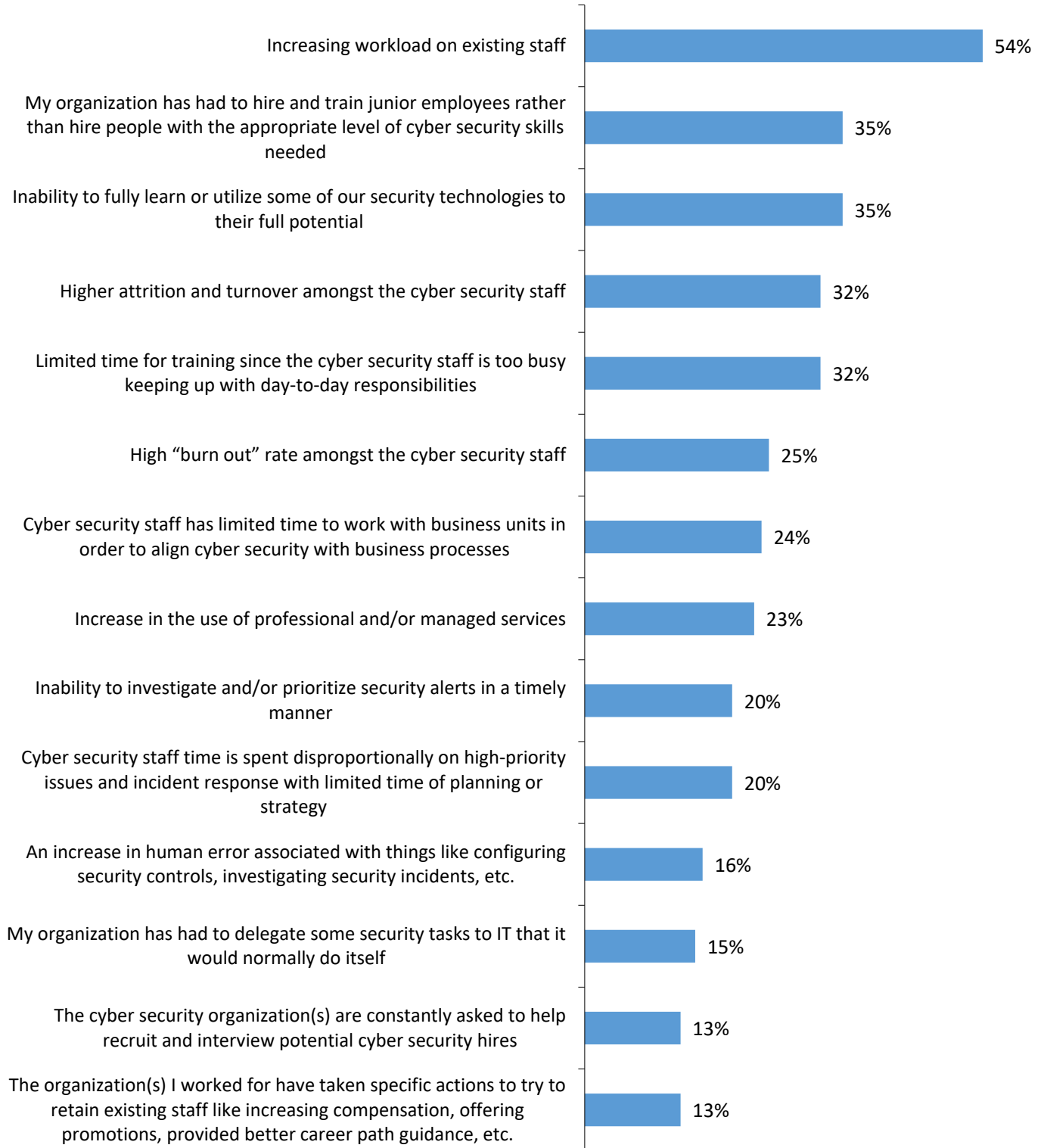
Figure 6. Impact of Cyber Security Skills Shortage



Source: Enterprise Strategy Group and ISSA, 2016

Figure 7. How Cyber Security Skills Shortage Has Impacted Organizations

You indicated that the organizations you've worked for over the past few years were impacted by the global cyber security skills shortage. What type of impact did the global cyber security skills shortage have on these organizations? (Percent of respondents, N=303, multiple responses accepted)



Source: Enterprise Strategy Group and ISSA, 2016

Figure 8. Area(s) with Biggest Shortage of Cyber Security Skills

In which of the following areas would you say that your organization has the biggest shortage of cyber security skills? (Percent of respondents, N=437, three responses accepted)









Source: Enterprise Strategy Group and ISSA, 2016

Bridging the Cyber Security Gap

The data presented in this ESG/ISSA research report (as well as the previous one published earlier this year) indicates a number of existing cyber security challenges. Many cyber security professionals are overworked, leading to lapses with skills training, security technology operations, and best practices. At the same time, many organizations continue to underemphasize cyber security, leading to a toxic work environment and inappropriately increasing IT risks.

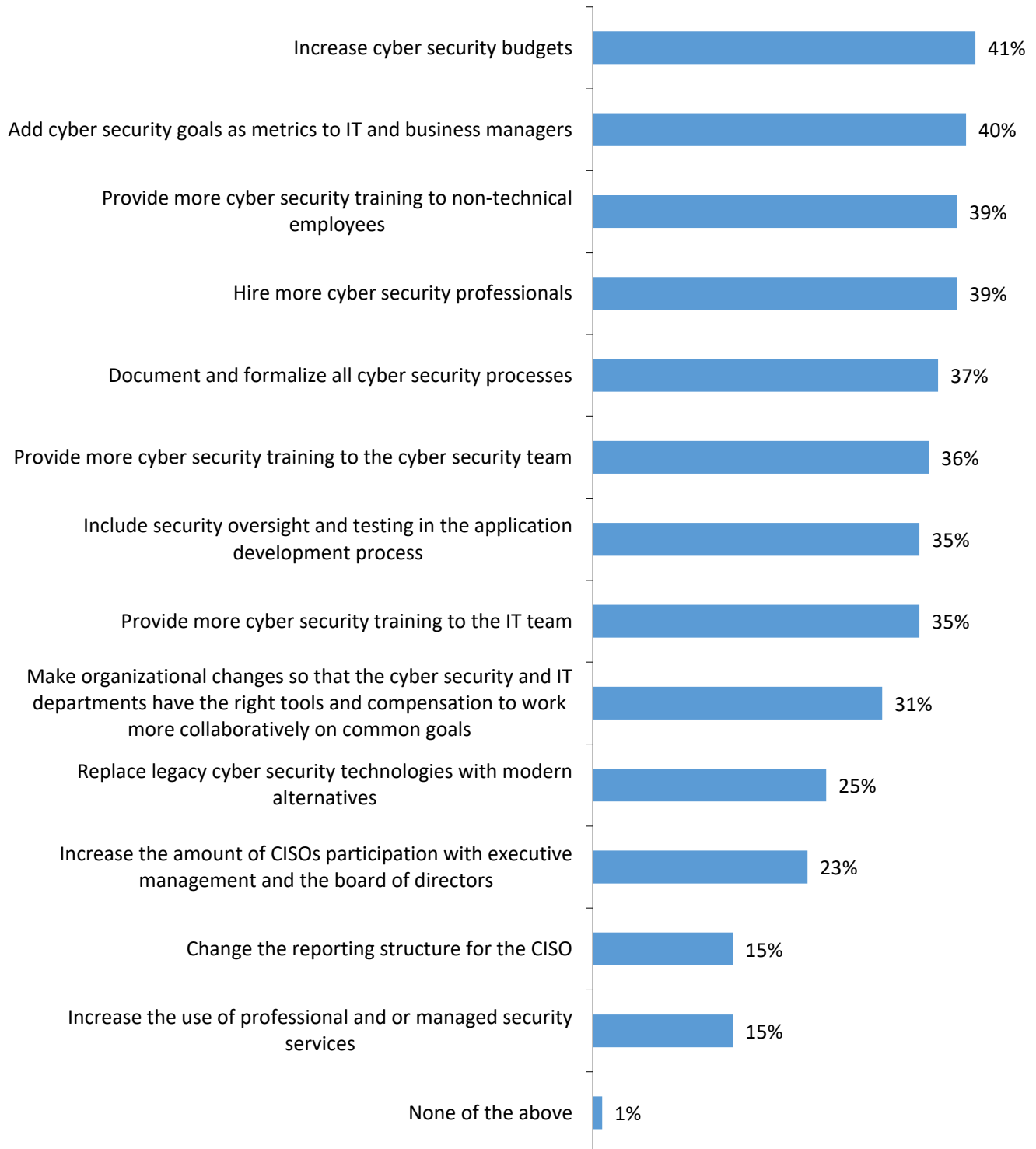
What steps should organizations take to address these critical issues? The cyber security professionals surveyed for this project have many suggestions (see Figure 9). In fact, one-third or more respondents came up with six different suggestions. For example:

-  • Forty-one percent of respondents would increase their organization's cyber security budget. Money is always an important component of improvement, so other responses provide a bit more insight.
-  • Forty percent of respondents say add cyber security goals as metrics to IT and business managers. So, cyber security professionals believe that overall cyber security could improve at their organizations if business and IT managers were invested in and accountable for cyber security. This type of "carrot and stick" approach has proven useful in industries like financial services.
-  • Thirty-nine percent of respondents suggest providing more cyber security training to non-technical employees. This is consistent with data appearing previously in Figure 3 of this report where 26% of respondents indicated that a lack of training of non-technical employees actually contributed to their experiences with security events. While many organizations offer some level of security training, it is often a one-time event highlighting basic cyber security concepts and hygiene. Cyber security professionals clearly believe this level of training is inadequate.
-  • Similarly, 39% of respondents propose hiring more cyber security professionals. Of course, this will be difficult due to the global cyber security skills shortage. Organizations will only be successful with this approach if they offer best-in-class compensation and establish and market themselves as a cyber security center of excellence.
-  • Thirty-seven percent of respondents recommend documenting and formalizing cyber security processes. This is a good suggestion as it can help organizations streamline operations and establish best practices. ISO and NIST standards can serve as a template to help here.
-  • Thirty-six percent of respondents advocate for more training for cyber security teams. This is an important consideration since the earlier [report](#) from ESG and ISSA revealed that 56% of cyber security professionals believe that their organizations should provide a bit more or significantly more training so the cyber security team can keep up with business and IT risk. Given this, increasing cyber security training should be a high priority for CISOs.

Responses varied slightly by role. Note that cyber security management recommends higher budgets, more business participation, and organizational changes while cyber security staff suggest an increase in training (see Table 3). This dichotomy illustrates differences in tactical and strategic thinking. While management's suggestions are worthwhile and supported in the ESG/ISSA research, CISOs should also enlist input from the cyber security staff so that tactical issues like the lack of cyber security training across the organization are not neglected.

Figure 9. Actions That Would Provide the Most Cyber Security Benefits to Organization

Which of the following actions would provide the most cyber security benefits for your organization moving forward? (Percent of respondents, N=437, multiple responses accepted)



Source: Enterprise Strategy Group and ISSA, 2016

Table 3. Actions That Would Provide the Most Cyber Security Benefits to Organization, by CISOs

| | Cyber security senior management (director, VP, CISO, CSO, etc.) (N=137) | Cyber security staff (admin, management, staff) (N=213) |
|---|--|---|
| Provide more cyber security training to the cyber security team | 28% | 41% |
| Provide more cyber security training to the IT team | 32% | 36% |
| Provide more cyber security training to non-technical employees | 35% | 38% |
| Increase the amount of CISO's participation with executive management and the board of directors | 36% | 16% |
| Increase cyber security budgets | 47% | 39% |
| Increase the use of professional and or managed security services | 19% | 11% |
| Change the reporting structure for the CISO (i.e., make changes so that the CISO reports to a different person than he or she currently does) | 24% | 14% |

Source: Enterprise Strategy Group and ISSA, 2016

Government and Cyber Security

In February 2016, U.S. President Barack Obama directed his administration to implement the Cybersecurity National Action Plan ([CNAP](#)), which included:

- The establishment of a commission on enhancing national cyber security.
- Government IT modernization.
- Strong authentication initiatives to help citizens secure their online activities.
- A \$19 billion investment as part of the president's fiscal year 2017 budget proposal.

This U.S. plan is just the latest in a series dating back through several administrations. Other national governments are undertaking cyber security initiatives of their own.

Are these efforts worthwhile? Asked another way, are nations really vulnerable to some type of cyber-attack on critical infrastructure that could lead to devastating results? The cyber security professionals surveyed for this research project clearly believe this to be the case—62% say that their country is very vulnerable to a significant cyber-attack on its critical infrastructure, while another 35% claim that their country is somewhat vulnerable to this type of attack (see Figure 10).

Of course, national governments also recognize cyber-vulnerabilities around critical infrastructure. This is one reason that many have established various cyber security policies, programs, and initiatives. Unfortunately, many government cyber security strategies remain nebulous at best—at least within the cyber security professional community. As the ESG/ISSA research illustrates, 26% of cyber security professionals say that their government's cyber security strategy is extremely unclear and not at all thorough, while another 37% claim that their government's cyber security strategy is somewhat unclear and not very thorough (see Figure 11).

It is also worth noting that one-third (33%) of CISOs surveyed believe that their government's cyber security strategy is extremely unclear and not at all thorough. In other words, those cyber security professionals with the most experience and exposure to government cyber security strategies still believe that their governments are not delivering a cogent set of cyber security messages and programs.

Government programs may be unclear and incomplete, but that doesn't mean they are unwelcome. In fact, the ESG/ISSA data reveals that the opposite is true—57% of cyber security professionals believe that their government should be significantly more active with cyber security strategies and defenses, while 32% say that their government should be somewhat more active with cyber security strategies and defenses (see Figure 12).

Survey respondents were also asked to identify the cyber security actions their government should take, assuming it ratcheted up its commitment in this area. The top responses included the following (see Figure 13):

- Just over half (54%) of cyber security professionals want governments to create better ways to share information with the private sector. Of course, this has been proposed often before. For example, the [Cybersecurity Information Sharing Act](#) (S.754) is described as a bill meant to “develop procedures to share cybersecurity threat information with private entities, nonfederal government agencies, state, tribal, and local governments, the public, and entities under threats.” Cyber security professionals may want governments to go beyond legislation alone and provide further help by developing and promoting threat intelligence sharing standards and investing in technology infrastructure that can help automate and enable asymmetric, ad-hoc, and trusted threat intelligence sharing among loosely coupled networked organizations.





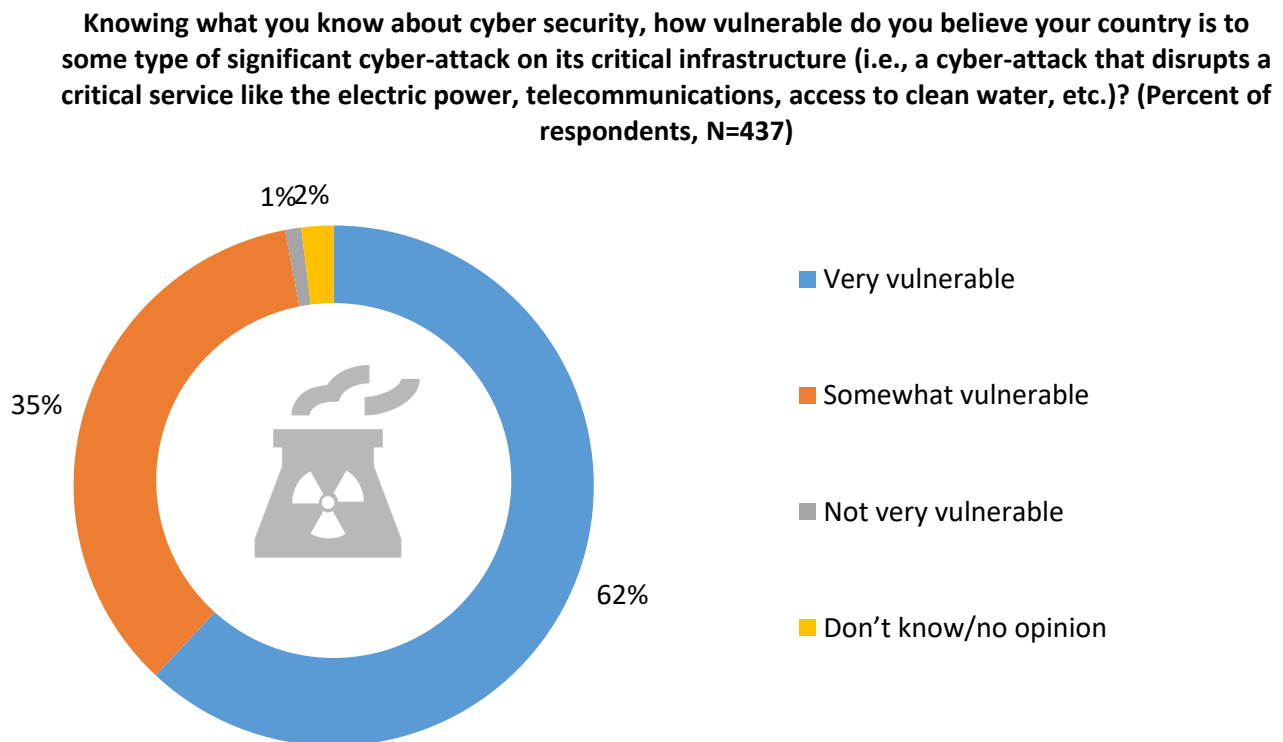
- Forty-four percent of cyber security professionals recommend that governments provide incentives that improve cyber security. For example, federal governments could provide tax breaks for organizations that increase cyber security training and invest in additional cyber security defenses and monitoring capabilities.



- Forty-three percent believe that governments should provide funding for cyber security professional training and education. While some governments have dedicated some cyber security education funding, these programs tend to be done on an ad-hoc basis. Cyber security professionals would like to see a more centralized and strategic approach to such investments in more cyber security centers of excellence. Given the problems around cyber security training exposed by this research project, more government-sponsored cyber security training would be a wise investment of taxpayer money.

Once again, CISOs tended to have stronger opinions about government priorities than the survey population at large (see Table 4).

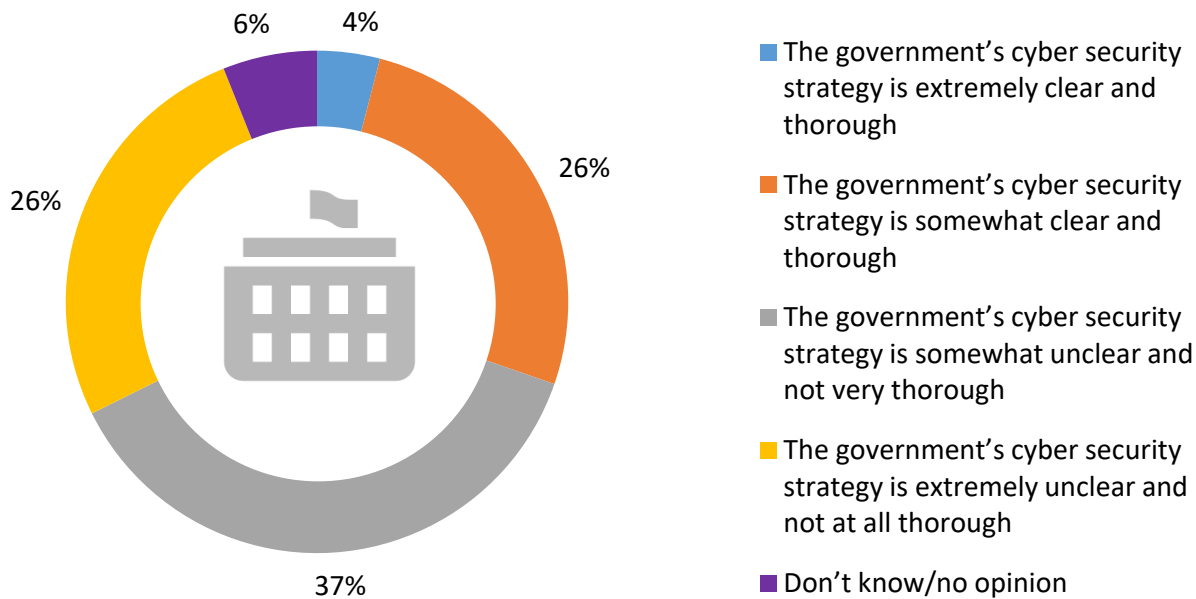
Figure 10. Vulnerability of Respondents' Country to a Cyber-attack



Source: Enterprise Strategy Group and ISSA, 2016

Figure 11. Respondents' Sentiment on Cyber Security Strategy of Their Country's Government

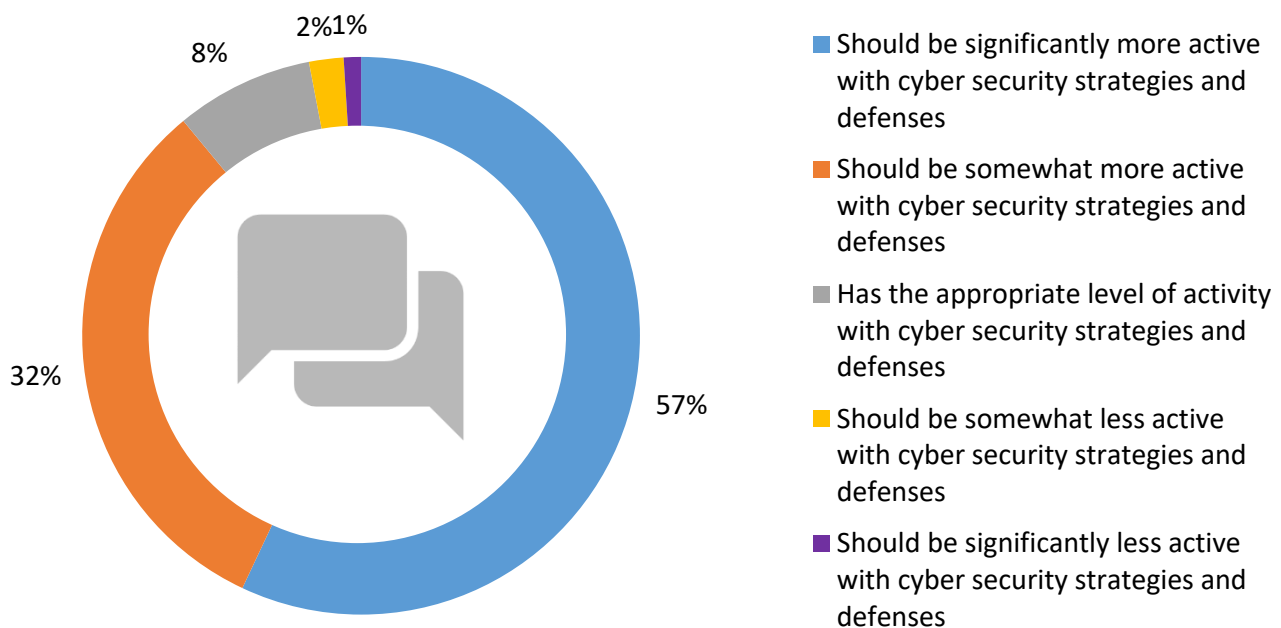
Which statement best reflects your opinion on the cyber security strategy of your country's government? (Percent of respondents, N=437)



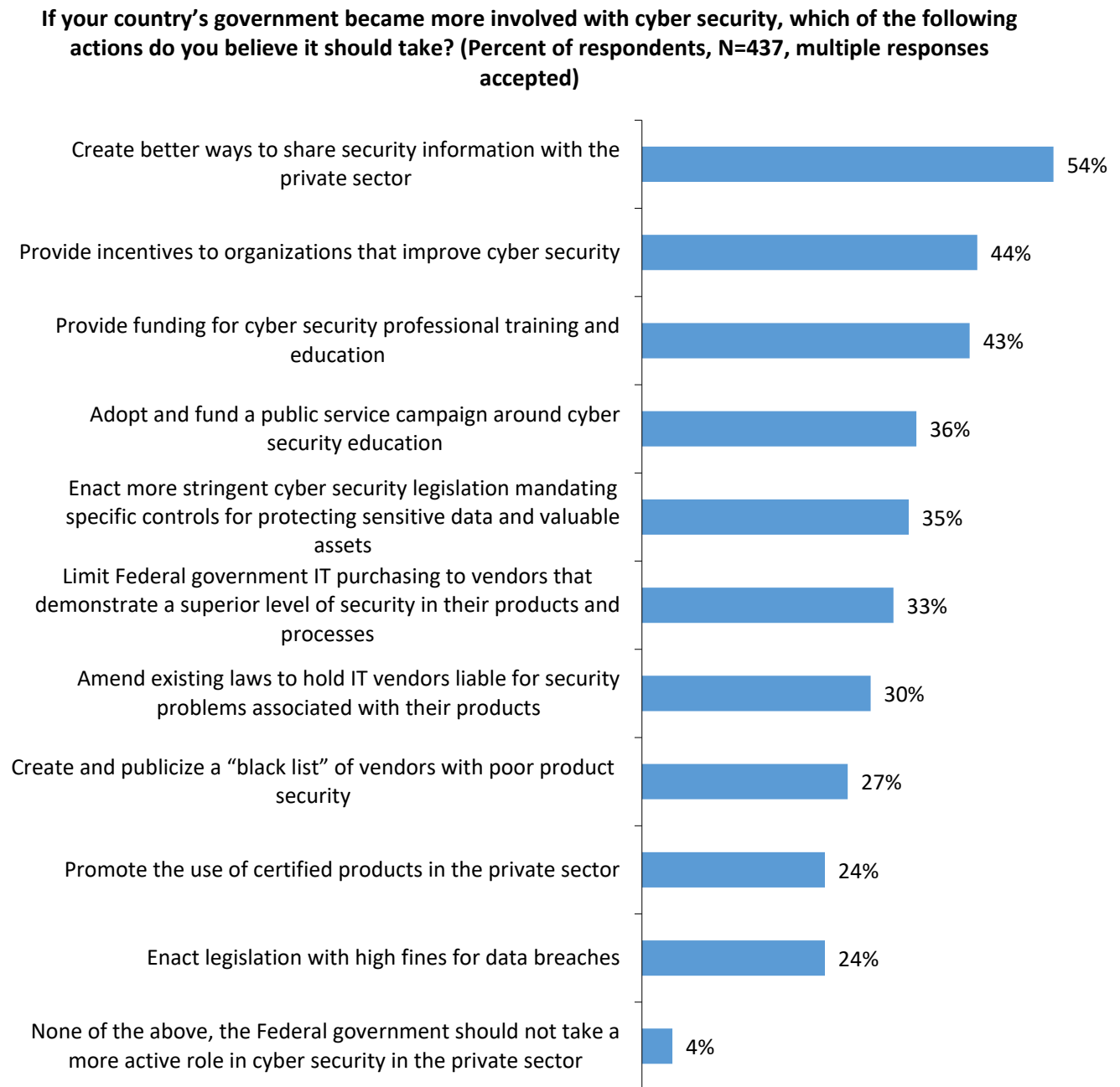
Source: Enterprise Strategy Group and ISSA, 2016

Figure 12. How Active Government Should Be in Cyber Security

Please respond to this statement by selecting one of the following responses. "In my opinion, the government of my country..." (Percent of respondents, N=437)



Source: Enterprise Strategy Group and ISSA, 2016

Figure 13. Actions Government Should Take If It Were to Become More Involved with Cyber Security

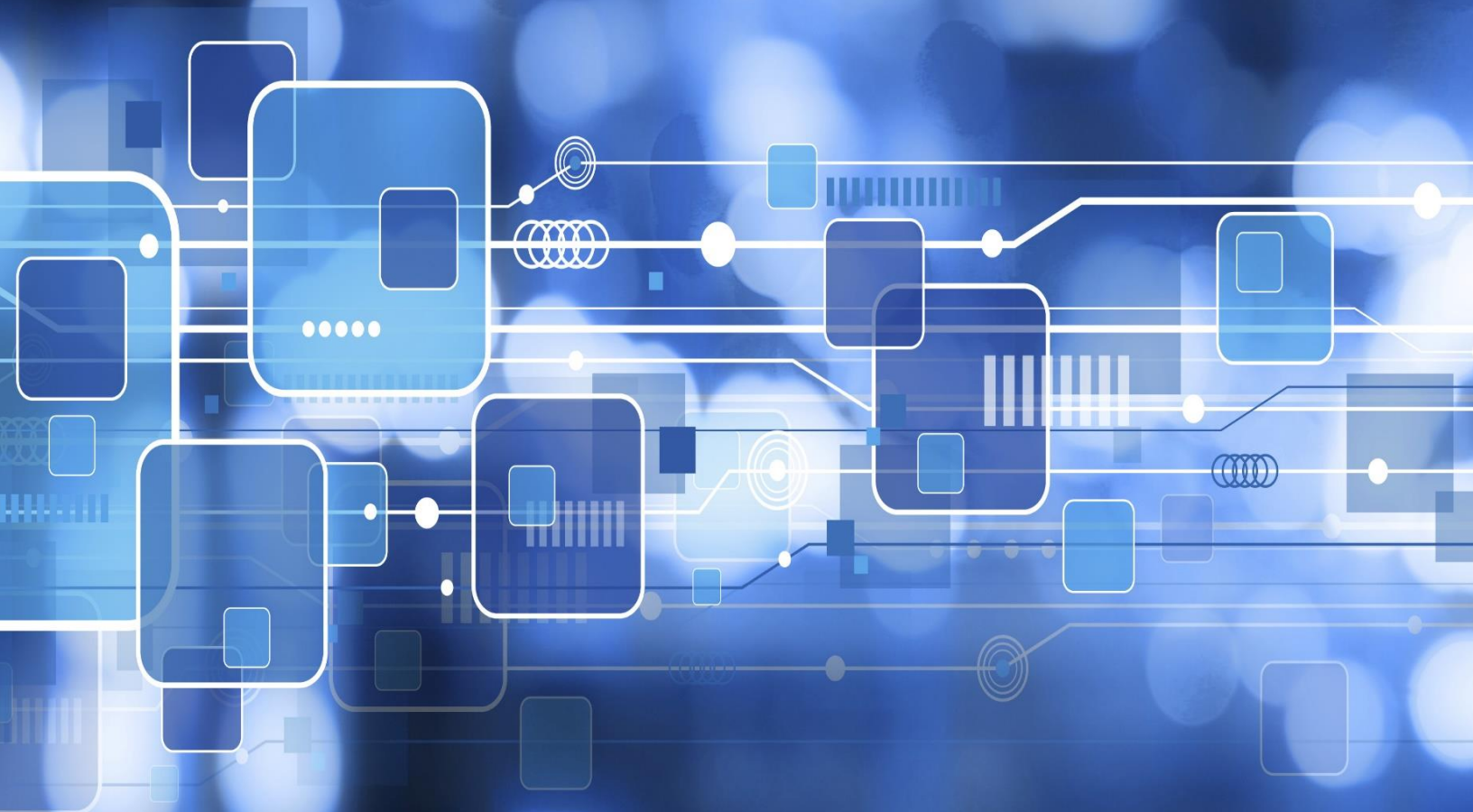
Source: Enterprise Strategy Group and ISSA, 2016

Table 4. Actions Government Should Take If It Were to Become More Involved with Cyber Security, by CISOs

| | Percentage of CISOs (N=61) | Percentage of total survey population (N=437) |
|---|-------------------------------|--|
| Enact legislation with high fines for data breaches | 31% | 24% |
| Amend existing laws to hold IT vendors liable for security problems associated with their products | 30% | 36% |
| Create better ways to share security information with the private sector | 64% | 54% |
| Provide funding for cyber security professional training and education | 54% | 43% |
| Limit federal government IT purchasing to vendors that demonstrate a superior level of security in their products and processes (i.e., ISO certification or a new cyber security certification) | 43% | 33% |
| Promote the use of certified products in the private sector | 38% | 24% |

Source: Enterprise Strategy Group and ISSA, 2016

Conclusion



The Bigger Truth

When it comes to the state of cyber security today, this ESG/ISSA research report presents some particularly troubling data. Cyber security professionals admit that:

- The organizations they work for continue to experience security incidents that disrupt business and IT operations.
- They believe that most organizations—including those providing critical infrastructure services—are vulnerable to cyber-attacks.
- The organizations they work for are impacted by the global cyber security skills shortage, leading to excessive workloads, inappropriate skill levels in some areas, and acute shortages in the areas of security analytics, application security, cloud security, and elsewhere. This is especially alarming since the first report revealed that cyber security professionals are not getting the proper level of training they need for mitigating risk, understanding the threat landscape, or responding to incidents as they occur.
- Cyber security professionals believe that current government cyber security strategies are lacking and that governments should provide more incentives, investment, programs, and overall help.

These ramifications have a profound impact on cyber security professionals and the organizations they work for.

Top Five Research Implications and Recommendations

The research presented in the two ESG/ISSA reports indicates that cyber security professionals face several daunting tasks. Their primary job is to protect their organizations' digital assets, but they are being asked to fulfill this mission while understaffed, lacking the right skills, and not always receiving the proper level of training.

Given these realities, cyber security professionals and the organizations they work for should:

- **Assume their organizations will experience one or several cyber-attacks or data breaches.** As the data indicates, 54% of organizations admit that they've experienced one or several cyber security incidents over the past year, while 92% agree that most organizations are vulnerable to some type of significant cyber-attack or data breach. It is also worth noting that the percentage of organizations experiencing security incidents may in fact be much higher, as at least 26% of the survey population answered "maybe," "don't know," or "prefer" not to say to each type of cyber security incident they were asked about. The ESG/ISSA data simply reinforces a common cyber security truism—organizations should expect to experience security compromises on an ongoing basis. This reality means that large and small organizations must have formal plans and processes in place for incident response. Furthermore, these plans should extend beyond the IT domain to include business executives, legal counsel, HR managers, etc. For those looking for a template in this area, the [NIST-800-61 Computer Incident Handling Guide](#) can help.
- **Take the cyber security skills shortage into account as part of every initiative and decision.** The two ESG/ISSA reports certainly reinforce previous data detailing the global cyber security skills shortage. In fact, 29% of cyber security professionals say that the cyber security skills shortage has had a significant impact on their organization, with ramifications for cyber security professionals' workload, training, and even their ability to use their security technologies correctly. The skills shortage also impacts day-to-day IT initiatives as survey respondents report a shortage of application security, cloud security, and mobile computing security specialists. While CISOs can't use the cyber security skills shortage as a way to stop business and IT progress, they should assume a cyber security personnel and skills deficit in each decision they make. For example, implementing advanced cyber security analytics tools may not be a good investment if the cyber security staff doesn't have ample time for product



training, software customization, or ongoing operations. Given the fact that the cyber security skills shortage won't abate anytime soon, CISOs should:

- Emphasize ease of use for all security technology purchases.
- Initiate and push projects for security automation and orchestration that use technology to alleviate tedious manual processes.
- Find use cases for managed security services.



- **Use the data from the two ESG/ISSA reports to educate business executives.** Although business managers are certainly more aware of cyber security issues than in the past, the ESG/ISSA research indicates that many organizations remain cyber security laggards. For example, when survey respondents were asked to identify the root causes of security incidents, 21% said that business and executive management tend to treat cyber security as a low priority. Many of the data points presented in the two ESG/ISSA reports could be used to help educate business managers on the extent of cyber security challenges. For example, CEOs should understand the implications of the cyber security skills shortage, the consistent lack of adequate cyber security training, and the need for more cyber security oversight from executives. The reports also present a fair number of suggested solutions. For example, 40% of cyber security professionals believe that adding cyber security goals as metrics to IT and business managers would provide cyber security benefits to organizations. If nothing else, these recommendations should help initiate a dialogue for business, IT, and security managers to brainstorm ways to improve cyber security that align with their mission and business requirements.



- **Push for more all-inclusive cyber security training.** Like the previous ESG/ISSA report, this publication consistently points to problems related to shortfalls in cyber security training:
 - Twenty-six percent of cyber security professionals say that a lack of adequate training for non-technical employees is one of the biggest contributors to security events at their organizations.
 - Thirty-two percent of cyber security professionals say that the cyber security skills shortage has led to limited time for training, since the cyber security team is too busy keeping up with day-to-day responsibilities.

Clearly, cyber security professionals recognize these training gaps and strongly recommend an increased focus in this area—39% say that providing more cyber security training to non-technical employees would be most beneficial, while 36% suggest increasing the amount of cyber security training for the cyber security staff. CISOs should take this data to heart and use it to lobby executives and HR staff to increase training budgets and commitments.



- **Actively lobby government legislators.** When it comes to government cyber security actions, cyber security professionals are not impressed in the least. Almost all (97%) of cyber security professionals believe that their nation's critical infrastructure is extremely vulnerable or vulnerable to some type of significant cyber-attack. Sixty-three percent believe that their government's cyber security strategy is unclear and incomplete. And 89% believe that their government should be more involved in cyber security strategies and defenses than they are today. Although cyber security professionals' opinions should be extremely visible in national cyber security policy discussions, they are often muted by lobbyists and others with self-serving agendas. Altering this situation will require more organization and a louder voice from the profession itself. Therefore, cyber security professionals should organize, engage legislators to participate in industry events and user conferences, and push large cyber security vendors to exert more government influence.

Research Methodology

To gather data for this report, ESG conducted an online survey of security and IT professionals from the [ISSA](#) member list (and beyond) in North America, Europe, Central/South America, Africa, Asia, and Australia between May 19, 2016 and June 12, 2016.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 437 security and IT professionals.

Please see the *Respondent Demographics* section of this report for more information on these respondents.

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

Respondent Demographics

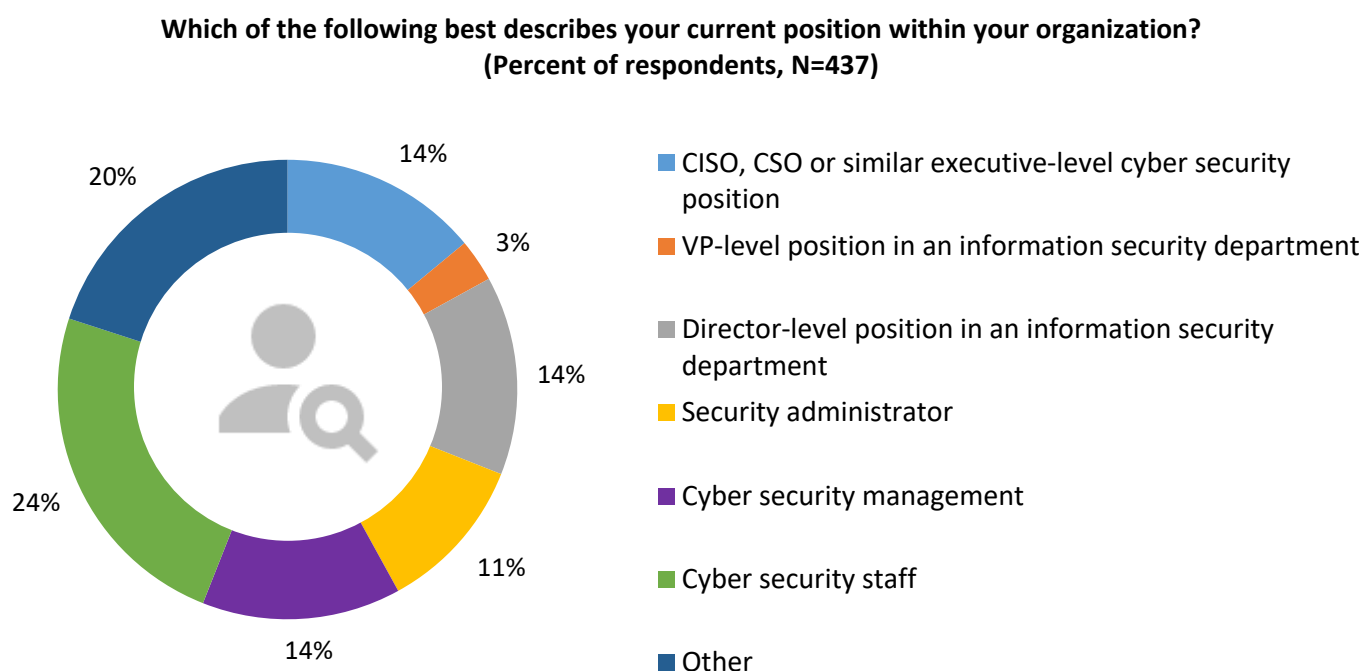


The data presented in this report is based on a survey of 437 qualified respondents and cyber security professionals. Figures 14-19 detail the demographics of the respondent base, including individual respondents' current role, responsibilities, and geographic location, as well as respondent organizations' total number of employees, primary industry, and annual revenue.

Respondents by Current Position

Respondents' current role is shown in Figure 14.

Figure 14. Respondents by Current Position



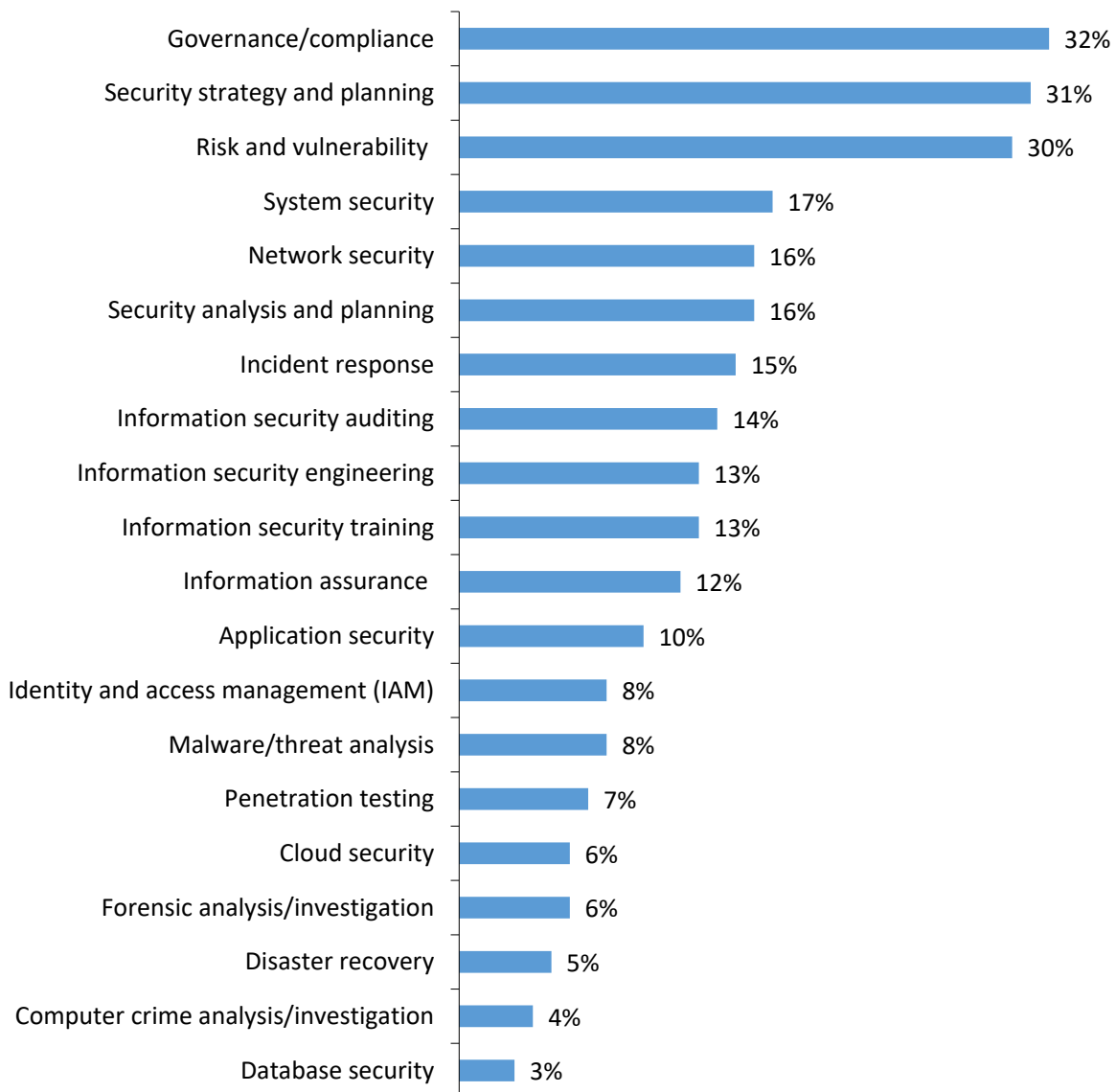
Source: Enterprise Strategy Group and ISSA, 2016

Respondents by Current Primary Responsibilities

Respondents' current primary responsibilities is shown in Figure 15.

Figure 15. Respondents by Current Primary Responsibilities

Which of the following best (i.e., most closely) describes your primary responsibilities within your organization? (Percent of respondents, N=437, three responses accepted)

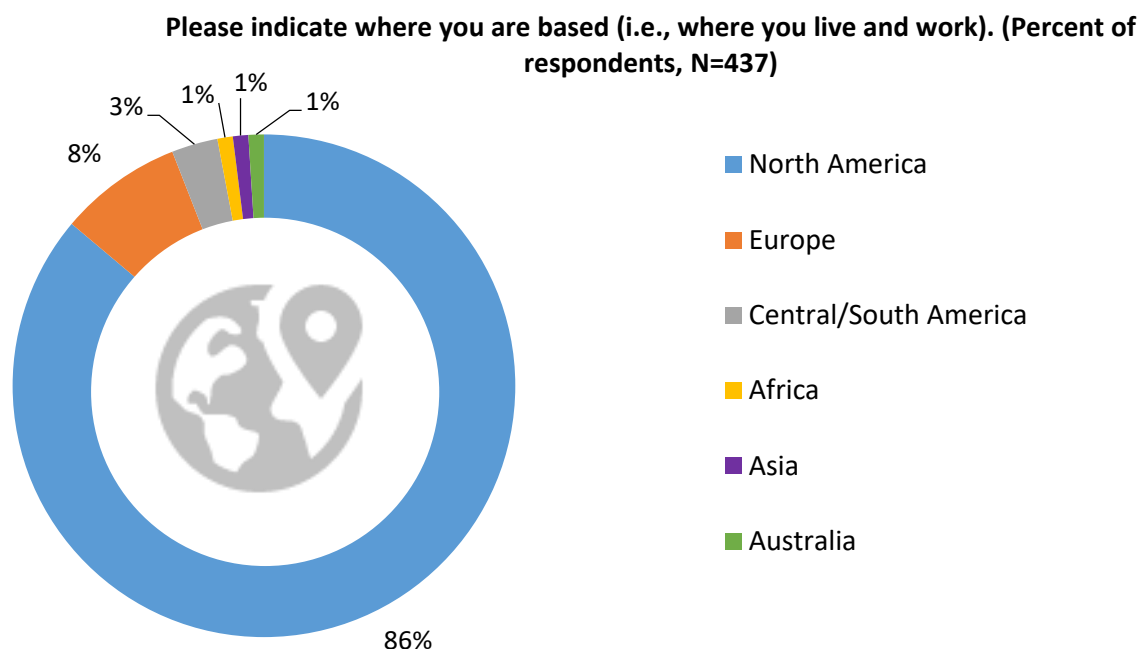


Source: Enterprise Strategy Group and ISSA, 2016

Respondents by Region

The regional breakdown of respondents is shown in Figure 16.

Figure 16. Respondents by Region

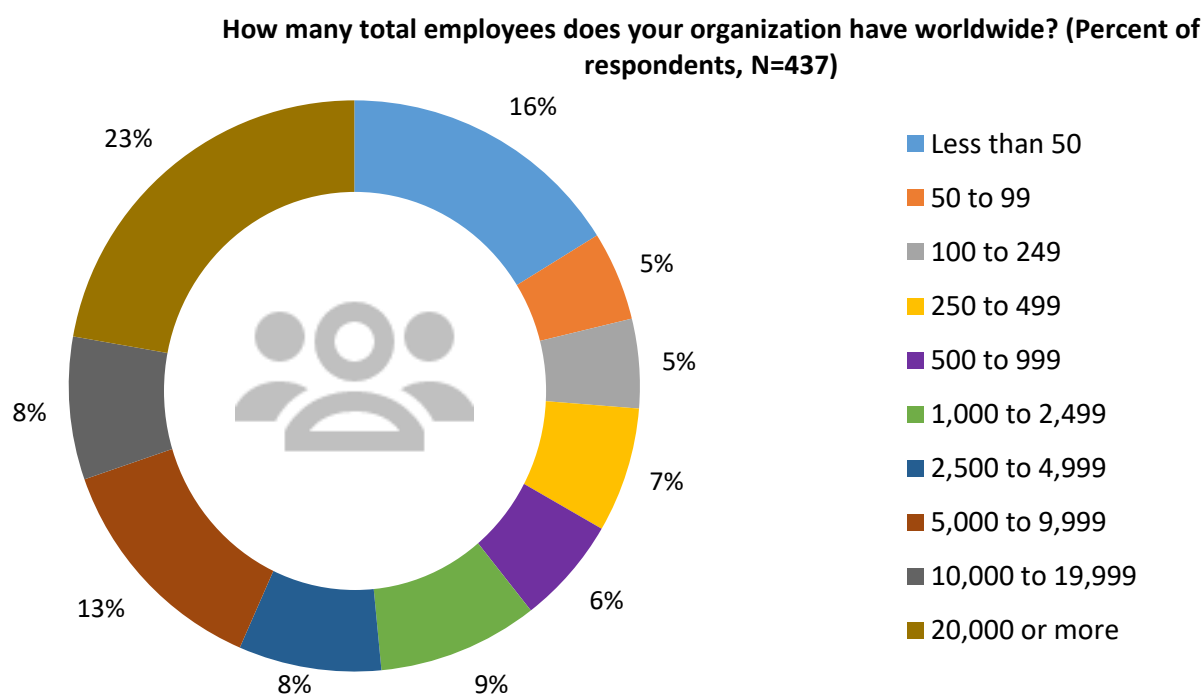


Source: Enterprise Strategy Group and ISSA, 2016

Respondents by Number of Employees

The number of employees in respondents' organizations is shown in Figure 17.

Figure 17. Respondents by Total Number of Employees Worldwide

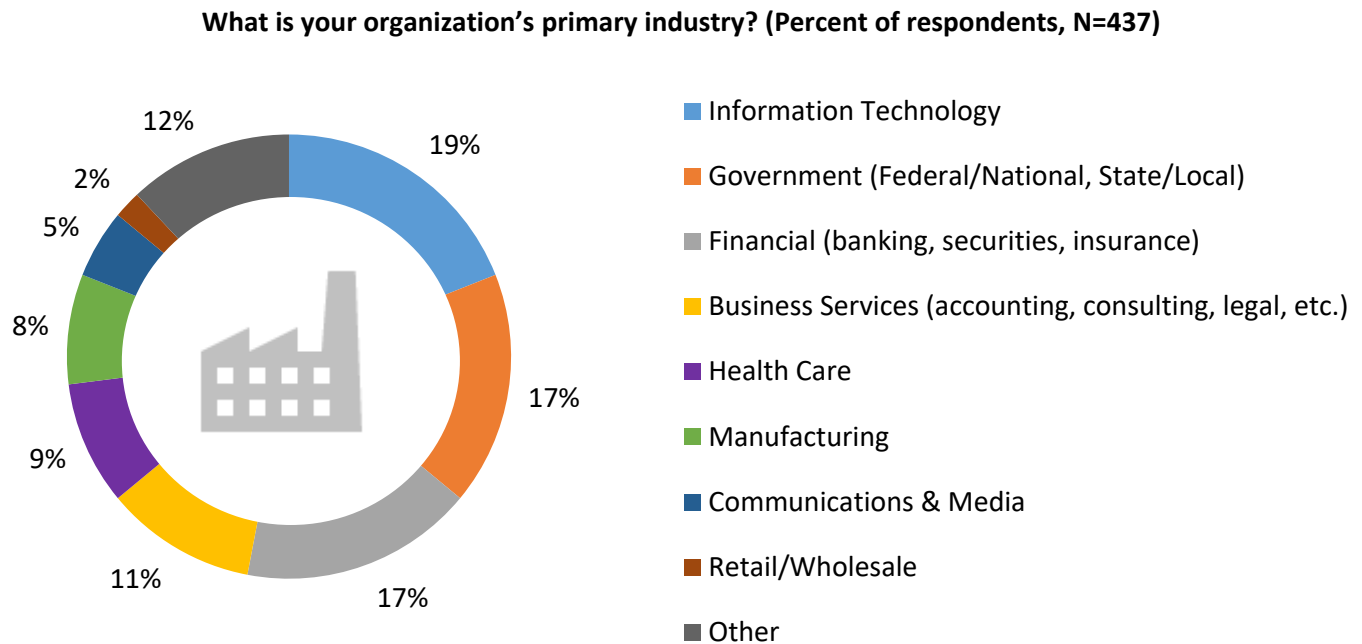


Source: Enterprise Strategy Group and ISSA, 2016

Respondents by Industry

Respondents were asked to identify their organization's primary industry. In total, ESG received completed, qualified respondents from individuals in 19 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 18.

Figure 18. Respondents by Industry

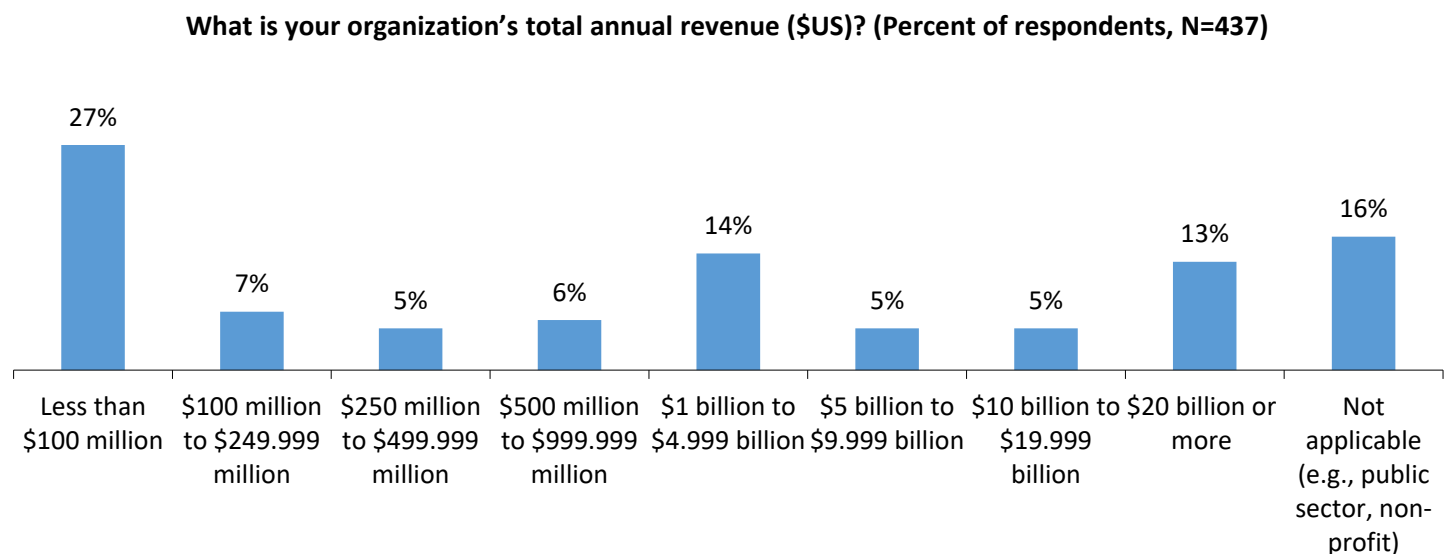


Source: Enterprise Strategy Group and ISSA, 2016

Respondents by Annual Revenue

Respondent organizations' annual revenue is shown in Figure 19.

Figure 19. Respondents by Annual Revenue



Source: Enterprise Strategy Group and ISSA, 2016

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

The Information Systems Security Association (ISSA) is the community of choice for international cyber security professionals dedicated to advancing individual growth, managing technology risk, and protecting critical information and infrastructure. ISSA members and award winners include many of the industry's notable luminaries and represents a broad range of industries - from communications, education, healthcare, manufacturing, financial and consulting to IT - as well as federal, state and local government departments and agencies. Through regional chapter meetings, conferences, networking events and content, members tap into a wealth of shared knowledge and expertise. Visit ISSA on the web at www.issa.org and follow us on Twitter at @ISSAINTL.

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

