RESEARCH REPORT

The Life and Times of Cybersecurity Professionals 2018

By Jon Oltsik, ESG Senior Principal Analyst and Fellow

April 2019

A Cooperative Research Project by ESG and ISSA

Enterprise Strategy Group

Information Systems Security Association International

Contents

List of Figures

List of Tables

Executive Summary

Report Conclusions

In late 2018 and early 2019, the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA) conducted its third annual research product focused on the lives and experiences of cybersecurity professionals. This year's report is based on data from a survey of 267 cybersecurity professionals and ISSA members. Ninety percent of survey respondents resided in North America, 5% came from Europe, 3% from Central/South America, 2% from Asia, and 1% from Africa (note: Total exceeds 100% due to rounding).

Based upon the data gathered as part of this project, the report concludes:

- **Cybersecurity teams are participating in data privacy efforts but may not be up to the task.** Eighty-four percent of ISSA members claim that the cybersecurity team at their organization has taken a more active role with data privacy over the past 12 months. This effort seems somewhat haphazard and immature, however, as 21% of respondents don't believe the cybersecurity team has been given the clear directions for its data privacy responsibilities, and 23% don't believe the cybersecurity team has been given the right level of training for its data privacy responsibilities.

- **Cybersecurity professionals are dedicated to their craft but need some career guidance.** Forty-two percent of survey respondents have worked in cybersecurity for at least 10 years, and 32% of respondents have worked at 2 or 3 jobs during this timeframe. Most (79%) started as IT professionals before switching their career to cybersecurity and were attracted to the technical challenges and moral implications associated with security. Unfortunately, many cybersecurity professionals aren't managing their careers proactively as only 31% believe they have a well-defined career path. Most believe that their career would benefit from a combination of a mentorship program, career mapping, and a technical training career plan.

- **Knowledge, skills, and abilities (KSA) development depends upon face-to-face interaction.** When asked to identify the most effective methods for KSA development, ISSA members pointed to attending specific cybersecurity training courses (71%), participating in professional organizations and events (68%), attending trade shows (51%), and participating in on-the-job mentoring programs (42%). For the third year in a row, industry certifications were most important for getting a cybersecurity job but not nearly as critical for KSA advancement as part of career development.

- **Job satisfaction depends upon an organizational commitment to cybersecurity.** While 39% of survey respondents claim to be very satisfied with their current job, a larger percentage (47%) were only somewhat satisfied. The research also reveals that the most important factors for cybersecurity job satisfaction include working for organizations that provide support and incentives for career advancement (40%), competitive or industry-leading compensation (38%), business management's commitment to strong cybersecurity (34%), and the ability to work with highly skilled individuals (34%). In a new question for 2018, survey respondents were also asked to identify the most stressful aspects of a cybersecurity job. The top choices included: Keeping up with the security needs of new IT initiatives (40%), finding out about IT initiatives/projects that were started by other teams within their organizations without proper security oversight (39%), trying to get end-users to better understand cyber-risks and change their behavior (38%), and trying to get the business to better understand cyber-risks (37%).

- **Training and skills development remain a problem.** For the third straight year, a majority (63%) of ISSA members don't think that their employer provides the cybersecurity team with the right level of training. The research also indicates that, while 93% of survey respondents agree that cybersecurity professionals must keep up with their skills or else the organizations they work for will be at a significant disadvantage against cyber-attackers, 66% claim that cybersecurity

job demands often preclude them from skills development. The critical and persistent imbalance with training needs and training performance must be addressed for organizations to have any hope of mitigating cyber-risks and defending themselves against advanced cyber-adversaries like nation states.

- **CISOs need to be more active with business executives.** Fifty-nine percent of organizations employ a CISO while 10% employ a virtual CISO. According to survey respondents, CISO success depends upon characteristics like communications skills (44%), leadership skills (42%), a strong relationship with business executives (35%), and a strong relationship with the CIO and IT leadership team (31%). Unfortunately, the research indicates that there is still some friction between CISOs and business executives as 28% of respondents don't believe their CISO is getting an adequate level of participation with executive management and boards of directors. This relationship is a "work-in-progress" at many firms, but for the third year in a row, progress here seems marginal at best.

- **The virtual CISO position (vCISO) is an attractive career option.** As previously stated, 10% of organizations surveyed now employ a virtual CISO. Furthermore, 29% of CISOs surveyed are working as a vCISO while another 21% are considering doing so. When asked why, 43% claim that working as a vCISO brings more variety and flexibility to a CISO position. These are positive benefits, but vCISOs may also seek to avoid some of the politics and stress associated with a CISO title while taking more control of their careers.

- **Lacking employee security awareness training and a growing workload lead to security incidents.** Nearly half (48%) of organizations admit to at least one security incident over the past two years. The percentage is likely much higher still as 40% of respondents either didn't know if their organizations suffered a security incident or preferred not to say. When asked to identify the root causes of these security incidents, 34% pointed to a lack of end-user training while 24% admitted that the cybersecurity team can't keep up with a growing workload. The lack of adequate security awareness training is especially troublesome since 46% of organizations say they've increased the amount of training for non-technical employees over the past 2 years. Based upon this research, it appears that end-user training may be done to meet regulatory compliance requirements, but it remains ineffective for changing end-user cybersecurity behavior.

- **ISSA members are pessimistic about cybersecurity in general.** Cybersecurity professionals are paid to question the status quo and remain paranoid. With that said, ISSA members appear to be downright skeptical about their chances for success. Most survey respondents believe that most organizations are either extremely vulnerable (39%) or somewhat vulnerable (52%) to a significant cyber-attack or data breach. When asked about the balance of power between cyber-adversaries and cyber-defenders, 59% believe that cyber-adversaries have a big advantage over cyber-defenders while 34% say that cyber-adversaries have a marginal advantage over cyber-defenders. ISSA members were also asked to identify the top cybersecurity challenges at their organizations. This list included an understaffed cybersecurity team (29%), a lack of cybersecurity knowledge from business executives (23%), a dependence on too many manual and/or informal processes (23%) and managing the complexity of too many disconnected security point tools (23%).

- **The cybersecurity skills shortage is not improving.** One-third of survey respondents believe that the global cybersecurity skills shortage has had a significant impact on their organization, while 41% say that the skills shortage has impacted their organizations somewhat. What type of impact? Two-thirds of those whose organization has been impacted say that the skills shortage has increased the workload on existing staff, 47% report an inability to fully learn or utilize some of their security technologies to their full potential, 41% say that their organization has had to recruit and train junior personnel rather than hire more experienced infosec pros, and 40% claim that the cybersecurity staff has limited time to work with business managers. The most acute skills shortages include cloud computing security (33%), application security (32%), and security analysis and investigations (30%). Looking back to years past, the

three-year research trend clearly indicates that organizations are not improving their ability to deal with the cybersecurity skills shortage. This increases cyber-risk for organizations, shareholders, customers, business partners, etc.

- **It's a "seller's market" for cybersecurity talent.** Given the skills shortage data above, it is no surprise that 44% of survey respondents are solicited to change jobs by recruiters at least once a week. What's more, 76% of survey respondents are solicited to change jobs by recruiters at least once a month. This trend creates a "seller's market" for cybersecurity talent along with salary inflation, high attrition, and cutthroat competition for skilled applicants. Once again, there is no relief in sight here.

- **Infosec changes are in play.** When asked to identify cybersecurity actions their organizations could take that would be most beneficial, 42% suggested adding cybersecurity goals and metrics to IT and business managers, 42% recommended increasing training for the cybersecurity team, 41% proposed increasing the cybersecurity budget, and 40% endorsed increasing training for non-technical employees. It appears that a lot of work remains ahead for cybersecurity improvement.

Based upon the results of this year's and past research projects, it is safe to conclude that cybersecurity progress has been marginal at best over the last three years. ESG and ISSA agree with security researcher and author Bruce Schneier's quote: "We may be making some cybersecurity improvements but we are getting worse faster." This overall lack of cybersecurity progress should be of concern to everyone.

Introduction

Research Objectives

In order to assess the experiences, careers, and opinions of cybersecurity professionals, ESG/ISSA surveyed 343 cybersecurity professionals representing organizations of all sizes, across all industries and geographic locations. Survey respondents were also ISSA members.

The survey and overall research project were designed to answer the following questions about:

- Cybersecurity careers
  1. How long had survey respondents worked as cybersecurity professionals?
  2. Why did they become cybersecurity professionals?
  3. How were they developing and advancing their careers?
  4. Were they happy at their jobs and with their career choices?
  5. What is necessary for cybersecurity job satisfaction? Alternatively, what alienates cybersecurity professionals and causes them to look for another job?
  6. Are cybersecurity professionals being actively recruited to change jobs?
  7. Are cybersecurity professionals experiencing burnout?
- Skills development
  1. How important is continuing skills development in the minds of cybersecurity professionals?
  2. How do cybersecurity professionals develop their skills? What works and what doesn't work?
  3. Do the responsibilities and workload associated with cybersecurity jobs get in the way of skills development?
  4. Do the organizations cybersecurity professionals work at provide adequate training, skills development programs, or services for career advancement?
- Cybersecurity organizational considerations
  1. Do organizations have CISOs or similar positions in place?
  2. What makes CISOs successful?
  3. Why do CISOs change jobs so often?
- Security incidents and vulnerabilities
  1. Have organizations suffered security incidents? If so, which types of security incidents?

2. What factors contributed to these incidents?
3. Do cybersecurity professionals believe that organizations are vulnerable to cyber-attacks?
4. Do cybersecurity professionals believe that their employers are vulnerable to cyber-attacks?

- The cybersecurity skills shortage

1. Do cybersecurity professionals believe that their organization has been impacted by the global cybersecurity skills shortage?
2. If so, in what way?
3. In which areas do their organizations have the biggest cybersecurity skills deficits?

- Cybersecurity activities

1. What types of cybersecurity actions have their organizations taken over the past few years?
2. What additional actions should their organizations take to help improve cybersecurity overall?

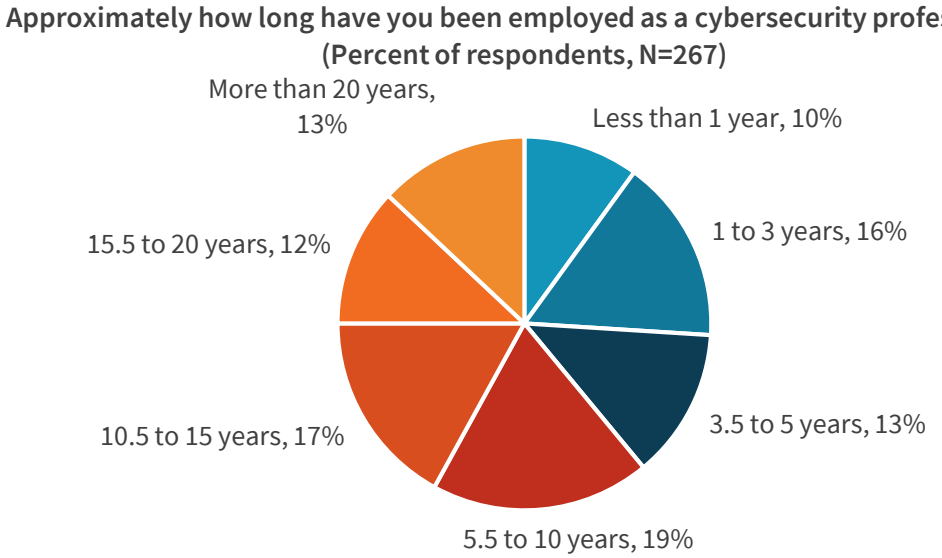
Survey participants represented a wide range of industries including health care, IT, financial services, manufacturing, business services, communications and media, and government. For more details, please see the *Research Methodology* and *Respondent Demographics* sections of this report.

Research Findings

The ISSA Survey Respondent

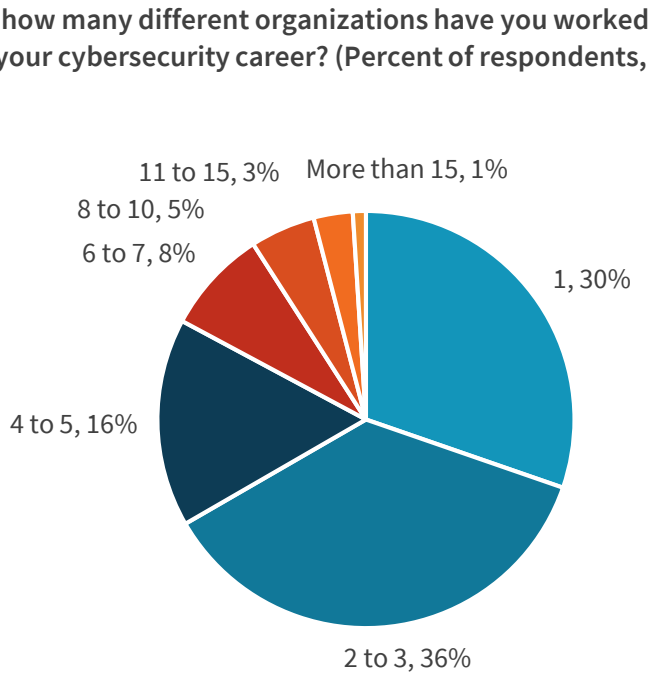
The ESG/ISSA research study is based upon a survey of a diverse group of cybersecurity professionals ranging from entry-level to senior positions. Twenty-six percent of respondents have three or less years of experience while 25% have more than 15 years of experience (see Figure 1). Most of the cybersecurity professionals (66%) have had three or fewer cybersecurity jobs through their careers (see Figure 2).

Figure 1. Length of Time Employed as a Cybersecurity Professional



Source: Enterprise Strategy Group

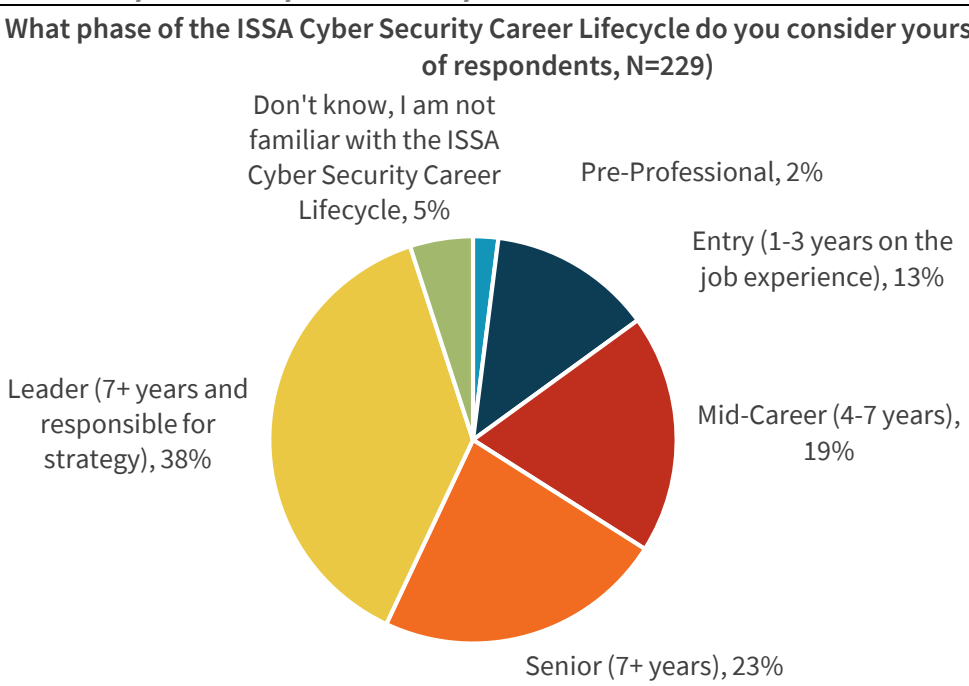
Figure 2. Number of Cybersecurity Jobs



Source: Enterprise Strategy Group

ESG/ISSA also wanted to align respondents' experience with the phases of the ISSA cybersecurity career lifecycle. Twenty-three percent of respondents consider themselves "senior," while 38% rank themselves as "leaders" (see Figure 3).

Figure 3. Phase of ISSA Cybersecurity Career Lifecycle

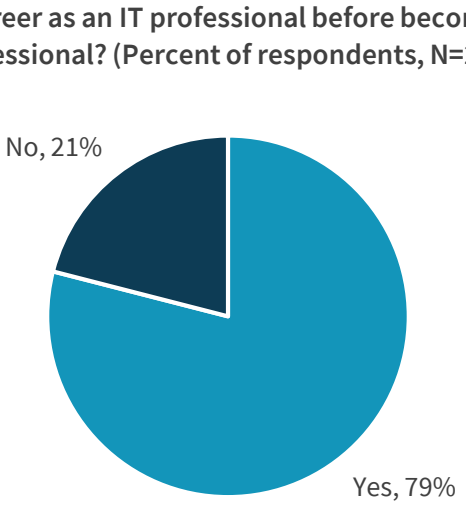


Source: Enterprise Strategy Group

The Cybersecurity Professional

Seventy-nine percent of survey respondents started their careers in IT and then migrated toward a cybersecurity focus over time (see Figure 4). Given the global cybersecurity skills shortage, CISOs should actively recruit new cybersecurity hires from IT departments within and outside of their organizations. These results are similar to the last two year's project (i.e., 2017: 77% came to cybersecurity from IT, 2016: 78% came to cybersecurity from IT).

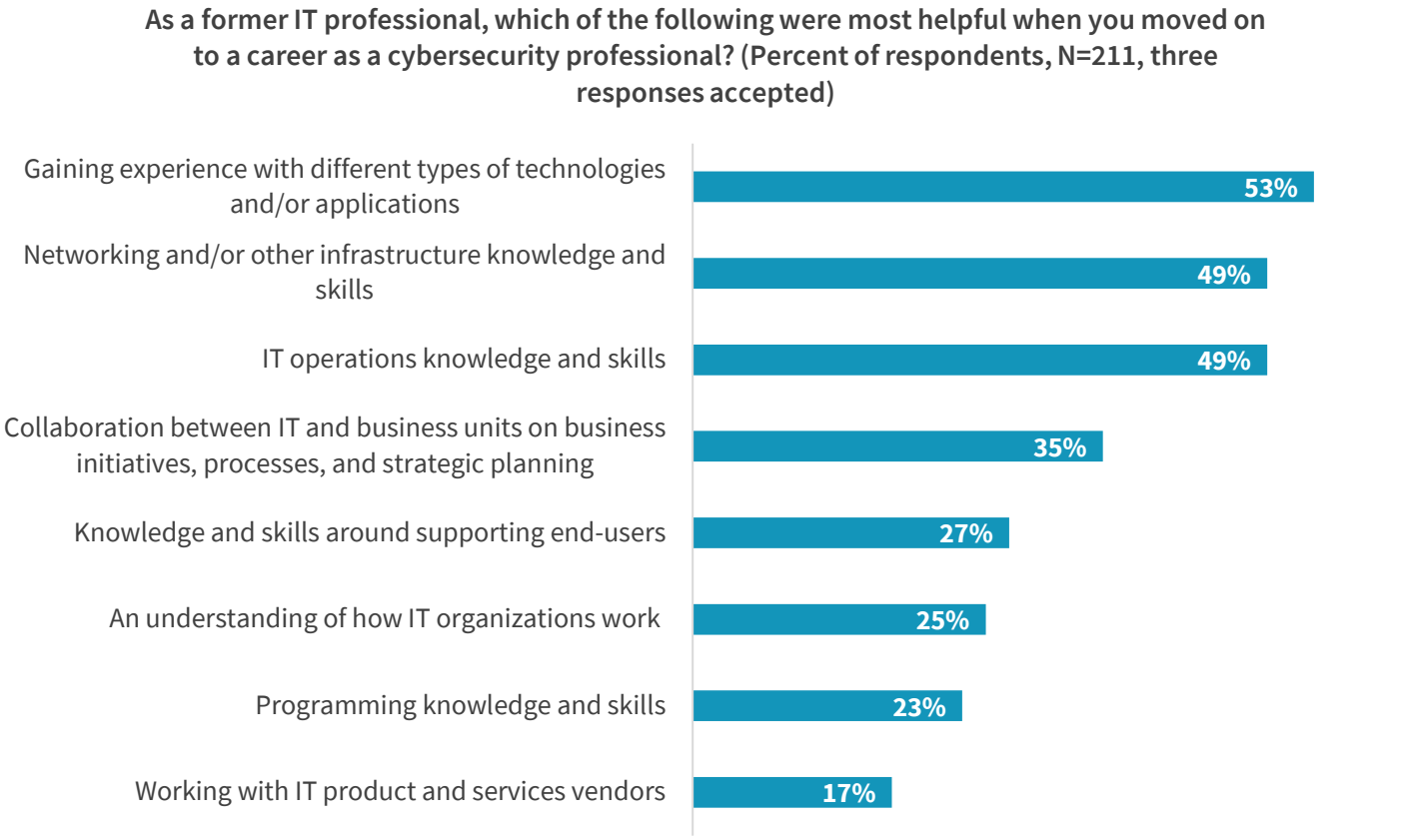
Figure 4. Cybersecurity Professionals Tend to Come from IT



Source: Enterprise Strategy Group

IT professionals bring lots of experience to cybersecurity when they make this transition. Survey respondents point to the most helpful of these skills when moving into cybersecurity: 53% say gaining experience with different types of technologies and applications, 49% point to networking technology and other types of infrastructure, and 49% identify IT operations skills (see Figure 5). Responses from each of the three years are consistent (see Table 1).

Figure 5. IT Skills Most Helpful for a Cybersecurity Career



Source: Enterprise Strategy Group

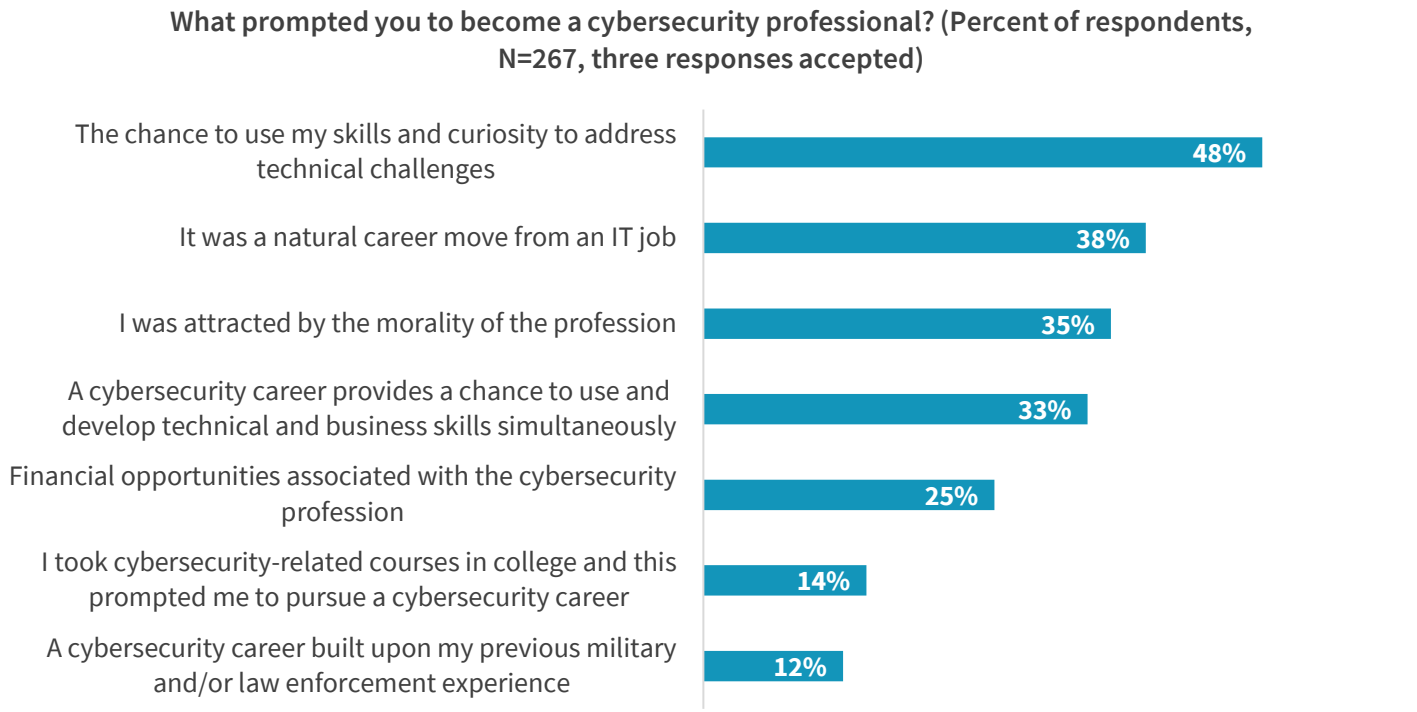
Table 1. Factors Most Helpful in Moving to a Cybersecurity Career, by Year

Top Four Factors Cited in 2016	Top Four Factors Cited in 2017	Top Four Factors Cited in 2018
Gaining experience with different types of technologies and/or applications	Networking and/or other infrastructure knowledge and skills	Gaining experience with different types of technologies and/or applications
IT operations knowledge and skills	IT operations knowledge and skills	Networking and/or other infrastructure knowledge and skills
Networking knowledge and skills	Gaining experience with different types of technologies and/or applications	IT operations knowledge and skills
Collaboration between IT and business units	Collaboration between IT and business units	Collaboration between IT and business units

Why do individuals choose to become cybersecurity professionals? Just under half (48%) claim that a cybersecurity career presents them with the chance to use their skills and curiosity to address technical challenges, 38% say that a cybersecurity career was a natural career move from an IT job, and 35% indicate that they were attracted by the morality of the (cybersecurity) profession (see Figure 6). Similar to past years, financial opportunities associated with cybersecurity careers

is far down the list. Cybersecurity professionals haven't changed much in the past three years—the top choices were consistent in 2016, 2017, and 2018.

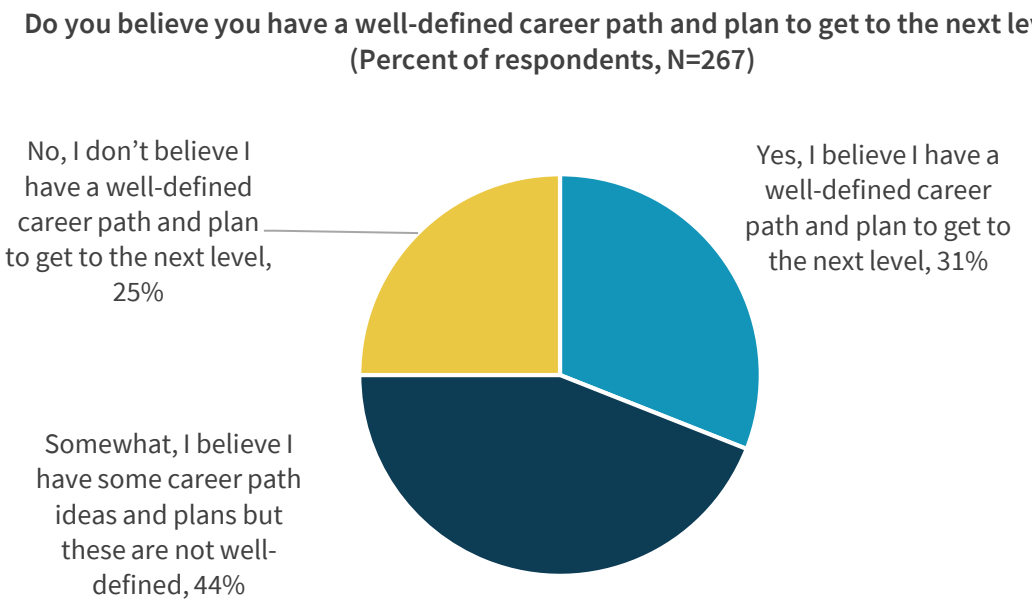
Figure 6. Reasons for Becoming a Cybersecurity Professional



Source: Enterprise Strategy Group

When it comes to career planning, cybersecurity professionals don't seem to be very proactive. Less than one-third (31%) have a well-defined career path, but more than two-thirds only have some career path ideas or don't believe they have a well-defined career path at all (see Figure 7). Based upon this data, CISOs should engage with the cybersecurity staff to help them explore ways to enhance their skills and build their career paths within the organization.

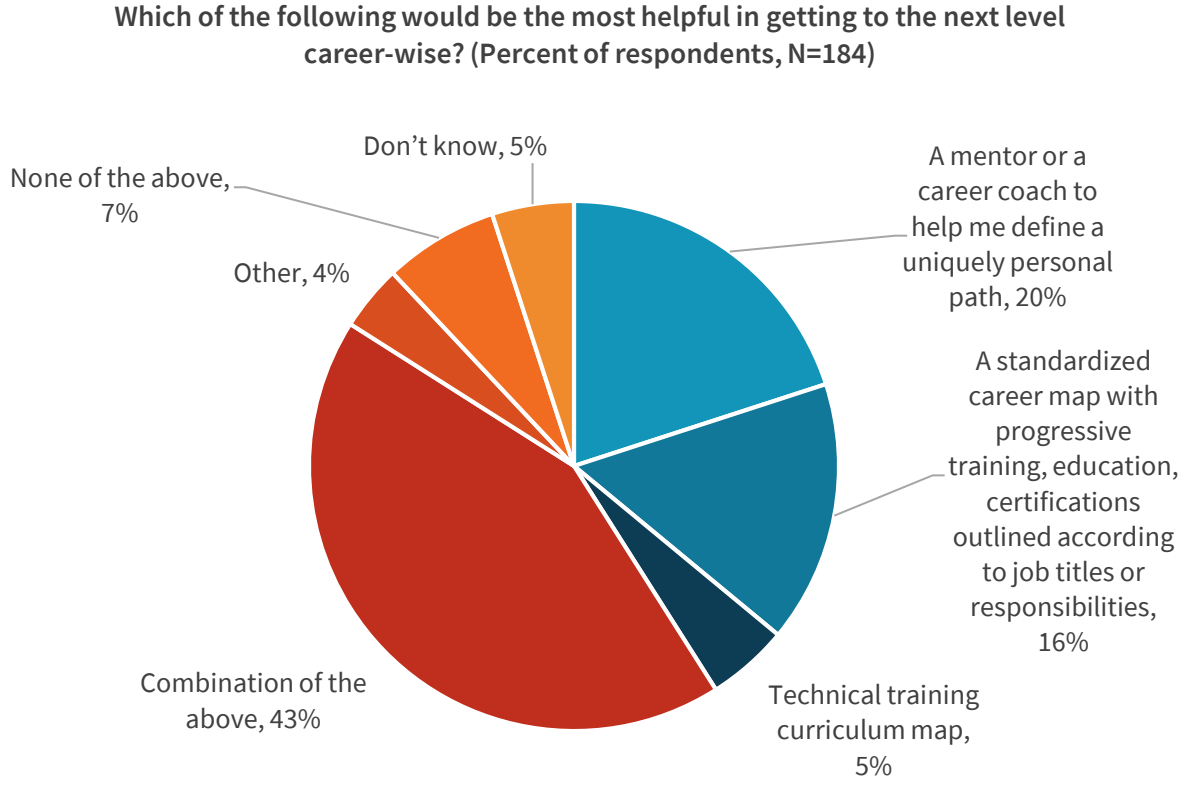
Figure 7. Do Respondents Believe They Have a Well-defined Career Path?



Source: Enterprise Strategy Group

Career progression for 43% of those surveyed would include a combination of mentoring, a standardized career map, and additional technical training (see Figure 8). Note that the results were consistent in all three years.

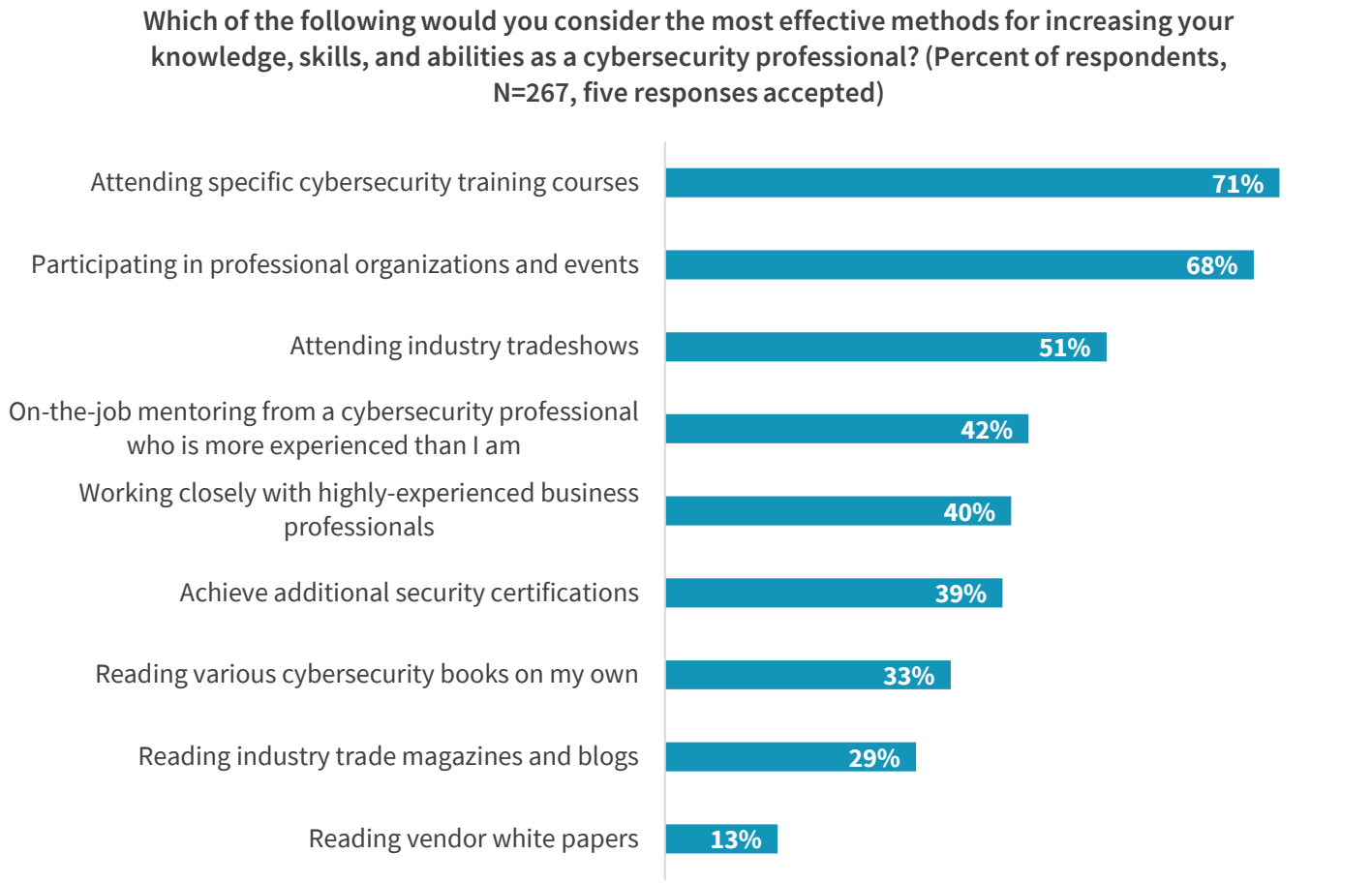
Figure 8. Most Helpful Factors in Progressing a Cybersecurity Career



Source: Enterprise Strategy Group

Similar to past years, respondents were asked their opinions on the most effective methods for increasing their cybersecurity knowledge, skills, and abilities (KSAs). Top activities for increasing KSAs included attending specific cybersecurity training courses (71%), participating in professional organizations (68%), and attending industry tradeshows like the RSA Security Conference or Black Hat (see Figure 9.). The top two responses have been consistent for all three years.

Figure 9. Most Effective Methods for Increasing KSAs



Source: Enterprise Strategy Group

Cybersecurity Certifications

Which certifications have ISSA members achieved? Just like 2017, survey respondents were asked to write-in the answer to this question and the top responses are listed in the figure below (see Figure 10).

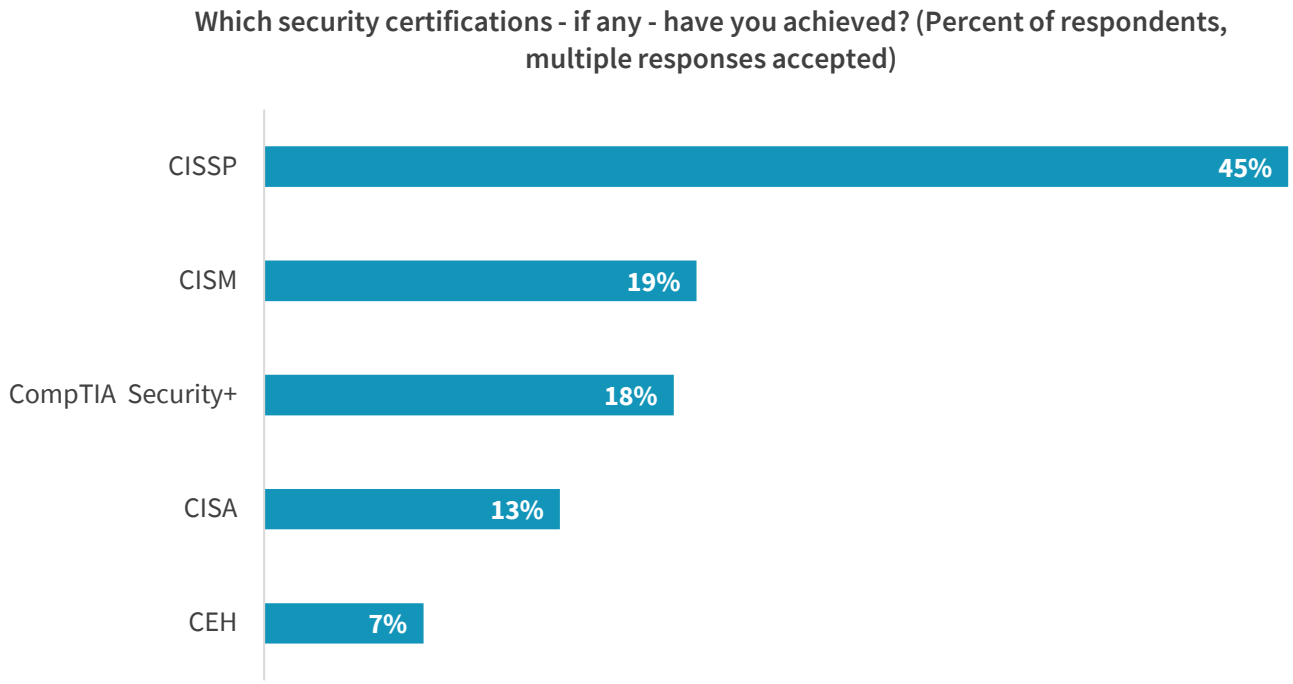
Of those certifications achieved, the most useful ones for getting a job are graphed in the figure below and compared to the results from the past two years (see Figure 11).

Three years of data demonstrates a consistent conclusion. Cybersecurity professionals often pursue a CISSP certification early in their careers as it is often a job requirement. After a CISSP, however, other certifications have more finite value. For example, a penetration tester may want to pursue a certified ethical hacker (CEH) certification but the value of this certification is somewhat marginal for other cybersecurity positions.

Given the number of certifications, there is now an entire industry composed of certification and training companies. Market noise may tempt cybersecurity professionals to fill their resumes with acronyms as they achieve numerous security

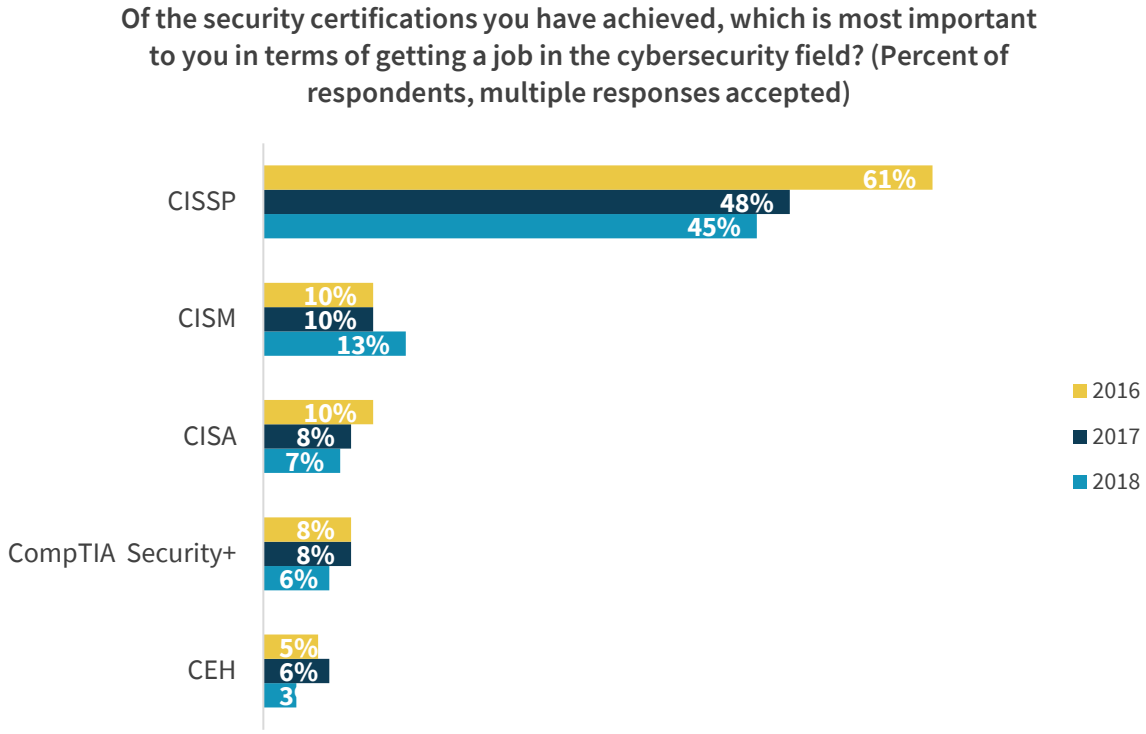
certifications. The ESG/ISSA data suggests that this may be a fool's errand, however. As in past years, cybersecurity professionals are best served by gaining CISSPs and then using other KSA outlets to advance their skill sets and careers.

Figure 10. Cybersecurity Certifications Achieved



Source: Enterprise Strategy Group

Figure 11. Most Important Certification Necessary to Get a Job

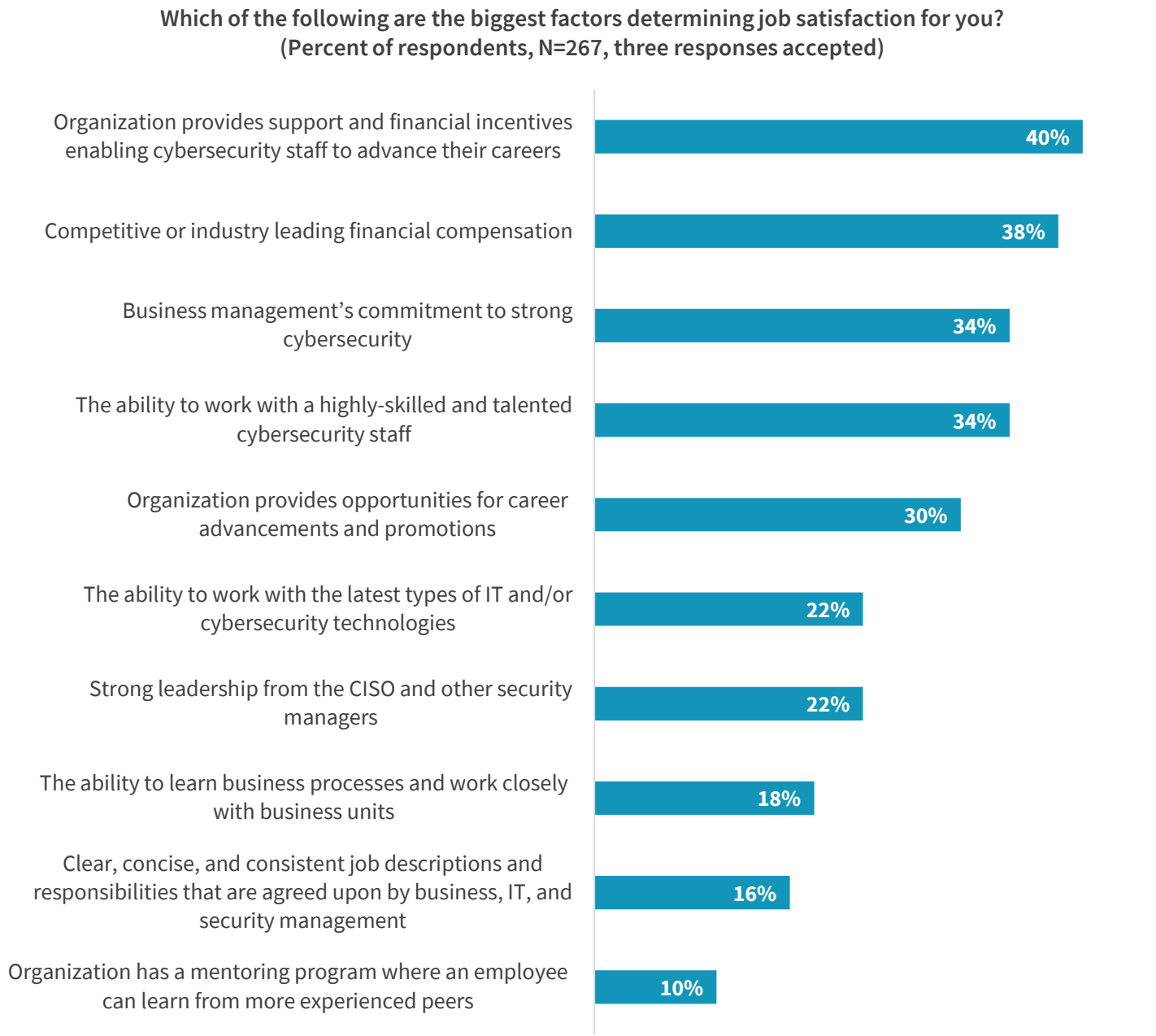


Source: Enterprise Strategy Group

Cybersecurity Jobs

Individuals become cybersecurity professionals for many reasons. Once they enter the profession, what do they look for when they join the cybersecurity ranks? According to this year's ESG/ISSA research, the top three priorities include working for an organization that provides support and financial incentives for career advancement, competitive/industry leading compensation, and business managers' commitment to strong cybersecurity (see Figure 12). Once again, these results have been consistent for three years.

Figure 12. Factors Determining Job Satisfaction



Source: Enterprise Strategy Group

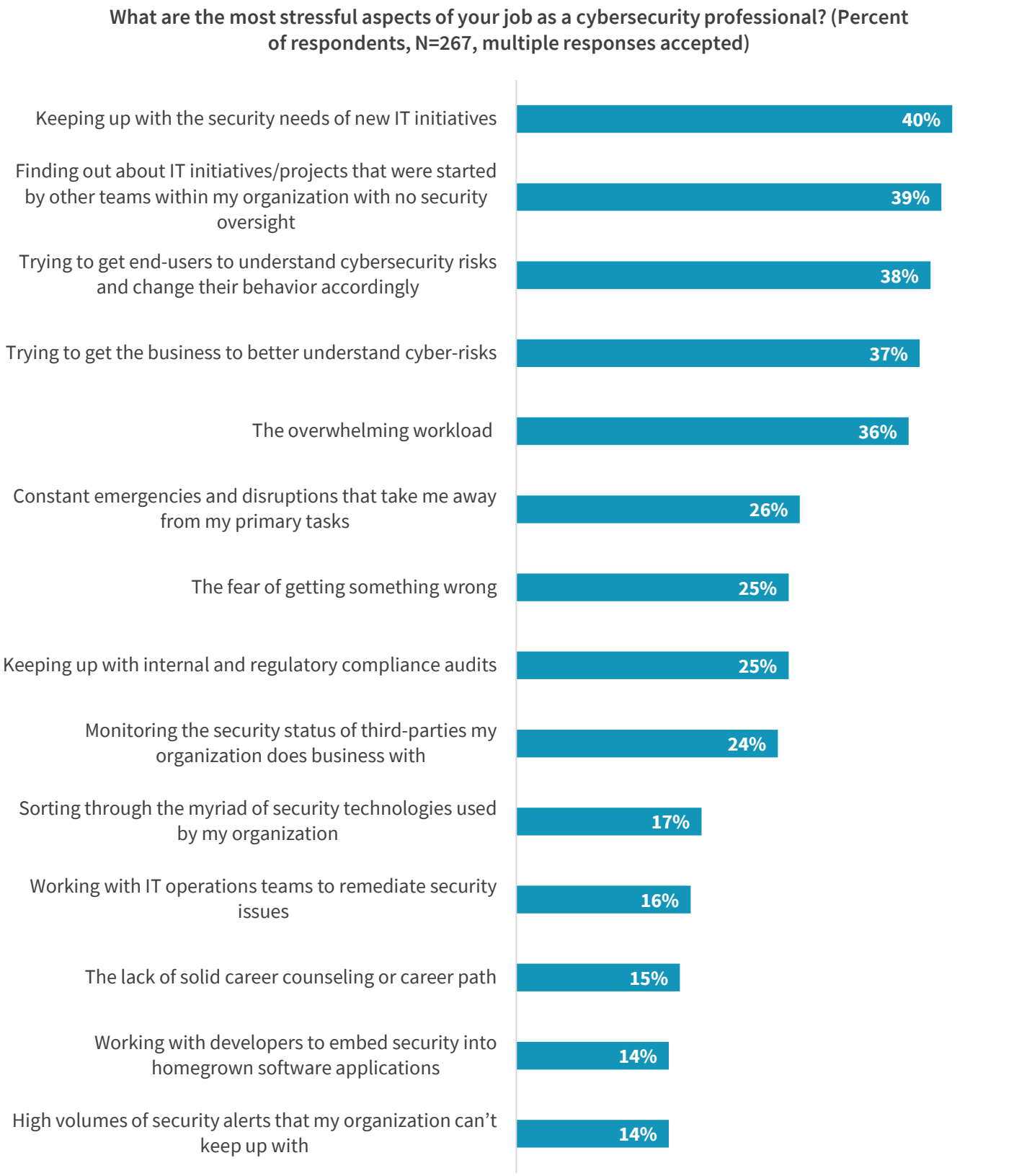
In a new question for 2018, survey respondents were asked to identify the most stressful aspects of a cybersecurity job (see Figure 13). The top results are as follows:

- 40% say that the most stressful aspect of a cybersecurity job is keeping up with the security needs of new IT initiatives. This may involve working more closely with business management, getting involved in project planning, working with third parties, or learning new technology skills (i.e., cloud computing, IoT, etc.).

- 39% say that the most stressful aspect of a cybersecurity job is finding out about IT initiatives/projects that were started by other teams with no security oversight. In these instances, cybersecurity teams are forced to catch up and add security controls as they can.

- 38% say that the most stressful aspect of a cybersecurity job is trying to get end-users to understand cybersecurity risks and change their behavior. As the saying goes, "people are the weak link in the cybersecurity chain," and in many cases, employees are not receiving the right level of security awareness training. This can lead to poor cybersecurity habits where end-users download malicious files, click on suspicious links, and fall for cyber-adversaries' social engineering tactics.

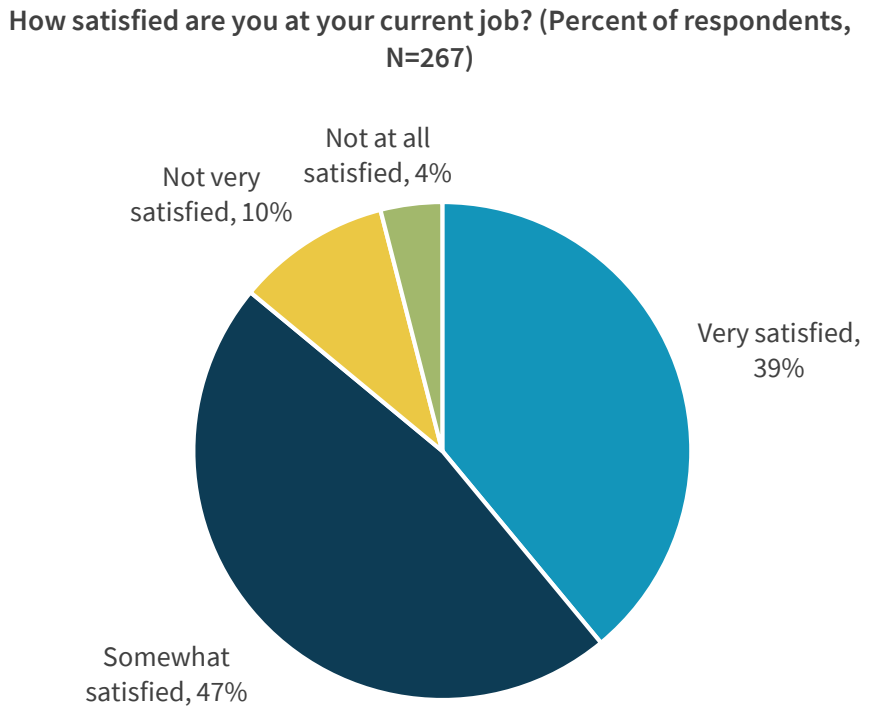
Figure 13. Most Stressful Aspects of Cybersecurity Jobs



Source: Enterprise Strategy Group

Clearly, a cybersecurity career comes with lots of challenges that can equate to issues with job satisfaction. The ESG/ISSA research highlights this tension as nearly half (47%) of survey respondents are only somewhat satisfied with their current job, compared to 39% who are very satisfied (see Figure 14). These results have been consistent for three years.

Figure 14. Level of Satisfaction with Current Job

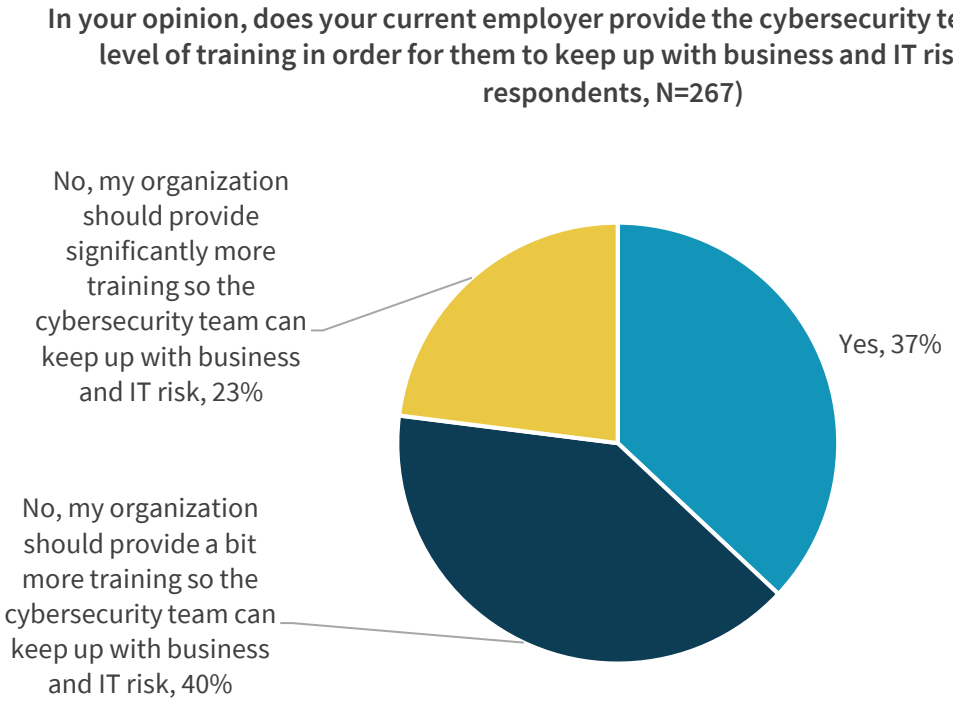


Source: Enterprise Strategy Group

As previously described, skills development is also a critical component of overall job satisfaction, but many organizations are not keeping up with an adequate level of cybersecurity training. Forty percent of ISSA members surveyed claim that their organizations should provide a bit more cybersecurity training while 23% believe their organizations should provide significantly more training (see Figure 15).

In 2018, 63% of organizations were not providing the proper amount of training to keep up with business and IT risks. Alarmingly, organizations are not making progress in this area as this percentage is similar to 2016 and 2017. It is safe to assume that many organizations are falling farther behind due to the lack of cybersecurity training.

Figure 15. Training Provided to Keep Up with Business and IT Risk



Source: Enterprise Strategy Group

Survey respondents were presented with many statements and asked whether they agreed or disagreed with each (see Figure 16). This data provides some strong opinions on the state of cybersecurity professional careers. For example:

- Identical to the 2017 results, 96% of survey respondents strongly agree or agree that cybersecurity professionals must keep up with their skills or their organizations face a significant disadvantage against cyber-adversaries.
- 86% of survey respondents strongly agree or agree that they are happy being a cybersecurity professional. This compares with 85% in 2017.
- 71% of survey respondents agree that they've had at least one job during their career where their employer didn't understand the requirements for cybersecurity defenses and operations. Unfortunately, this is an occupational hazard as there are still companies that will settle for "good enough security" rather than strive for strong security.
- 66% of survey respondents strongly agree or agree that while they try to keep up with their skills, it is difficult to do because of the demands of a cybersecurity career.

Note the polarizing situation between the first and last bullet above. Cybersecurity professionals believe it is imperative to keep up with their skills, yet many find it difficult to do so. CISOs should assess whether this is the case within their organizations and if so, address this with actions like job rotation and mandatory training requirements.

Figure 16. Respondents' Opinions on Cybersecurity Topics

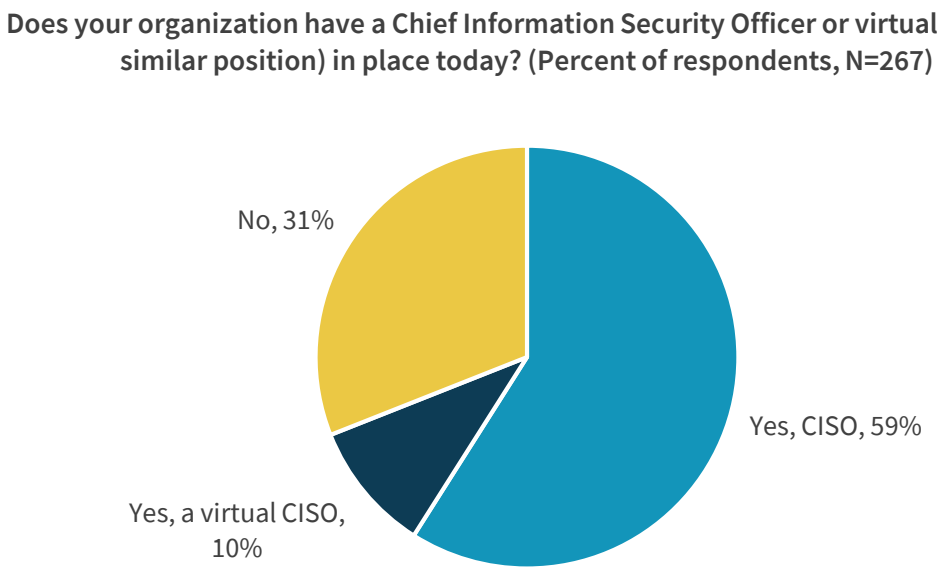
Please select one response per row that best reflects your opinion on each statement. (Percent of respondents, N=267)

Source: Enterprise Strategy Group

Cybersecurity Leadership

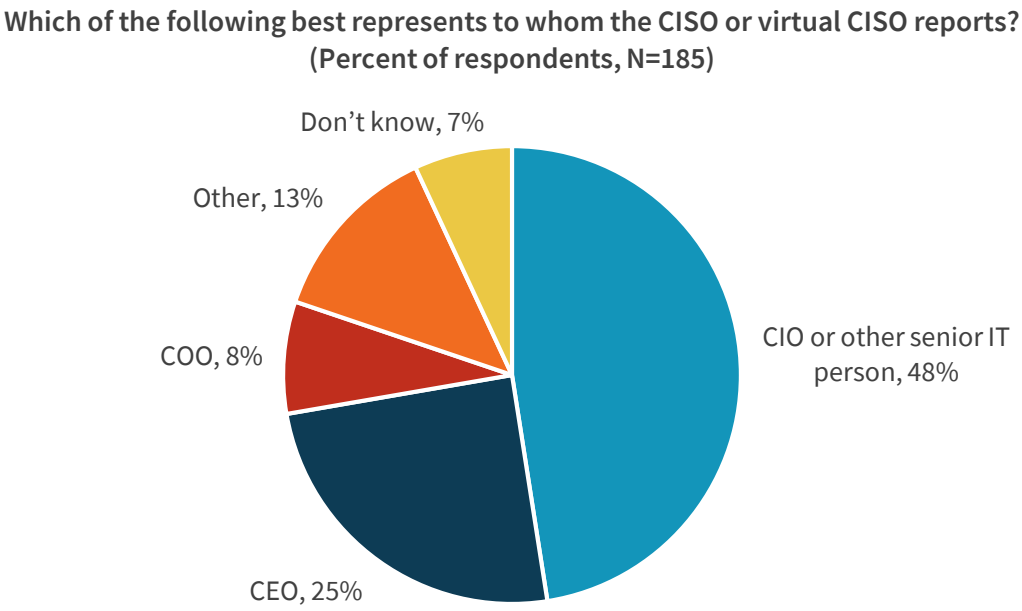
The majority of ISSA members surveyed work at organizations with a CISO (or equal position) employed (see Figure 17). Note that this year, ESG/ISSA included a virtual CISO which is a relatively new position. Ten percent of respondents reported that their organization has a virtual CISO. In many cases (48%), the CISO reports to a CIO or other senior IT person while 25% of CISOs report directly to a CEO. This is also consistent with past results (see Figure 18).

Figure 17. Does Organization Have a CSO/CISO?



Source: Enterprise Strategy Group

Figure 18. To Whom Does the CSO/CISO Report To?

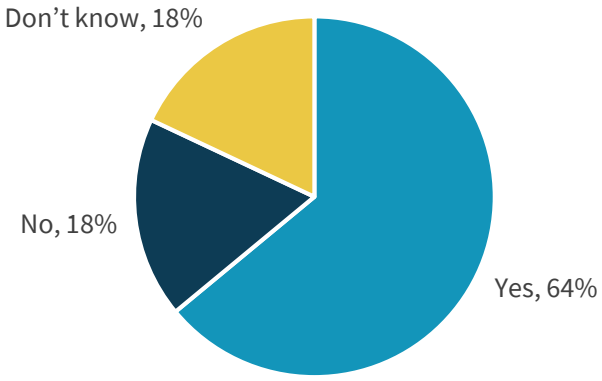


Source: Enterprise Strategy Group

A majority (64%) of survey respondents claim that their CISO is an active participant with executive management and the board of directors. This represents a bit of progress compared to last year (59%, see Figure 19).

Figure 19. Level of CISO Participation with Business Management

Is your organization's CISO or virtual CISO an active participant with executive management and the board of directors (or similar oversight group)? (Percent of respondents, N=185)

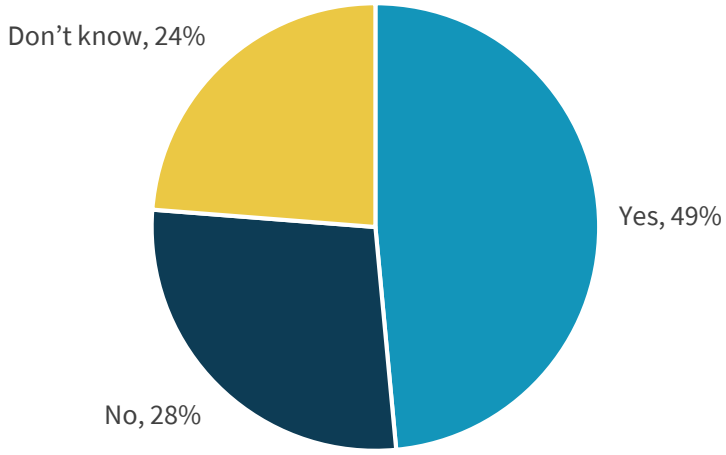


Source: Enterprise Strategy Group

While CISOs may be active participants with business managers, the question remains whether there is room for an even bigger contribution. Just under half (49%) of respondents believe CISOs participate at the right level but 28% seem to think that CISOs and business executives could do more together (see Figure 20).

Figure 20. Is CISO Level of Participation with Business Executives Adequate?

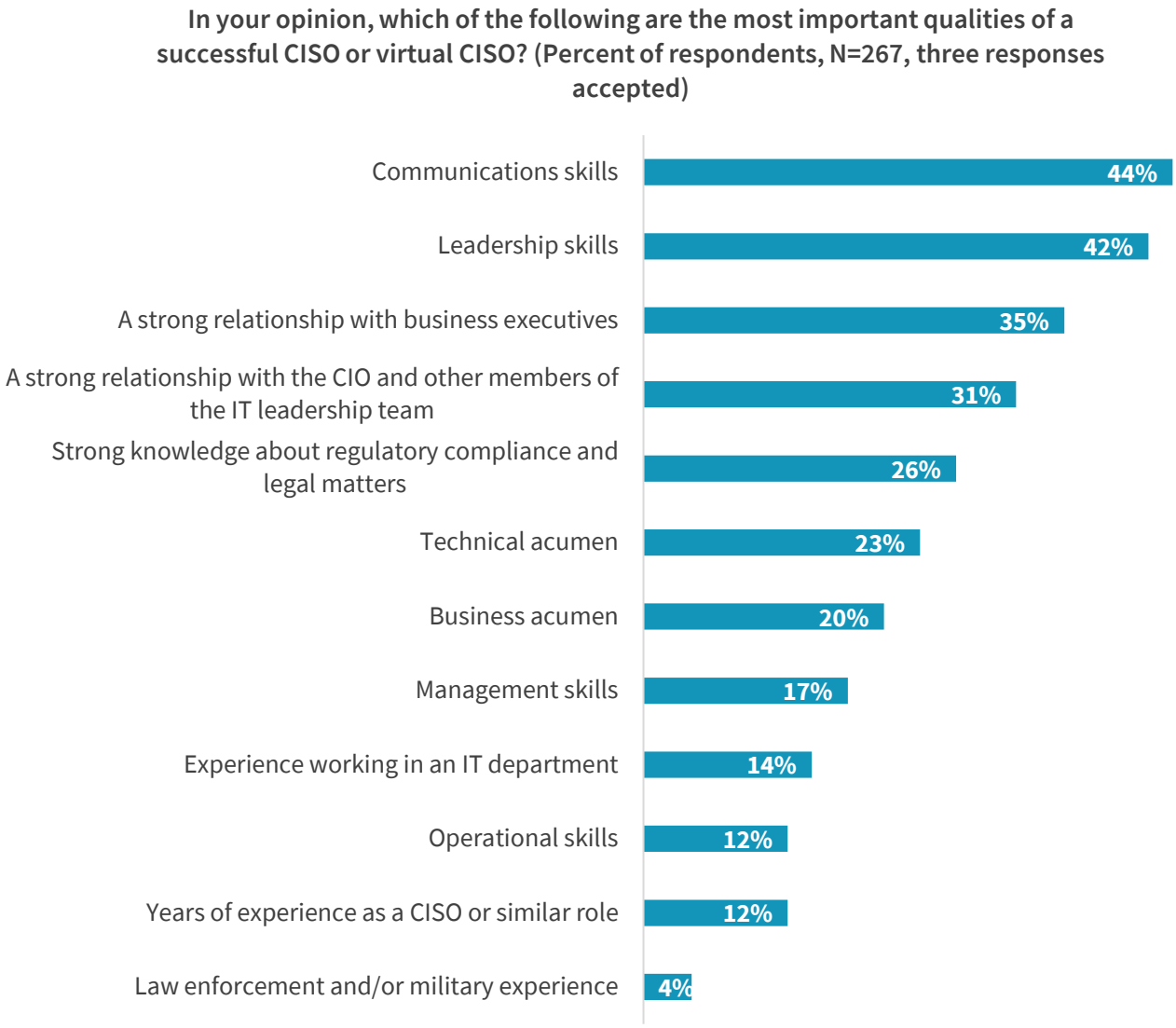
Do you think your CISO's or virtual CISO's level of participation with executive management and the board of directors is adequate? (Percent of respondents, N=185)



Source: Enterprise Strategy Group

What qualities make a CISO successful? The top responses in 2018 align with those of 2016 and 2017—namely, leadership skills, communications skills, a strong relationship with business executives, and a strong relationship with the CIO and IT leadership team (see Figure 21).

Figure 21. Most Important Qualities of a Successful CISO

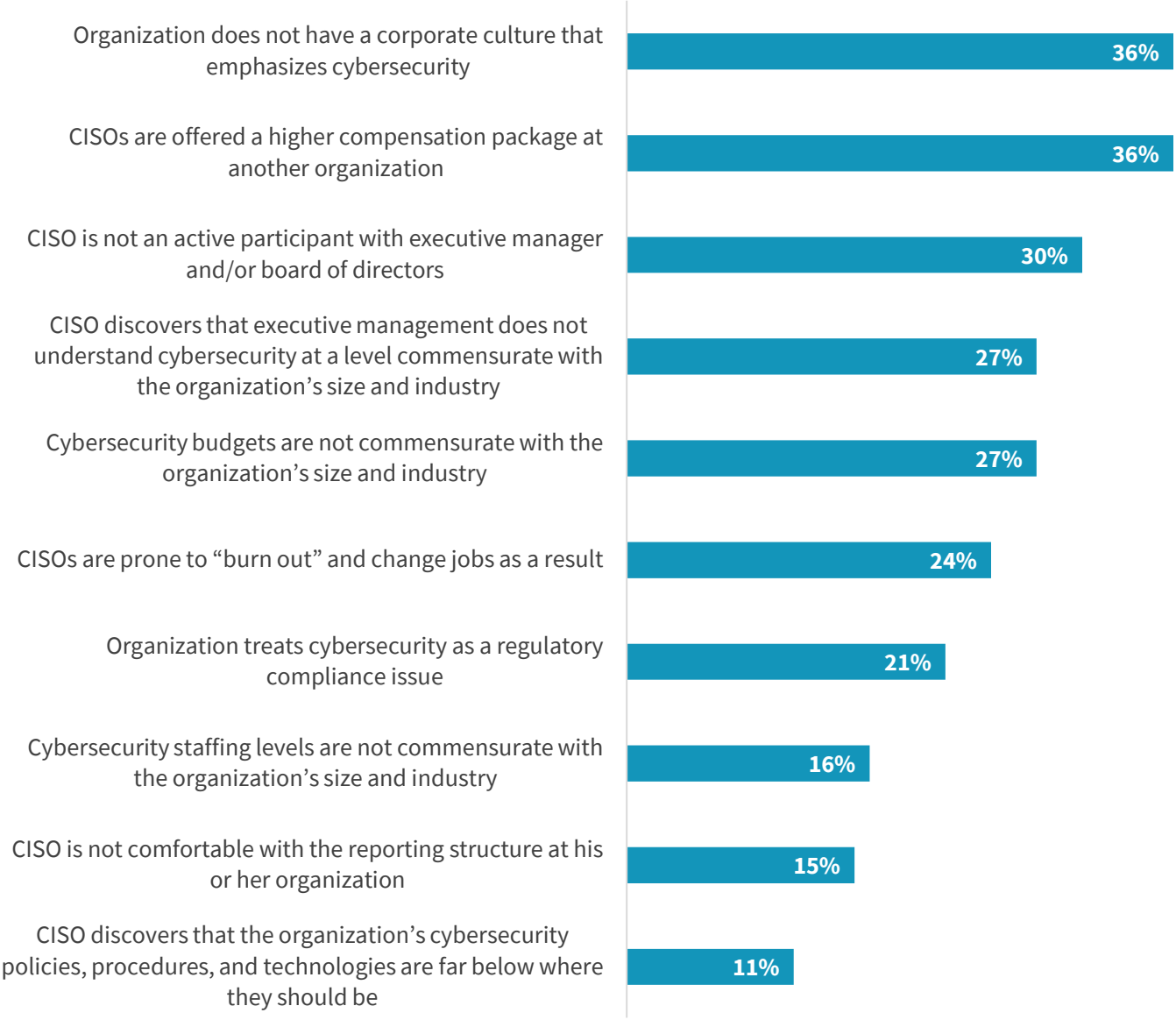


Source: Enterprise Strategy Group

CISOs are notorious "job hoppers," with the average tenure of each job around 24 to 48 months in length. Why do CISOs move on so quickly? ISSA members believe the main reasons CISOs move on include a corporate culture that doesn't include cybersecurity, higher compensation elsewhere, and a lack of participation with business management (see Figure 22). These results are consistent with past years.

Figure 22. Most Likely Factors to Cause a CISO to Leave an Organization

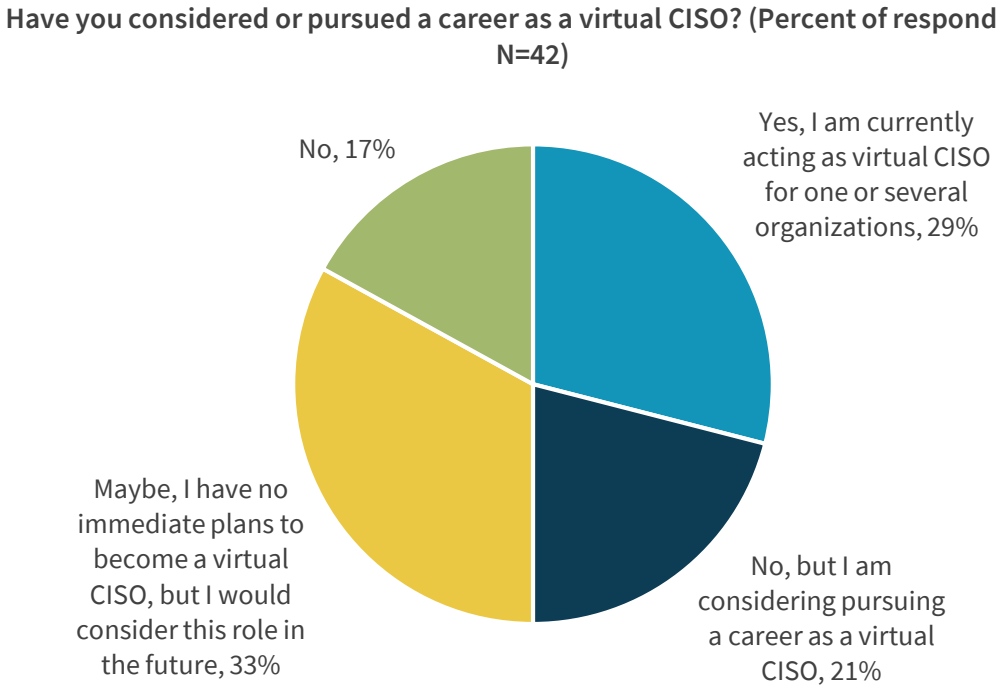
Industry research reports that the average tenure of a CISO is between 2 and 4 years. In your opinion, which of the following factors are likeliest to cause CISOs to leave one organization for another? (Percent of respondents, N=267, three responses accepted)



Source: Enterprise Strategy Group

Given the recent rise in the virtual CISO position, ESG/ISSA asked CISO respondents whether they've considered or pursued this type of position. Apparently, the virtual CISO career path is rather attractive—29% are currently acting as a virtual CISO for one or more organization, 21% are considering pursuing a virtual CISO career path, and 33% are open to becoming a virtual CISO sometime in the future (see Figure 23).

Figure 23. Consideration of a Virtual CISO Position



Source: Enterprise Strategy Group

Why become a virtual CISO? More variety/flexibility, the opportunity to span across industries, and the chance to work with multiple organizations (see Figure 24).

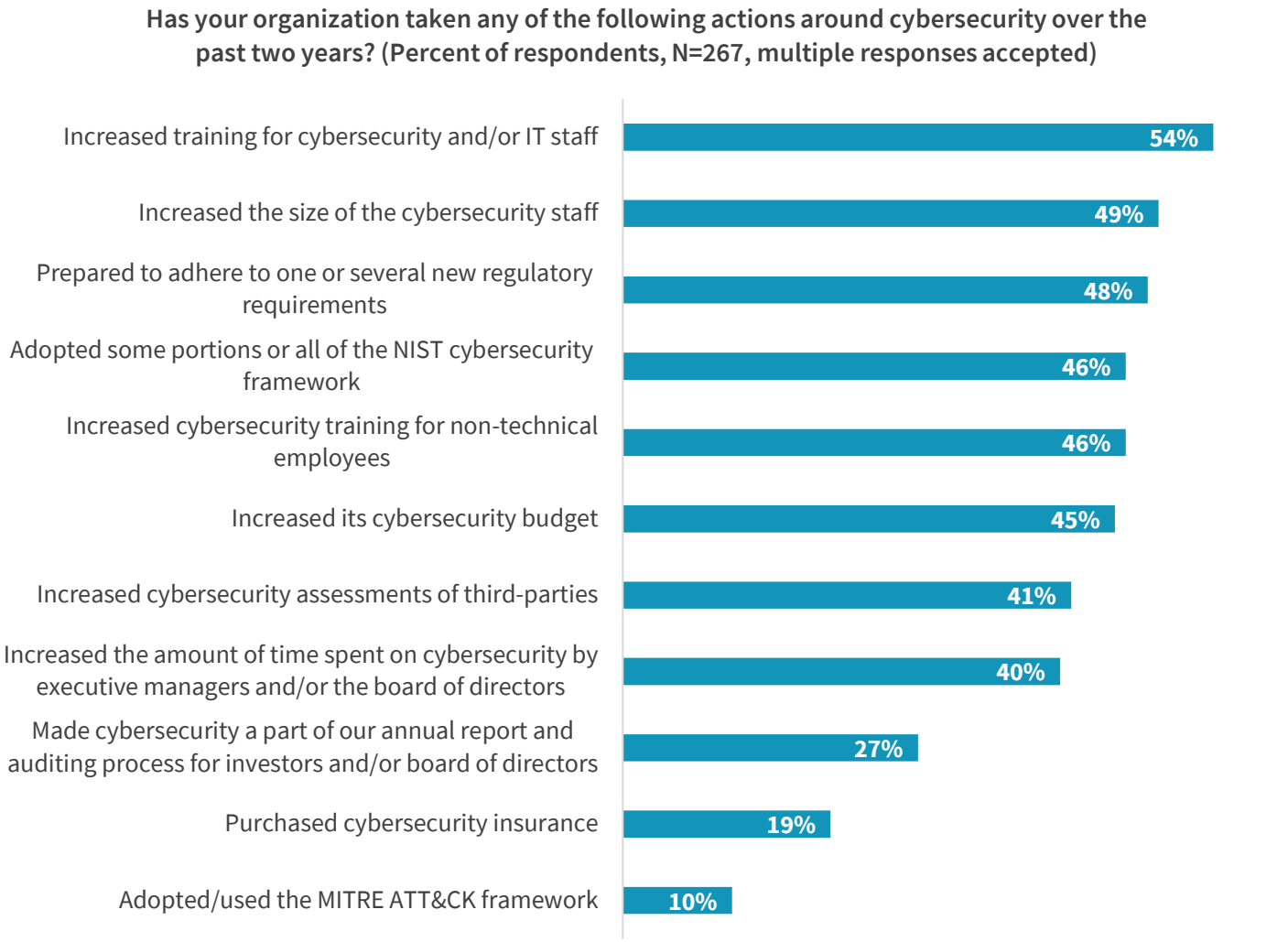
Figure 24. Attractive Attributes of a Virtual CISO Position

Source: Enterprise Strategy Group

The State of Cybersecurity

Survey respondents were asked to identify cybersecurity actions taken over the past two years. More than half (54%) of all organizations have increased training for cybersecurity and/or IT staff, 49% have increased the size of the cybersecurity staff, and 48% prepared to adhere to one or several new regulatory requirements (see Figure 25).

Figure 25. Cybersecurity Actions Taken over the Past Two Years



Source: Enterprise Strategy Group

Responses were a bit different in 2018 versus 2017 and the top five responses from each year are compared in Table 2.

Table 2. Cybersecurity Actions Taken over the Past Two Years by Year

Top Five Factors Cited in 2016	Top Five Factors Cited in 2017	Top Five Factors Cited in 2018
Engaged in one or more new cybersecurity initiative (i.e., deploying new types of cybersecurity technologies)	Adopted some portions or all of the NIST cybersecurity framework	Increased cybersecurity training for cybersecurity and/or IT staff
Increased security controls and monitoring for privileged users (i.e., IT administrators, etc.)	Increased cybersecurity training for cybersecurity and/or IT staff	Increased the size of the cybersecurity staff
Increased the size of the cybersecurity staff	Increased training for non-technical employees	Prepared to adhere to one or several new regulatory requirements
Adopted some portions or all of the NIST cybersecurity framework	Increased cybersecurity budget	Adopted some portions or all of the NIST cybersecurity framework
Implemented stronger controls to limit which users and devices can access sensitive applications and data	Prepared to adhere to one or several new regulatory requirements	Increased training for non-technical employees

Cybersecurity Incidents

ISSA members were asked about security incidents experienced by their organizations over the past two years. Nearly half (48%) of respondents have experienced at least one incident and only 12% claim no incidents. It is worth noting, however, that 40% of those surveyed said they don't know or prefer not to say (see Figure 26). Similarly, 34% of respondents selected "don't know/prefer not to say" in 2017.

Figure 26. Frequency of Security Incidents over the Past Two Years

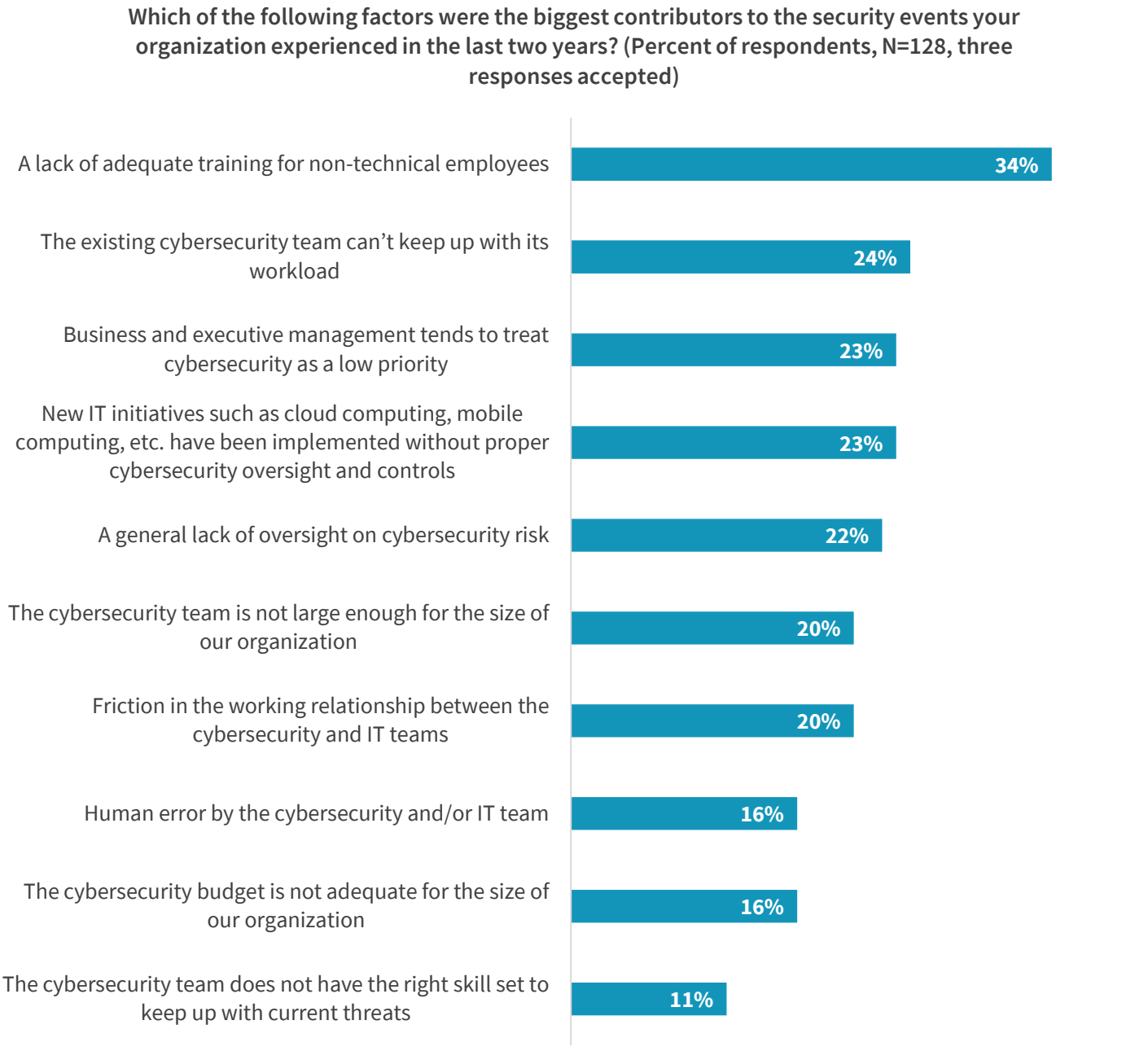
Source: Enterprise Strategy Group

Those respondents whose organizations experienced at least one security incident were then asked to identify root causes. ISSA members pointed to a lack of adequate training for non-technical employees, trouble keeping up with the

cybersecurity workload, and the fact that business and executive management tends to treat cybersecurity as a low priority (see Figure 27).

It is worth pointing out that a lack of adequate training for non-technical employees ranked first in 2017 and 2018. CISOs should gauge whether this is the case at their organizations and take the appropriate steps for security awareness training in response.

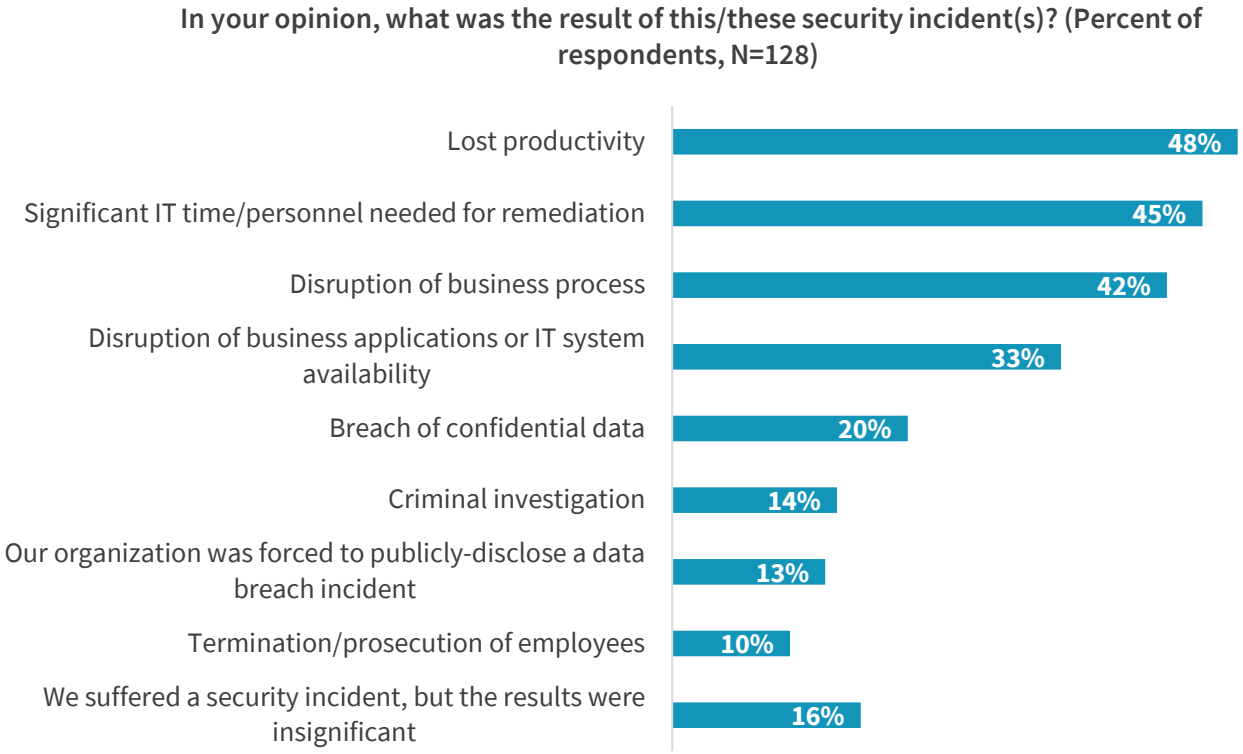
Figure 27. Biggest Contributors to Security Events Experienced



Source: Enterprise Strategy Group

The top three ramifications of security incidents were the same in 2017 and 2018—lost productivity, significant IT time/personnel for remediation, and disruption of business process (see Figure 28).

Figure 28. Results of Security Incidents

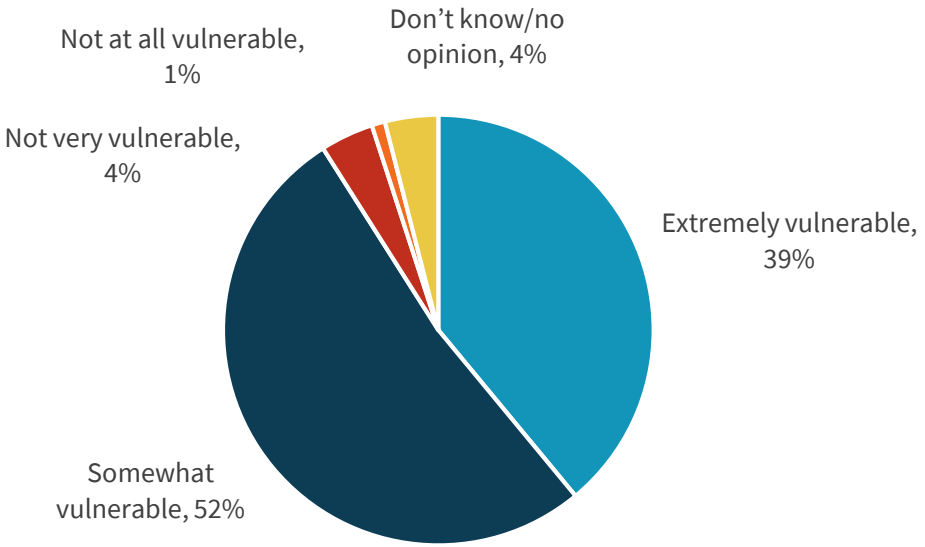


Source: Enterprise Strategy Group

Given the constant onslaught of data breaches, it is not surprising that 91% of survey respondents believe that most organizations are either extremely vulnerable or somewhat vulnerable to a significant cyber-attack (i.e., one that disrupts business processes or leads to a data breach, see Figure 29). These results have been relatively consistent over the past three research projects.

Figure 29. Vulnerability of Most Organizations to a Significant Cyber-attack or Data Breach

In your opinion, how vulnerable are most organizations (other than your own) to a significant cyber-attack or data breach (i.e., one that disrupts business processes or leads to theft of sensitive data)? (Percent of respondents, N=267)



Source: Enterprise Strategy Group

ISSA members were asked to identify the top cybersecurity challenges at their organizations. The first three responses were consistent with last year, namely (see Figure 30):

- **The cybersecurity staff is understaffed for the size of my organization.** An identical percentage of respondents (29%) selected this response in 2017 and 2018. Obviously, the global cybersecurity skills shortage continues to impact many organizations.
- **Business managers don't understand and/or support an appropriate level of cybersecurity.** While the percentage of ISSA members who selected this response was nearly identical (23% in 2018 versus 24% in 2017), this selection climbed from third to second place in 2018. ESG and ISSA are especially troubled by this response since it indicates that many business managers still don't recognize obvious and growing cyber-risks. It's likely that these organizations have bad reputations within the cybersecurity professional community and will struggle to hire and retain cybersecurity staff.
- **My organization depends upon too many manual and/or informal processes for cybersecurity.** Twenty-eight percent of respondents selected this choice in 2017 as compared to 23% in 2018. Still, manual processes continue to burden security operations staff—especially considering their continuously growing workload.

Twenty-three percent of ISSA members also selected "managing the complexity of too many disconnected point tools for cybersecurity." Thus, this response was tied for second place in 2018, moving up from fifth place in 2017 at 17%. It's likely that an increasing cybersecurity workload along with a reliance on manual processes exacerbated challenges associated with purchasing, testing, deploying, configuring, and operating disconnected point tools over the past year.

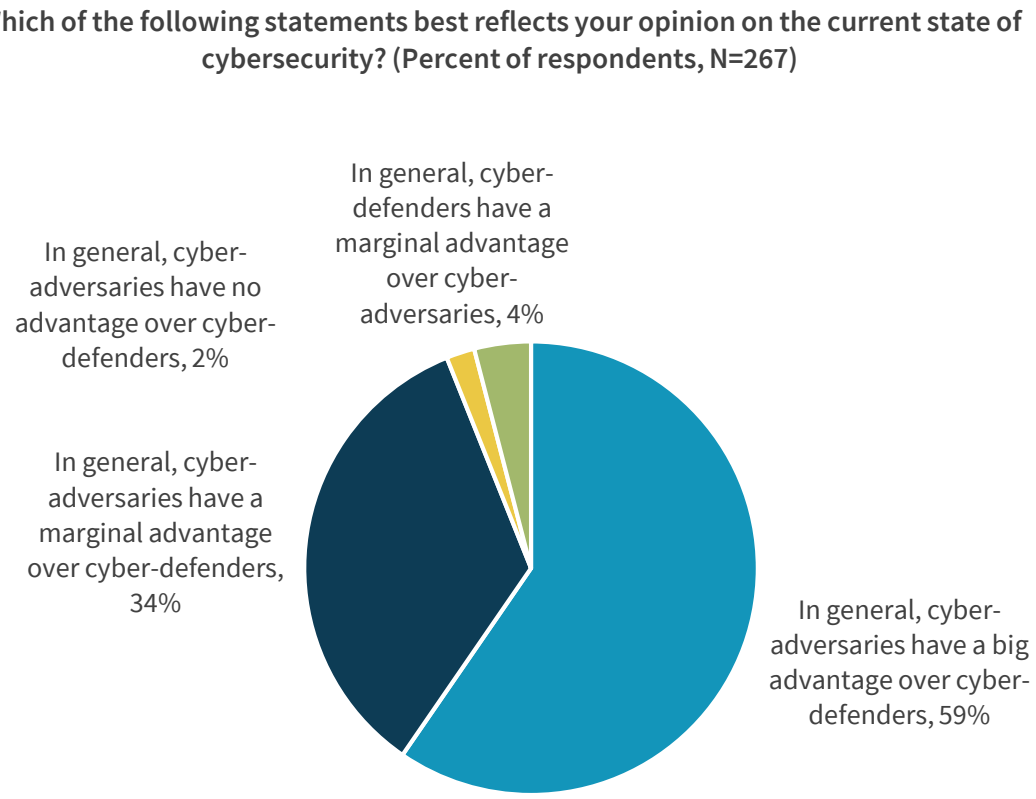
Figure 30. Biggest Cybersecurity Challenges

Which of the following would you say are the biggest cybersecurity challenges at your organization? (Percent of respondents, N=266, three responses accepted)

Source: Enterprise Strategy Group

In another new question for 2018, ISSA members were asked to compare the status of cyber-adversaries versus cyber-defenders. The results are not surprising but alarming nonetheless as more than half (59%) of respondents believe that cyber-adversaries have a big advantage over cyber-defenders while 34% felt that cyber-adversaries have a marginal advantage over cyber-defenders (see Figure 31). Alternatively, only 4% believe that cyber-defenders have any type of advantage over cyber-adversaries.

Figure 31. Cyber-adversaries Have a Distinct Advantage over Cyber-defenders



Source: Enterprise Strategy Group

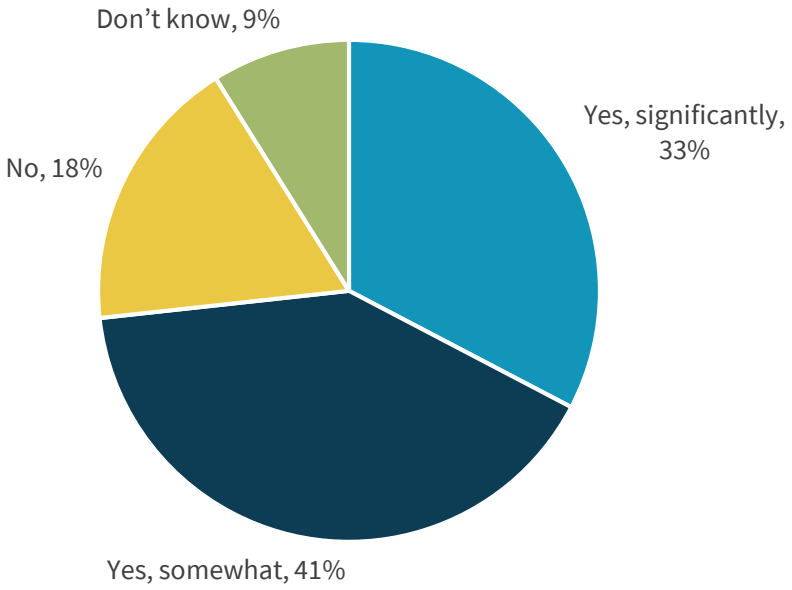
In summary, the ESG/ISSA data reveals a pattern of security incidents resulting in business disruption. Organizations remain bogged down with numerous cybersecurity challenges such as a shortage of personnel, a reliance on manual processes, and an infrastructure made up of disconnected point tools. This combination must have a profound impact on cybersecurity productivity. Finally, cybersecurity professionals are pessimistic about their plight, believing that most organizations are vulnerable to cyber-attacks and that cyber-adversaries have the upper hand. If cybersecurity is improving, it isn't improving by much.

The Cybersecurity Skills Shortage

As in past years, ESG and ISSA wanted to understand how the global cybersecurity skills shortage is impacting organizations. The data indicates that the situation is not improving, as 33% of cybersecurity professionals say that the cybersecurity skills shortage has had a significant impact on their organizations, while 41% claim that their organizations have been impacted somewhat by the global cybersecurity skills shortage (see Figure 32). These responses were similar to those of 2016 (29% said "significantly," 40% said "somewhat") and 2017 (27% said "significantly," 43% said "somewhat").

Figure 32. Level of Impact of the Cybersecurity Skills Shortage

There has been a lot written about the global cybersecurity skills shortage. Has this trend impacted the organizations you've worked for over the past few years? (Percent of respondents, N=267)



Source: Enterprise Strategy Group

Once again, survey respondents working at organizations impacted by the cybersecurity skills shortage were asked to identify the associated consequences. Increasing workload on existing staff was the top response for the third year in a row (see Figure 33). Additionally, the cybersecurity skills shortage has impacted organizations in numerous other ways, including:

- **Modifying hiring and operating strategies.** Since organizations can't find skilled professionals, they often hire and train junior personnel or outsource security tasks to service providers.
- **Impacting the relationship with the business.** Alarmingly, 40% say that the cybersecurity staff has limited time to work with business units to align cybersecurity with business processes. This means that the skills shortage impacts everyone—shareholders, customers, employees, etc.
- **Ineffective use of cybersecurity technologies.** Nearly half (47%) of respondents say that the cybersecurity skills shortage has led to a situation where organizations don't have the time or personnel to fully learn or utilize some security technologies to their full potential. Clearly, security controls are of little use if they are underutilized.
- **High "burn-out" rates.** While workload is increasing, cybersecurity teams remain understaffed. Little wonder then why cybersecurity professionals spend an inordinate amount of time firefighting, leading to employee burn-out.

Figure 33. How the Cybersecurity Skills Shortage Has Impacted Organizations

Source: Enterprise Strategy Group

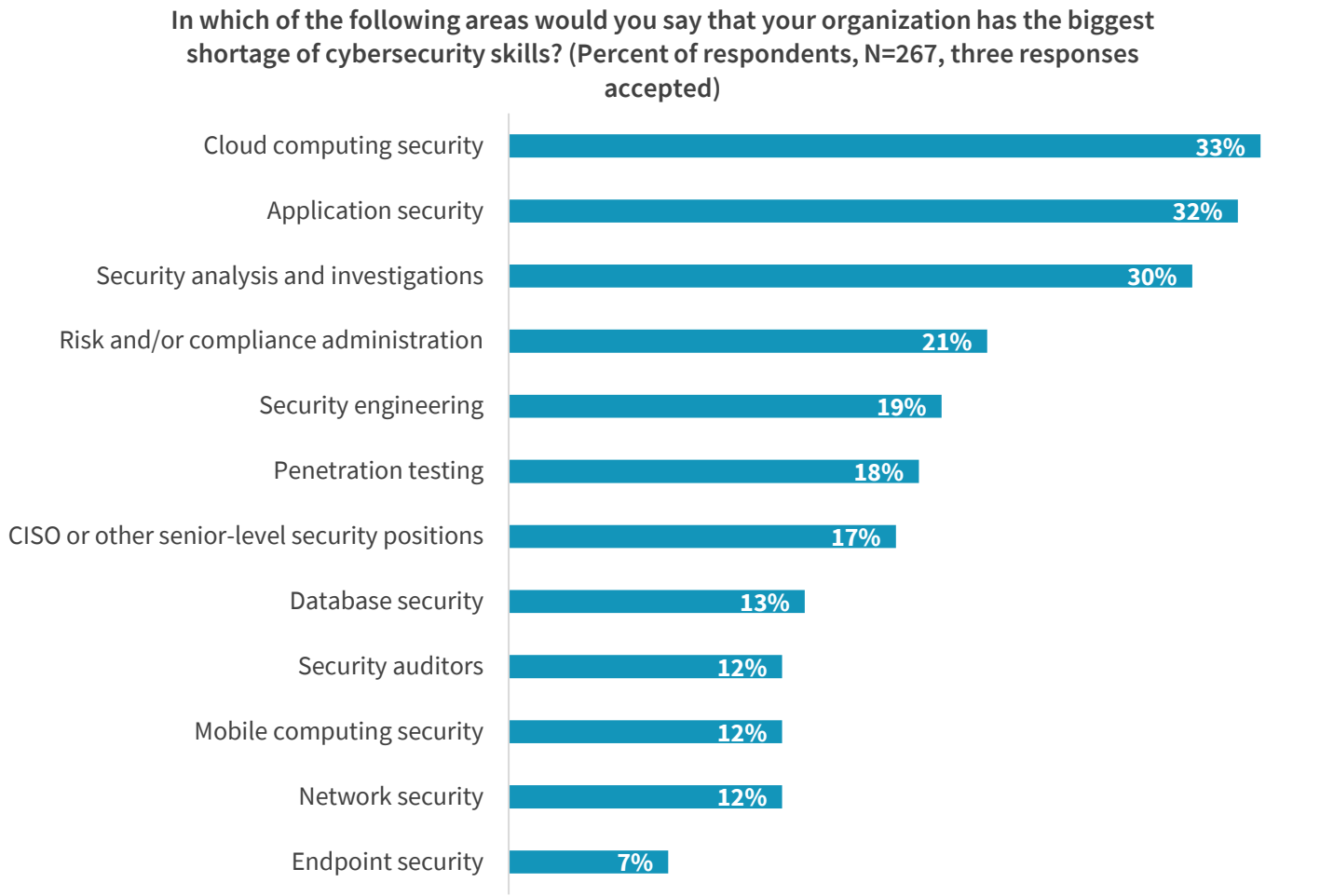
There were slight changes to the order of responses in 2018. The top four responses for the past three ESG/ISSA research projects are displayed in Table 3.

Table 3. How the Cybersecurity Skills Shortage Has Impacted Organizations by Year

Top Four Factors Cited in 2016	Top Four Factors Cited in 2017	Top Four Factors Cited in 2018
Increased workload on existing staff	Increased workload on existing staff	Increased workload on existing staff
Need to hire and train junior staff rather than experienced cybersecurity professionals	Need to hire and train junior staff rather than experienced cybersecurity professionals	Inability to utilize/learn some security technologies to their full potential
Inability to utilize/learn some security technologies to their full potential	Cybersecurity staff time is spent disproportionally on high priority events	Need to hire and train junior staff rather than experienced cybersecurity professionals
Higher attrition and turnover in cybersecurity staff	Cybersecurity team has limited time to work with business units	Cybersecurity team has limited time to work with business units

While most organizations are feeling the impact of the global cybersecurity skills shortage, ESG/ISSA wanted to understand the areas where cybersecurity skills shortages were most acute. The top areas in 2018 included cloud computing security (33%), application security (32%), and security analysis and investigations (30%, see Figure 34). These three areas have topped the list in all three years of the ESG/ISSA research effort.

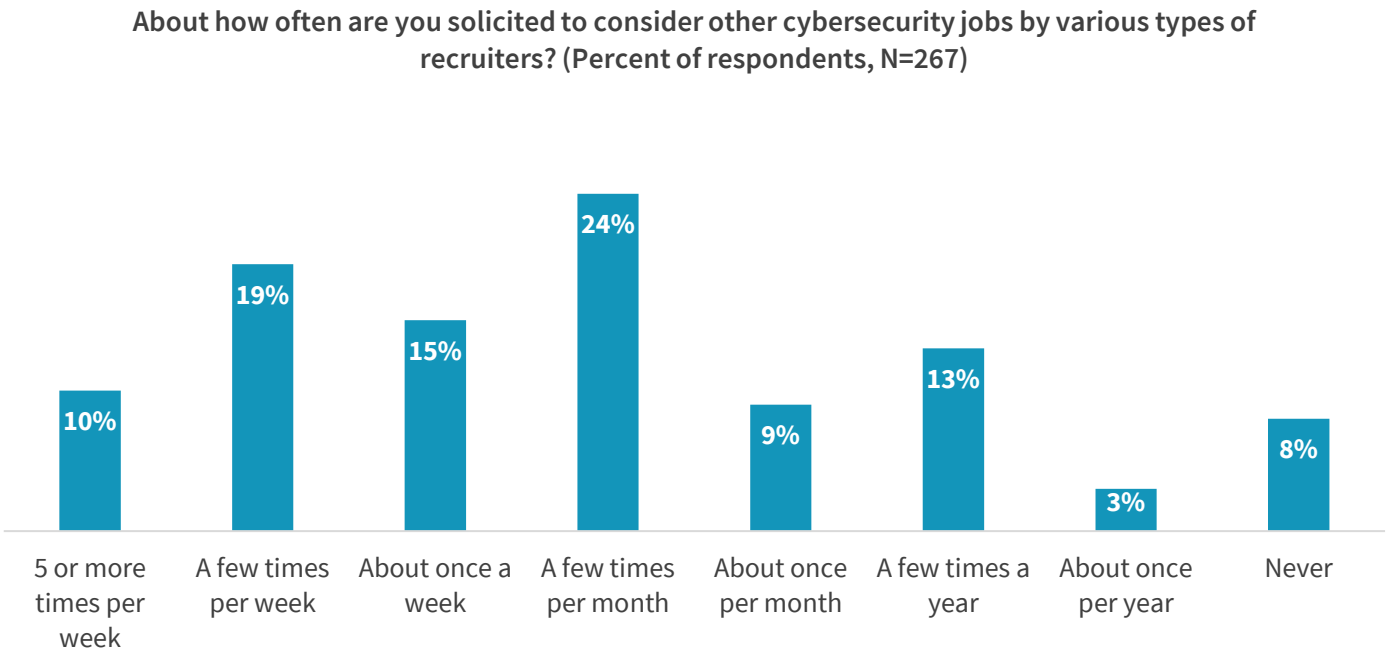
Figure 34. Area(s) with Biggest Shortage of Cybersecurity Skills



Source: Enterprise Strategy Group

The global cybersecurity skills shortage has created a "sellers' market" for cybersecurity talent where skilled cybersecurity professionals are constantly contacted by recruiters and offered significantly higher compensation to take another position. In 2018, 44% of ISSA members say that they are solicited to consider other cybersecurity jobs at least once per week, while more than three-quarters (77%) are solicited at least once per month (see Figure 35). These results are consistent with past years.

Figure 35. Frequency of Solicitation by Job Recruiters

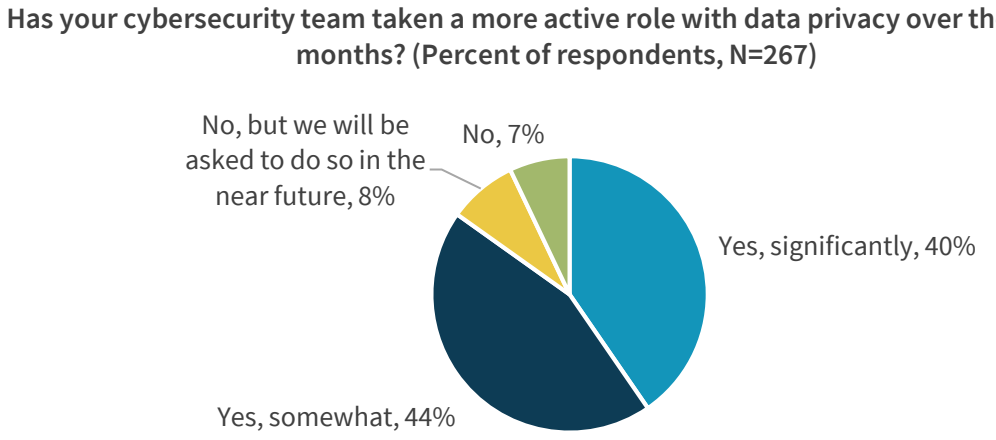


Source: Enterprise Strategy Group

The Quest for Cybersecurity Improvement

In a new thread for 2018, ESG/ISSA asked respondents several questions about data privacy. The research reveals that 84% of respondents claim that the cybersecurity team at their organization has taken a more active role in data security while 8% expect to be asked to do so in the future (see Figure 36).

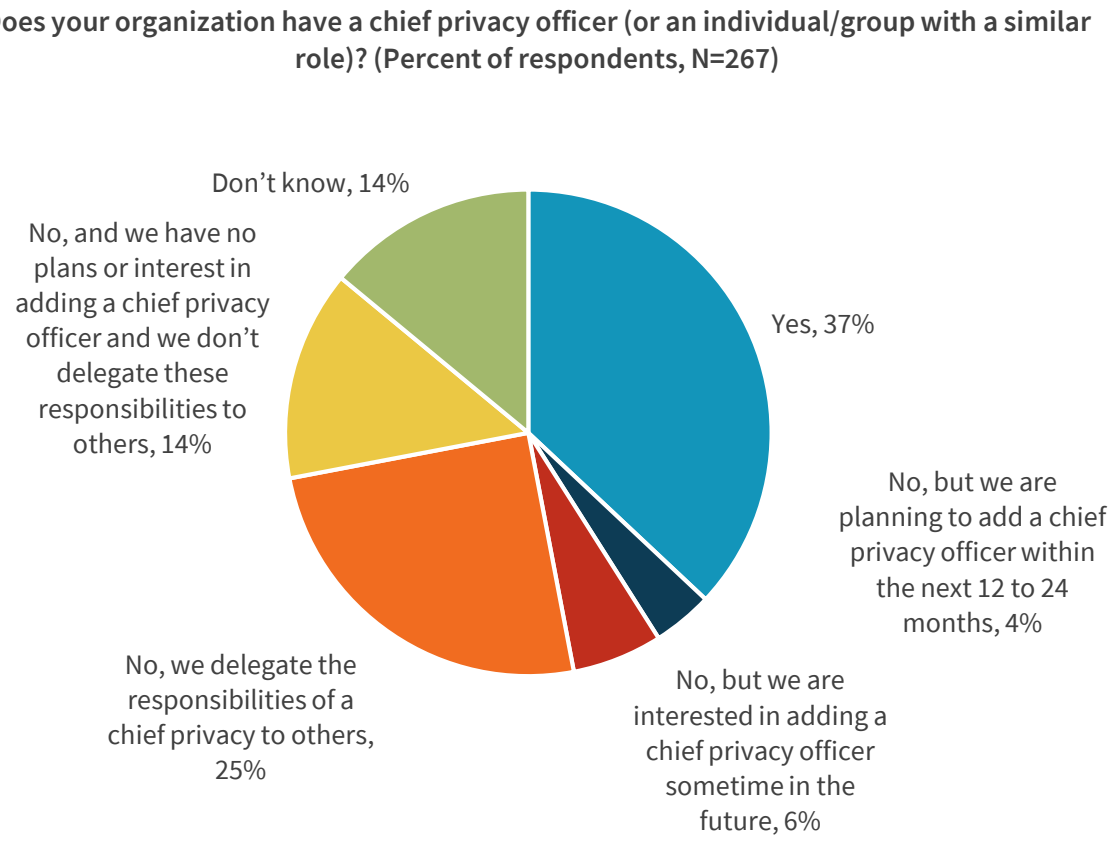
Figure 36. Cybersecurity Teams Are More Active in Data Privacy



Source: Enterprise Strategy Group

While cybersecurity teams are getting more involved, data privacy is often the responsibility of a chief privacy officer rather than a CISO. Do organizations have this role in place? As it turns out, 37% of organizations do (see Figure 37), far lower than the 69% that employ a CISO or virtual CISO. As regulations like GDPR and the California Consumer Privacy Act (CCPA) gain momentum, more organizations will likely create positions for chief privacy officers. This is likely to create a shortage of qualified professionals, driving salary inflation.

Figure 37. Does Organization Have a Chief Privacy Officer?



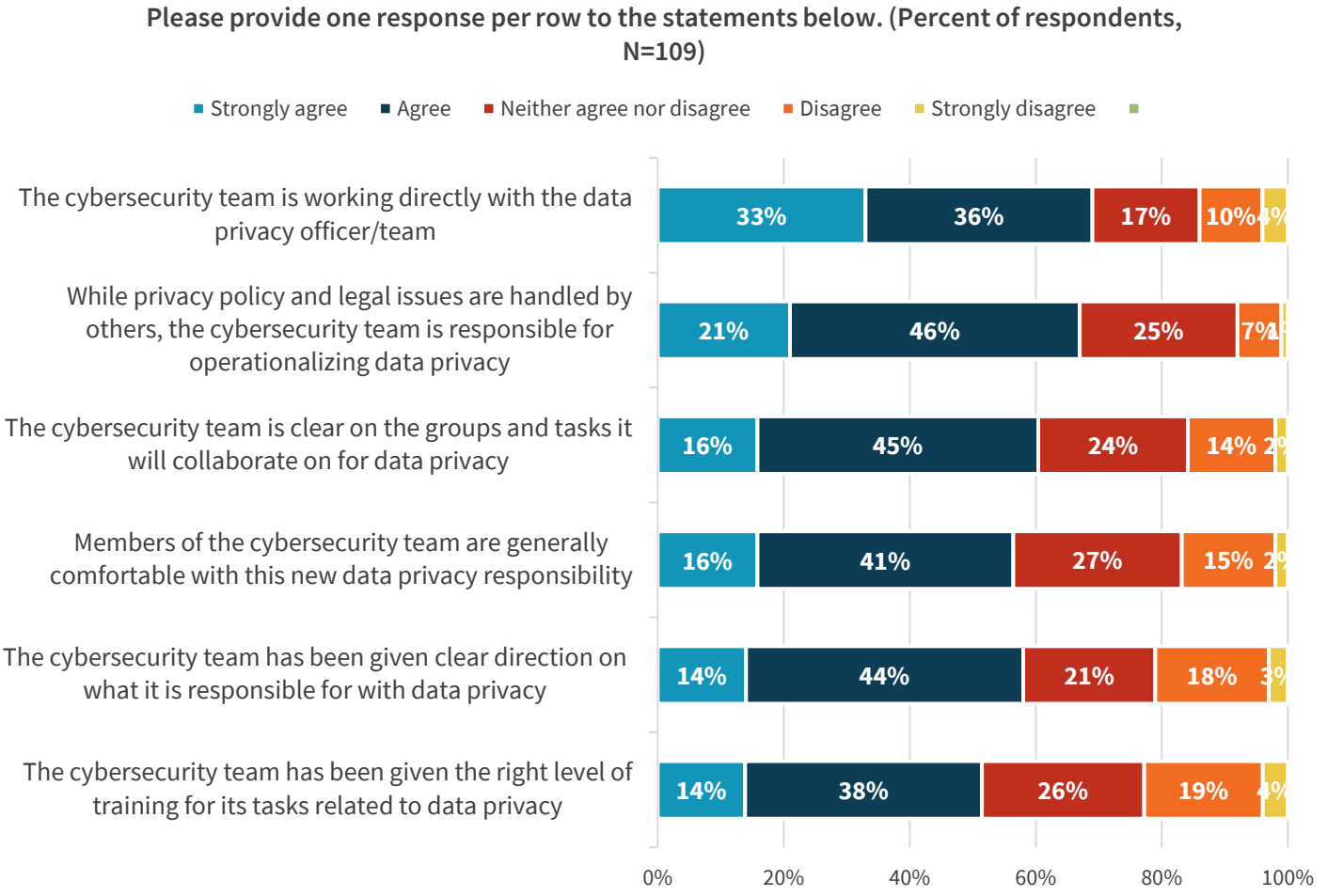
Source: Enterprise Strategy Group

Cybersecurity teams may be more involved in data privacy, but the data indicates that there is still a lot of work ahead. Cybersecurity teams are working with chief privacy officers to operationalize data privacy, but the data also indicates:

- 23% strongly disagree or disagree that cybersecurity teams have been given the right level of training for their tasks related to data privacy.
- 21% strongly disagree or disagree that cybersecurity teams have been given clear direction on what they are responsible for with data privacy.

Based upon this data, CISOs should assess whether their teams are prepared for their new data privacy responsibilities or not. Unprepared organizations must define best practices, create clear roles and responsibilities, and provide adequate training to the cybersecurity staff.

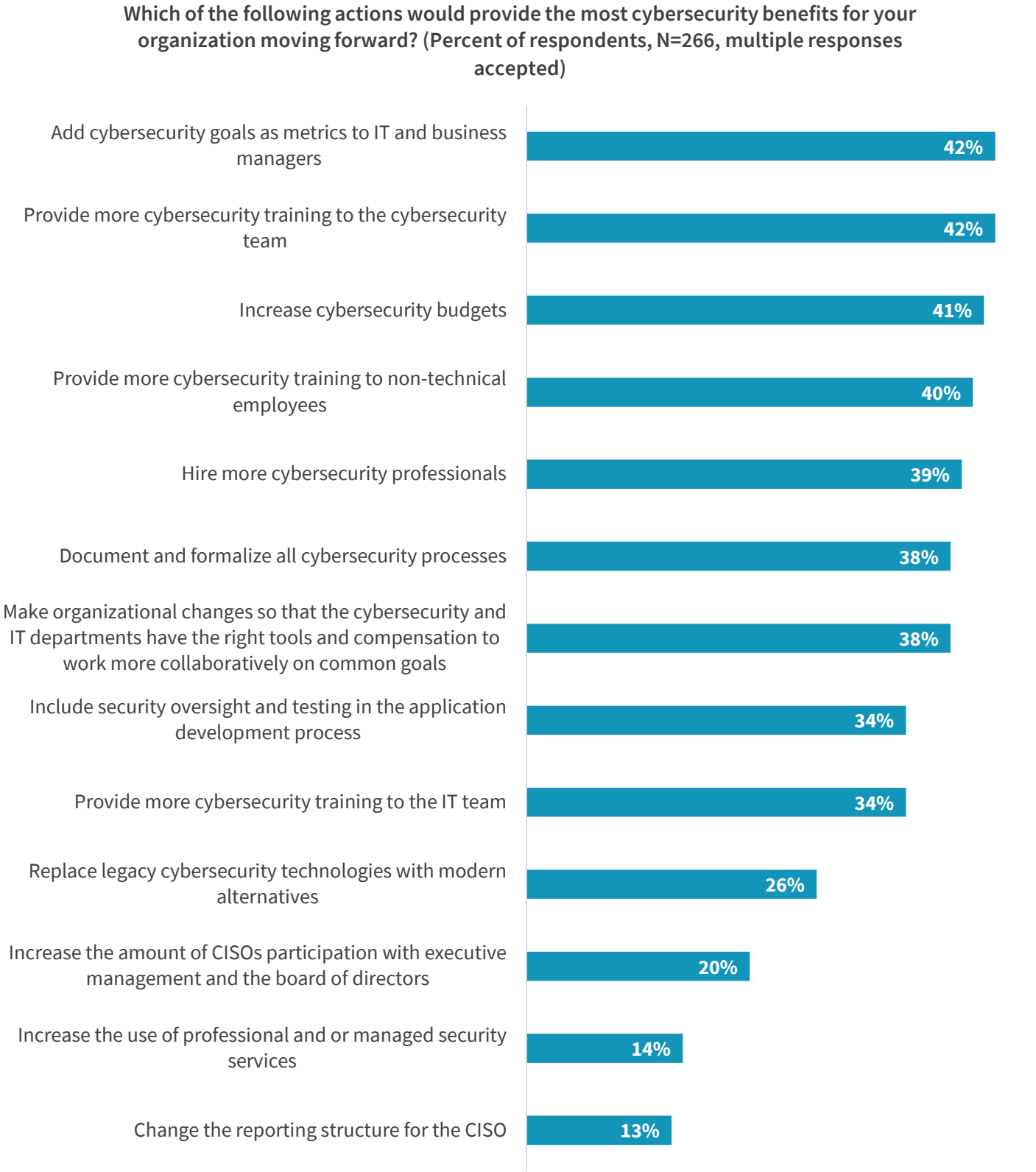
Figure 38. Data Privacy Opinions



Source: Enterprise Strategy Group

Finally, cybersecurity professionals were asked to identify the most beneficial cybersecurity actions their organizations could take in the future. The most commonly identified actions include adding cybersecurity goals and metrics to IT and business managers (42%), providing more cybersecurity training to the infosec team (42%), increasing the cybersecurity budget (41%), and providing more cybersecurity training to non-technical employees (40%, see Figure 39). Responses are tightly clustered, indicating that many organizations need to work on improvements across people, processes, and technologies.

Figure 39. Actions That Would Provide the Most Cybersecurity Benefits



Source: Enterprise Strategy Group

Conclusion

The ESG/ISSA report reveals several pervasive issues:

1. Cybersecurity professionals continue to focus on short-term responsibilities and don't pay enough attention to career development.
2. Most cybersecurity professionals don't pursue or receive the right level of skills development to address the rapidly evolving threat landscape. This leads to a steady increase in cyber-risk at their organizations.
3. While many cybersecurity professionals are content with their career choice, they remain rather pessimistic about cybersecurity in general. Most feel that organizations are highly vulnerable to cyber-attacks and believe that cyber-adversaries have a distinct advantage over defenders.
4. The cybersecurity skills shortage continues to impact most organizations, meaning that they don't have the right skills or staff to keep up with a growing workload. Once again, this can lead to unacceptably high levels of cyber risk.
5. While it's hard to believe in 2019, many organizations still eschew strong cybersecurity in favor of "good enough" cybersecurity.

Implications for Cybersecurity Professionals

As always, cybersecurity professionals should use the ESG/ISSA research for career planning. This is especially true for those in the early stages of a cybersecurity career or individuals seeking to enter the field. The data indicates that cybersecurity professionals should:

- Remain proactive toward career development. Just as in past reports, the 2018 study reveals that most cybersecurity professionals don't have a well-defined career path or plan to get to the next level. ESG/ISSA believe that cybersecurity professionals should invest time in career development and planning at all stages of their career lifecycles. Given the growing diversity around cybersecurity, professionals can take their careers in different directions including cybersecurity technology, cyber-risk management, data privacy, or a more business-centric direction.
- Gain hands-on experience at the expense of more industry certifications. While a limited number of industry certifications (i.e., CISSP, CISM, CompTIA Security+) are useful on resumes and to find jobs, cybersecurity professionals get a lot more career value from interfacing with peers, attending trade shows, and participating in focused technical training sessions. This type of hands-on career participation is highly recommended.
- Highlight business skills development. The bad news is that despite a continuous wave of cybersecurity headlines, there is still a large gap between cybersecurity and business priorities and knowledge. The good news is that this gap opens opportunities for savvy cybersecurity professionals. Those that can align cybersecurity oversight, risk management, and technical knowledge with business strategy and processes have the opportunity to become the next generation of CISOs.
- Job shop if you must. The research indicates that too many organizations still minimize their commitment to cybersecurity as much as possible. Given the overall market, cybersecurity professionals shouldn't suffer the frustration of working in this type of environment. To avoid similar dead-end positions, cybersecurity professionals

should look for opportunities at organizations that provide training incentives, career development services, and mentoring programs to maximize the potential for job satisfaction.

- **Anticipate and plan for a cybersecurity skills shortage.** For the third year in a row, the ESG/ISSA data suggest that most organizations are experiencing the impact of the cybersecurity skills shortage in one way or another. Cybersecurity professionals (and especially CISOs) must assume that they will be short on people and skills in every decision they make and every project they undertake. To address the cybersecurity skills shortage directly, infosec pros will need to increase their dependence on managed/professional services, automate manual processes, do everything they can to decrease the attack surface, improve cyber-risk management data analysis, prioritization, and mitigation, and experiment with more use of advanced analytics technologies.

Research Implications for Employers

All organizations face cutthroat competition to recruit, hire, train, and retain top cybersecurity talent. To succeed where others fail, organizations must:

- **Look for cybersecurity bodies in new places.** Typically, cybersecurity professionals come from three areas: IT, enforcement, and the military, but these wells seem to be running dry. To bridge this gap, organizations must be more creative by recruiting outside these safe havens. CISOs should be charismatic leaders who preach the virtues and excitement of a cybersecurity career, taking this message to business units, universities, career fairs, etc. Their stories should include the diverse opportunities around a cybersecurity career, with different paths toward business, legal, geopolitical, and technical destinations.

- **Push for more internal cybersecurity training.** Regrettably, cybersecurity training levels are inappropriately low at many organizations, increasing cyber-risk. As the research clearly indicates, a cybersecurity career demands continuing education, so infosec managers must make education and training a top priority. CISOs should encourage staff members to join professional organizations, attend trade shows, and pursue advanced training courses. Smart CISOs will also develop mentoring programs and push for continuous and required onsite training on a regular basis.

- **Create a center of cybersecurity excellence.** The research indicates that cybersecurity professionals find job satisfaction at organizations that provide adequate levels of training, have a cybersecurity culture, and employ a talented cybersecurity staff. Alternatively, infosec pros become frustrated when they aren't included in business and IT planning or are forced to fight with ignorant end-users. Since CISOs must fight to attract and retain cybersecurity talent, they should use the ESG/ISSA data as a guideline for creating a cybersecurity center of excellence. How? Partner with CEOs and business leaders to create a hands-on cybersecurity culture. Work with HR to establish continuous end-user security awareness training. Dedicate staff hours for training and continuing education. Invest in staff skills progression and career development. When all these activities are up and running, spread the word far and wide. This may not alleviate the impact of the skills shortage, but it will give an organization an advantage over many others.

- **Professionalize incident response.** Many organizations will experience one or several security incidents over the next year and cyber-attackers are growing more sophisticated and nefarious. This unfortunate reality means that organizations must have skills and processes in place to detect and respond to security incidents as quickly as possible. CISOs must assess their abilities in these areas and seek out help if they aren't up to the critical tasks at hand. Furthermore, organizations must replace informal and manual processes with best practices. For those looking for a template in this area, the NIST-800-61 Computer Incident Handling Guide can help.

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, and Asia, and Australia between December 3, 2018 and January 22, 2019.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, we were left with a final total sample of 267 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.

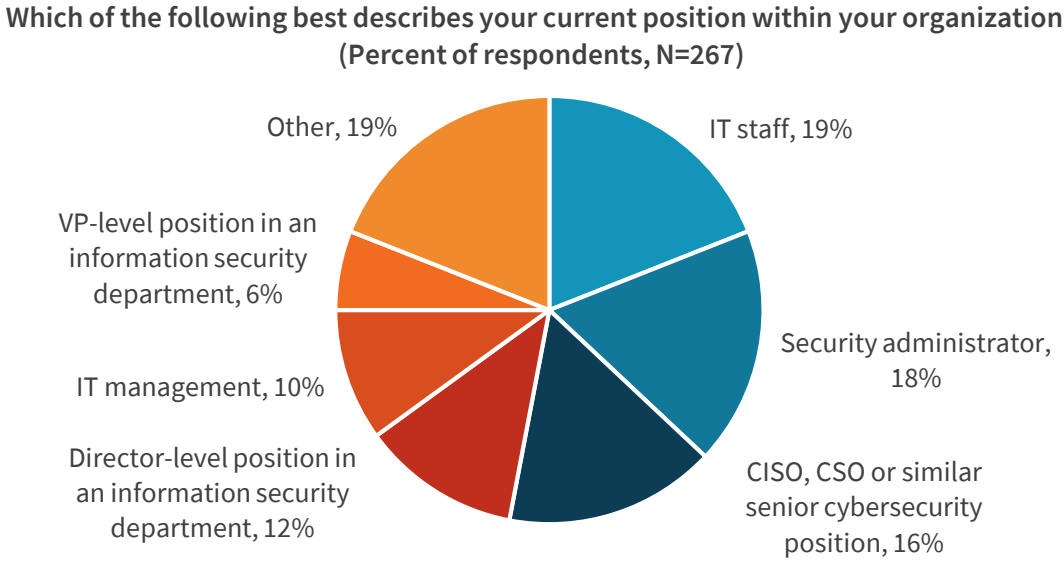
Respondent Demographics

The data presented in this report is based on a survey of 343 qualified respondents and cybersecurity professionals. Figures 40 - 43 detail the demographics of the respondent base at an individual and organizational level.

Respondents by Current Position

Respondents' current role is shown in Figure 40.

Figure 40. Respondents by Current Position

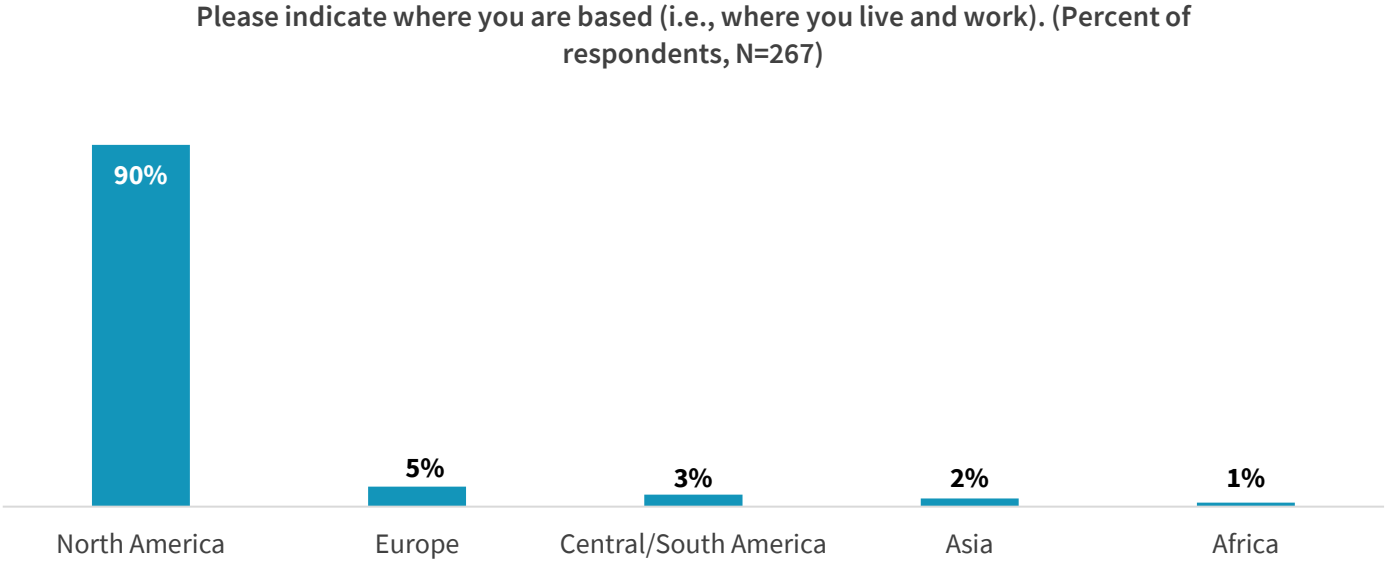


Source: Enterprise Strategy Group

Respondents by Region

The regional breakdown of respondents is shown in Figure 41.

Figure 41. Respondents by Region

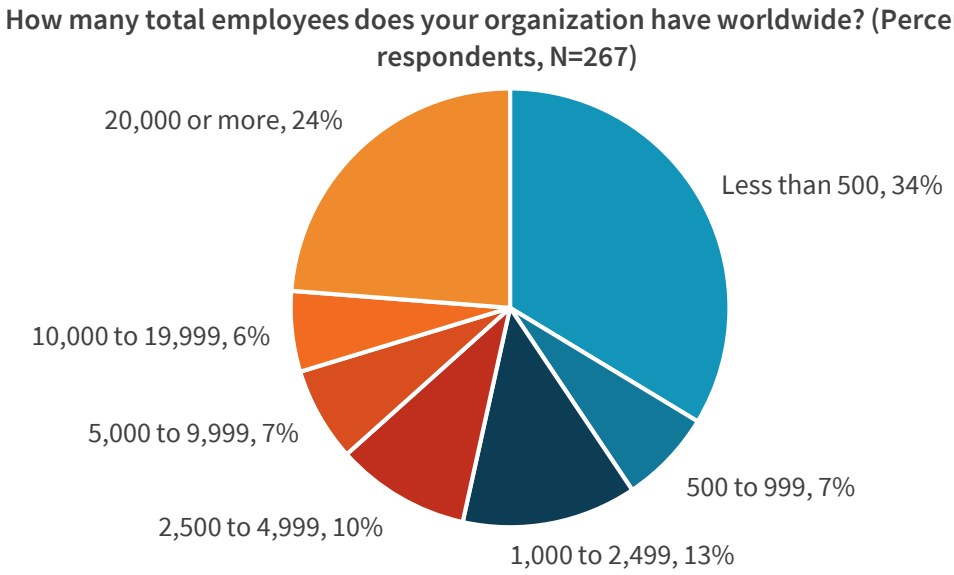


Source: Enterprise Strategy Group

Respondents by Number of Employees

The number of employees in respondents' organizations is shown in Figure 42.

Figure 42. Respondents by Number of Employees

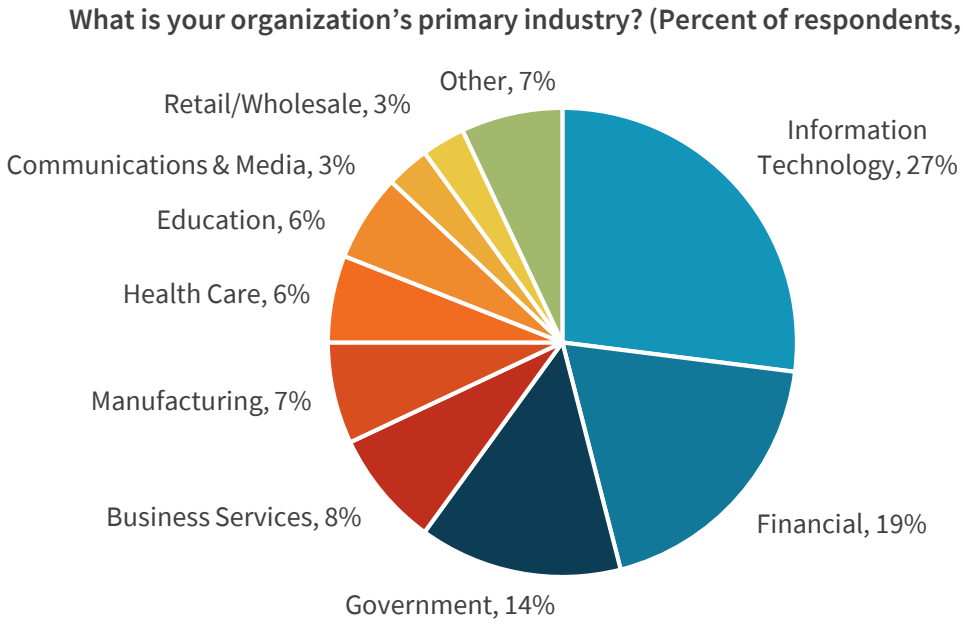


Source: Enterprise Strategy Group

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 43.

Figure 43. 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