ESG RESEARCH REPORT

# The Life and Times of Cybersecurity Professionals 2020

A Cooperative Research Project by ESG and ISSA

By Jon Oltsik, Senior Principal Analyst and Fellow

July 2020

## Contents

## List of Figures

## Executive Summary

### Report Conclusions

In late 2019 and early 2020, the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA) conducted the fourth annual research project focused on the lives and experiences of cybersecurity professionals. This year's report is based on data from a survey of 327 cybersecurity professionals and ISSA members. Ninety-two percent of survey respondents resided in North America, 4% came from Europe, 3% from Asia, and 1% from Central/South America (note: total exceeds 100% due to rounding).

#### The Cybersecurity Profession in Crisis: After 10 Years, Why Has Nothing Changed?

As this and past reports clearly indicate, organizations and cybersecurity professionals are not looking at the profession strategically. There is a continuous lack of training, career development, and long-term planning. As a result, cybersecurity professionals often muddle through their careers with little direction, jumping from job to job and enhancing their skill sets on the fly rather than in any systematic way. This, combined with the continued cybersecurity skills shortage, has stalled cybersecurity progress.

The data uncovered in this research year over year also demonstrates that there are multiple issues contributing to the problem of "a cybersecurity skills gap," Including that businesses don't understand the role of information security, there is no clear and agreed upon career map within our profession, and cybersecurity professionals are under constant stress of attempting to improve collaboration efforts with IT. Cybersecurity will only exhibit a positive change through a more holistic approach.

What's needed is an approach for continuous cybersecurity education and professional development: starting at the public education level, a comprehensive globally accepted career development plan, and career mapping against multiple business disciplines to weave cybersecurity within the business. These efforts are only a partial answer to improvement and change.

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

- The cybersecurity skills shortage is getting worse. This year, 70% of ISSA members believe their organization has been impacted by the global cybersecurity skills shortage. ESG/ISSA added a question to this year's survey to answer this question. The results are distressing—45% believe the cybersecurity skills shortage (and its impact) have gotten worse over the past few years, while 48% say it's about the same today as it was over the past few years. Only 7% believe things have gotten better. The top ramifications of the skills shortage include an increasing workload, unfilled open job requisitions, and an inability to learn or use cybersecurity technologies to their full potential. No single action (funding, college programs, retraining, etc.) is working to bridge the cybersecurity skills gap. What's needed is a holistic approach of continuous cybersecurity education (starting with public education), comprehensive career development, and career mapping/planning—all with support from and integration with the business.

- Cybersecurity professionals continue to need some career guidance. In this year's survey, 63% of respondents have worked in cybersecurity for less than 3 years, with 76% starting as IT professionals before switching their career to cybersecurity. As in the past, however, 68% of the cybersecurity professionals surveyed don't have a well-defined career path and historical solutions are only compounding problems, confusing security professionals while lacking any real guidance. For those interested in a cybersecurity career, ISSA members recommend they find a mentor, get basic cybersecurity certifications, find cybersecurity internships, and join a professional organization.

- Almost half of cybersecurity professionals want to become CISOs. In this year's survey, 16% of respondents were CSOs, CISOs, or in a similar cybersecurity position. Of the remaining participants, 47% admit that they'd like to become a CISO in the future. To achieve this position, ISSA members say they need to develop their leadership, business, and communications skills. This points to the fact that, while career options remain murky, business education should be part of any and all cybersecurity career development plans.

- Cybersecurity careers depend upon hands-on experience. This year, ESG/ISSA asked survey participants to choose which was most important for their career development: hands-on experience or security certifications. The results weren't close—52% chose hands-on experience. Still, 44% claim that hands-on experience and certifications are equally important. Clearly, hands-on experience is critical, but it should be supplemented with the right certifications at the right times. The point here is that certifications MUST be supplemented with practical knowledge about how to derive, implement, and operate technical requirements for policy enforcement.

- Cybersecurity job satisfaction goes beyond compensation. Aside from compensation, cybersecurity job satisfaction is a function of many factors such as support and encouragement for continuing cybersecurity education, business management's commitment to strong cybersecurity, and the ability to work with a highly skilled and talented cybersecurity staff. Organizations with all these qualities will have a distinct advantage in recruiting and hiring as they add to their cybersecurity staff.

- Cybersecurity careers can lead to personal issues. The pace and stress of a cybersecurity job can lead to personal consequences—29% of respondents say that they've either experienced significant personal issues as a result of cybersecurity job stress or they know someone else who has. This percentage may be even higher, as 17% either don't know or prefer not to say.

- Cybersecurity training remains inadequate. In 2020, most survey respondents don't believe their organization provides the right level of cybersecurity training. In this year's survey, 36% of respondents reported that they thought that their organizations should provide a bit more cybersecurity training, while 29% believe their organizations should provide significantly more training. Based on 4 years of research, training seems to be a perpetual shortcoming. Cybersecurity professionals should make business managers aware of this problem and understand the ramifications. This is likely the first step toward a cooperative solution.

- It takes years to become a proficient cybersecurity professional. In a new question for 2020, ESG/ISSA asked survey respondents to speculate on how long it takes a cybersecurity professional to become proficient at their job. The highest percentage of respondents (39%) believe it takes anywhere from 3 to 5 years to develop real cybersecurity proficiency, while 22% say 2 to 3 years, and 18% claim it takes more than 5 years. This speaks to the time necessary to understand the use of technology, factor in security models and principles, and then apply this knowledge toward supporting business goals.

- CISOs are business, not technical, leaders. When asked to identify the most important qualities of a successful CISO, two characteristics stood out above all else: communications skills and leadership skills. Lagging these "must have" skills, 38% of respondents chose management skills, while 36% say business skills. Technical skills were last on the list. The complexity of knowledge necessary for success is a perfect blend of technical knowledge, business acumen, security strategy, and educational ability.

- CISO effectiveness is a mixed bag. For the first time, ESG/ISSA asked survey respondents to provide feedback on their CISO's effectiveness. While 42% rated the CISO as very effective, it's somewhat concerning that a larger percentage (47%) responded somewhat effective, while 12% said not very effective or not at all effective. Overall, there is room for improvement. This may reveal that few CISOs have the blend of business, leadership, communications, and technical skills necessary for success.

- Governments and schools are not keeping up with cybersecurity challenges. In 2020, ESG/ISSA added a new survey question, asking respondents to rate several constituencies in terms of their ability to keep up with cybersecurity challenges. The results are not encouraging, especially regarding government agencies and public schools. Most respondents believe that government agencies should be doing somewhat or a lot more to address cybersecurity challenges, while 84% of respondents believe that public schools/institutions should be doing somewhat or a lot more to address cybersecurity challenges. This data reflects an age-old cybersecurity belief—cybersecurity is most effective when it is baked in, rather than bolted on, to any discipline or culture.

- Cyber-adversaries maintain an advantage over defenders. For the second year in a row, ISSA members were asked to compare the status of cyber-adversaries with that of cyber-defenders. The results are even more alarming than last year, as 67% of respondents believe that cyber-adversaries have a big advantage over cyber-defenders as compared to 59% in the 2018-2019 project.

While we are making some fragmented progress, the same issues present themselves year after year, including a shortage of skills, under-trained employees, and the stress and strain caused by a career in the cybersecurity field. These disturbing trends should be of concern to corporate directors and business executives, not just CISOs.

# 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 other jobs?
  6. Are cybersecurity professionals being actively recruited to change jobs?
  7. Do rank-and-file cybersecurity professionals aspire to become CISOs?
- Skills development
  1. How important is continuous 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 workloads 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?
  4. Are CISOs becoming virtual CISOs? If so, why?

- 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?
4. Is the cybersecurity skills shortage improving?
5. Are organizations doing enough to address this?

- 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?

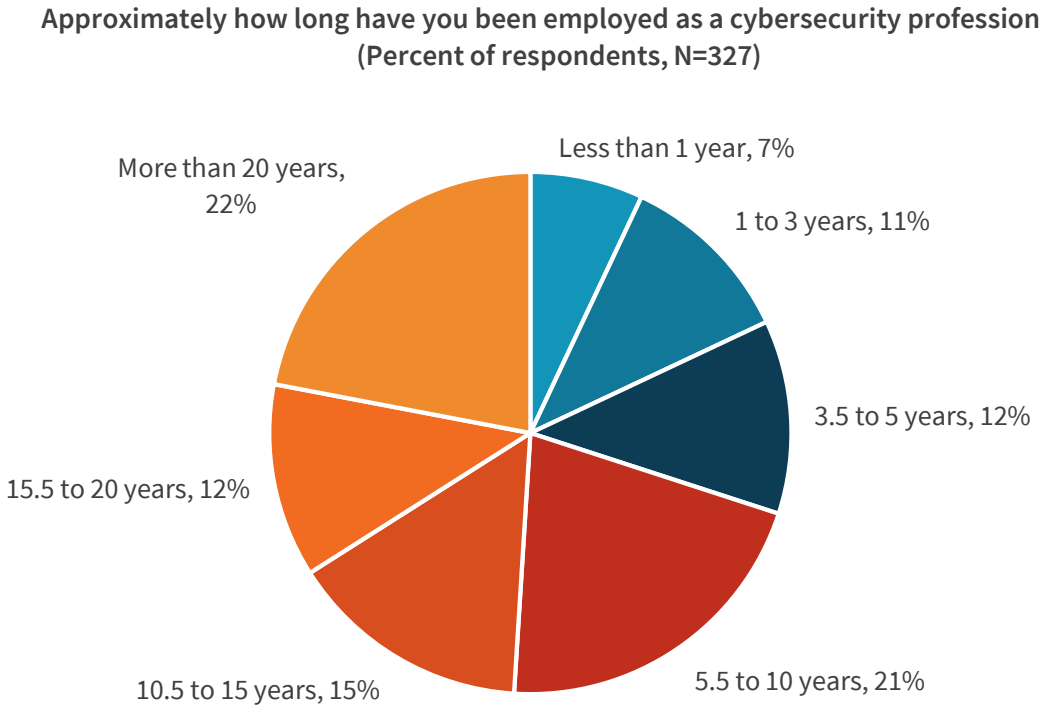
Survey participants represented a wide range of industries including information technology, financial services, government, business services, and manufacturing. For more details, please see the *Research Methodology* and *Respondent Demographics* sections of this report.

## Research Findings

### The ISSA Survey Respondents

The ESG/ISSA research study is based upon a survey of a group of cybersecurity professionals and ISSA members from entry-level to senior positions. In this year's survey, 30% of respondents have less than 5 years of experience, 36% have 5.5 to 15 years of experience, and 34% have more than 15 years of experience in the cybersecurity field (see Figure 1).

**Figure 1. Length of Time Employed as a Cybersecurity Professional**



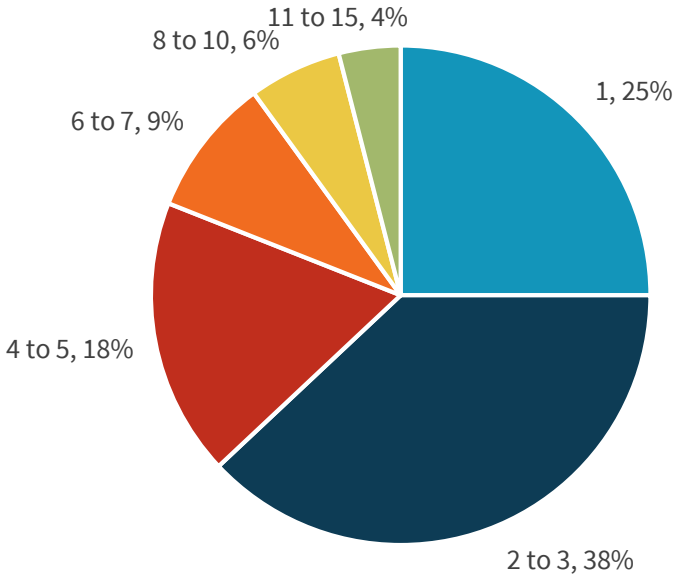

*Source: Enterprise Strategy Group*

Most of the cybersecurity professionals (63%) have had three or fewer cybersecurity jobs throughout their careers (see Figure 2).

ESG/ISSA also asked about respondents' experience in relation to the phases of the ISSA cybersecurity career lifecycle. Twenty percent of respondents consider themselves "senior," while 49% rank themselves as "leaders" (see Figure 3).

## Figure 2. Number of Cybersecurity Jobs

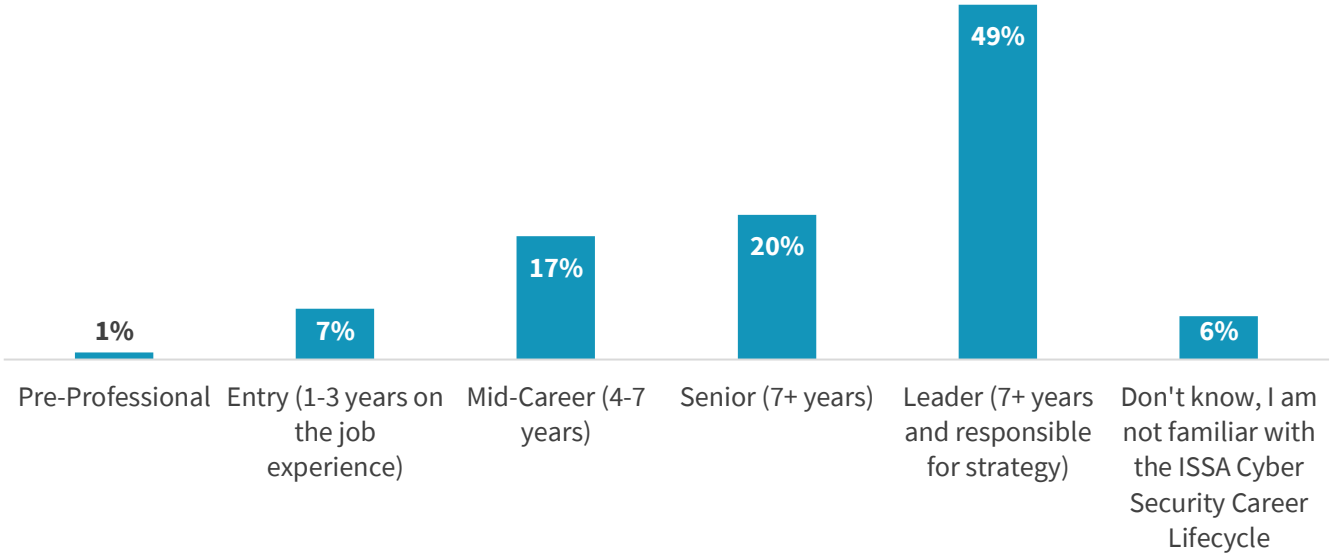
**Approximately how many different organizations have you worked for during the span of your cybersecurity career? (Percent of respondents, N=327)**




*Source: Enterprise Strategy Group*

## Figure 3. Phase of ISSA Cybersecurity Career Lifecycle

**What phase of the ISSA Cyber Security Career Lifecycle™ do you consider yourself? (Percent of respondents, N=293)**

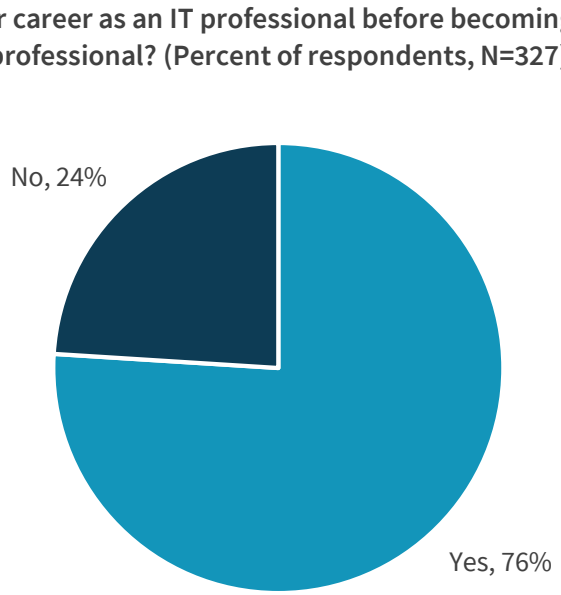



*Source: Enterprise Strategy Group*

## The Cybersecurity Professional

Seventy-six percent of survey respondents started their careers in IT and then moved to cybersecurity (see Figure 4). These results are similar to the results from the last three years of the project (i.e., 2018-2019: 79% came to cybersecurity from IT, 2017: 77% came to cybersecurity from IT, 2016: 78% came to cybersecurity from IT).

**Figure 4. Cybersecurity Professionals Tend to Come from IT**

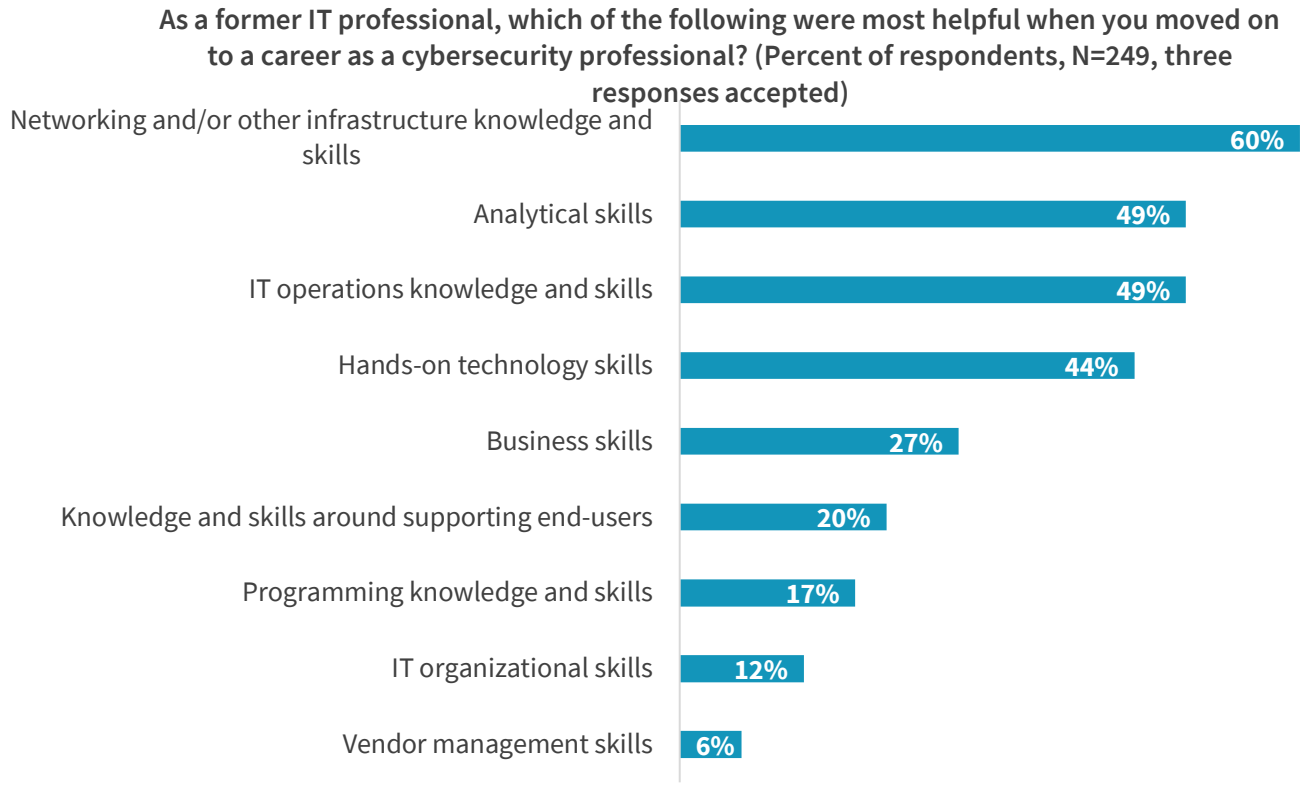



*Source: Enterprise Strategy Group*

Survey respondents were asked to identify the most helpful of these skills when moving into cybersecurity: 60% say networking and other infrastructure experience, 49% say analytical skills, and 49% point to IT operations knowledge and skills (see Figure 5). These results have been consistent over the past three years as well.

Once again, ESG and ISSA asked survey respondents why they became cybersecurity professionals. The top answers have been consistent for four years running (see Figure 6).

## Figure 5. IT Skills Most Helpful for a Cybersecurity Career




*Source: Enterprise Strategy Group*

## Figure 6. Reasons for Becoming a Cybersecurity Professional


*Source: Enterprise Strategy Group*

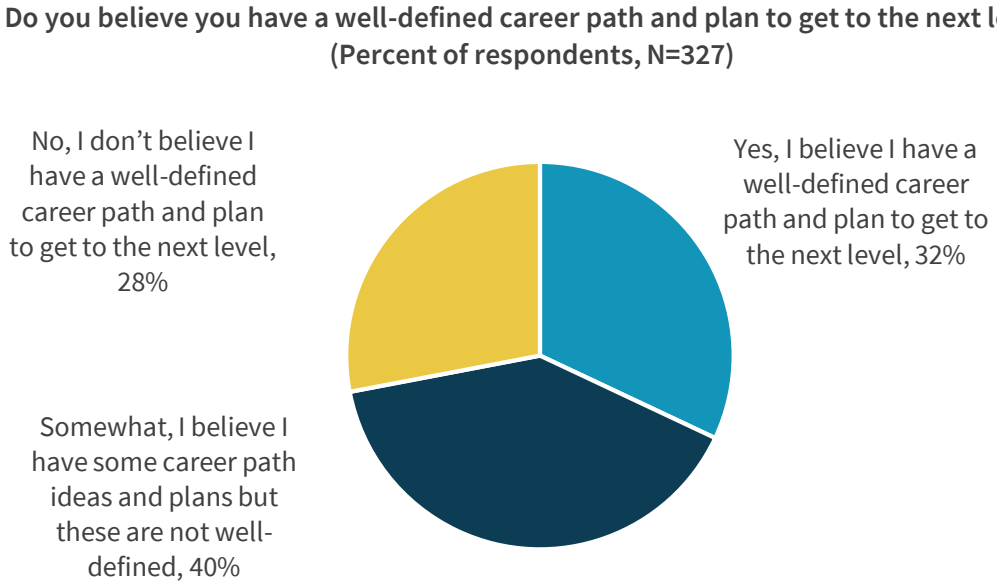
In 2020, ESG/ISSA added a new survey question, asking survey respondents for their recommendations for those seeking to enter the cybersecurity field. More than one-quarter (26%) of respondents suggested finding a mentor, 20% proposed getting a basic cybersecurity certification, and 16% recommended a cybersecurity internship (see Figure 7).

**Figure 7. Advice for Individuals Who Want to Get into Cybersecurity**


*Source: Enterprise Strategy Group*

When it comes to career planning, cybersecurity professionals don't seem to be very proactive. Less than one-third (32%) have a well-defined career path, but more than two-thirds (68%) have some career path ideas or don't believe they have a well-defined career path at all (see Figure 8). Organizations must be more proactive, helping cybersecurity professionals better navigate their career choices and paths.

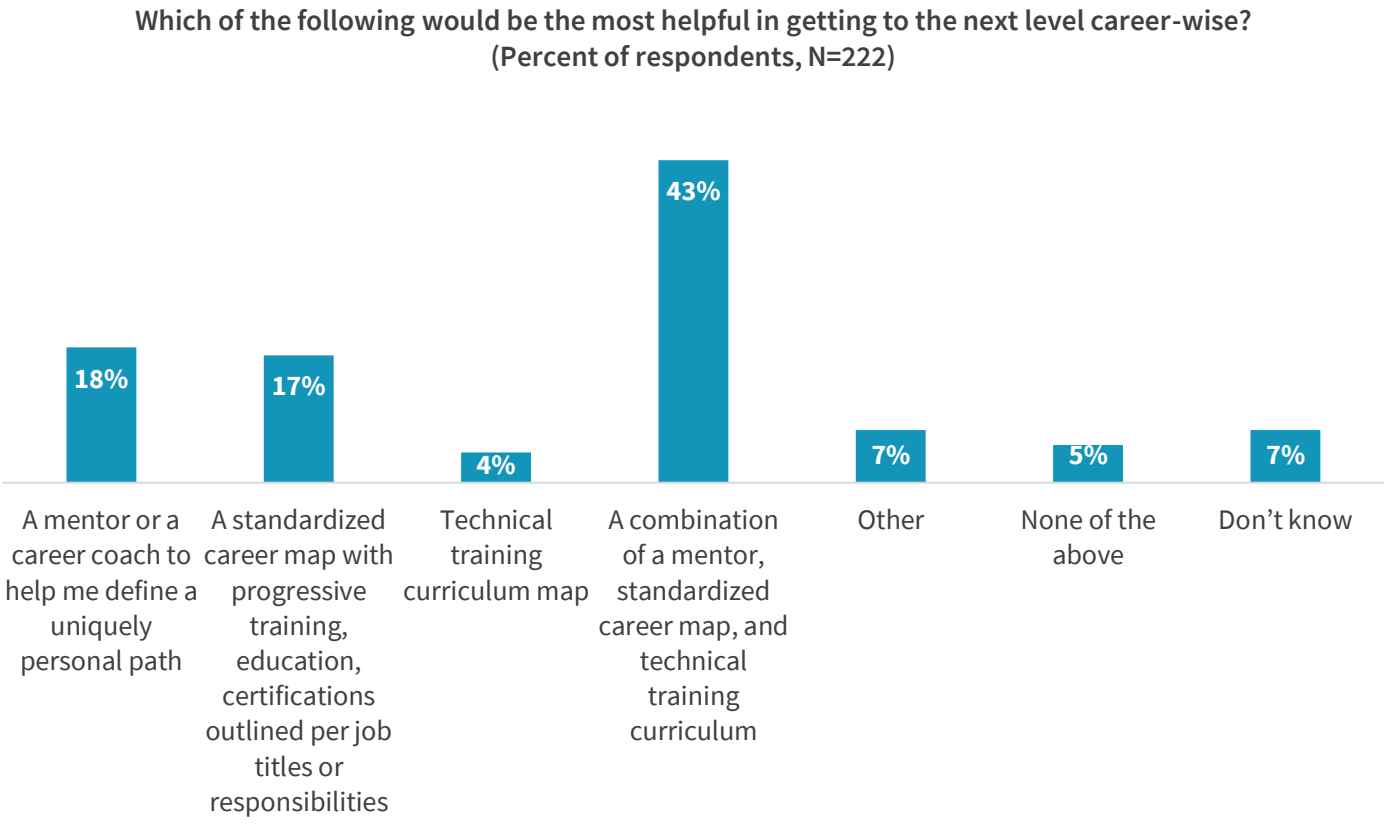
## Figure 8. Do Respondents Believe They Have a Well-defined Career Path?




*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 9). Note that the results were consistent in all four years.

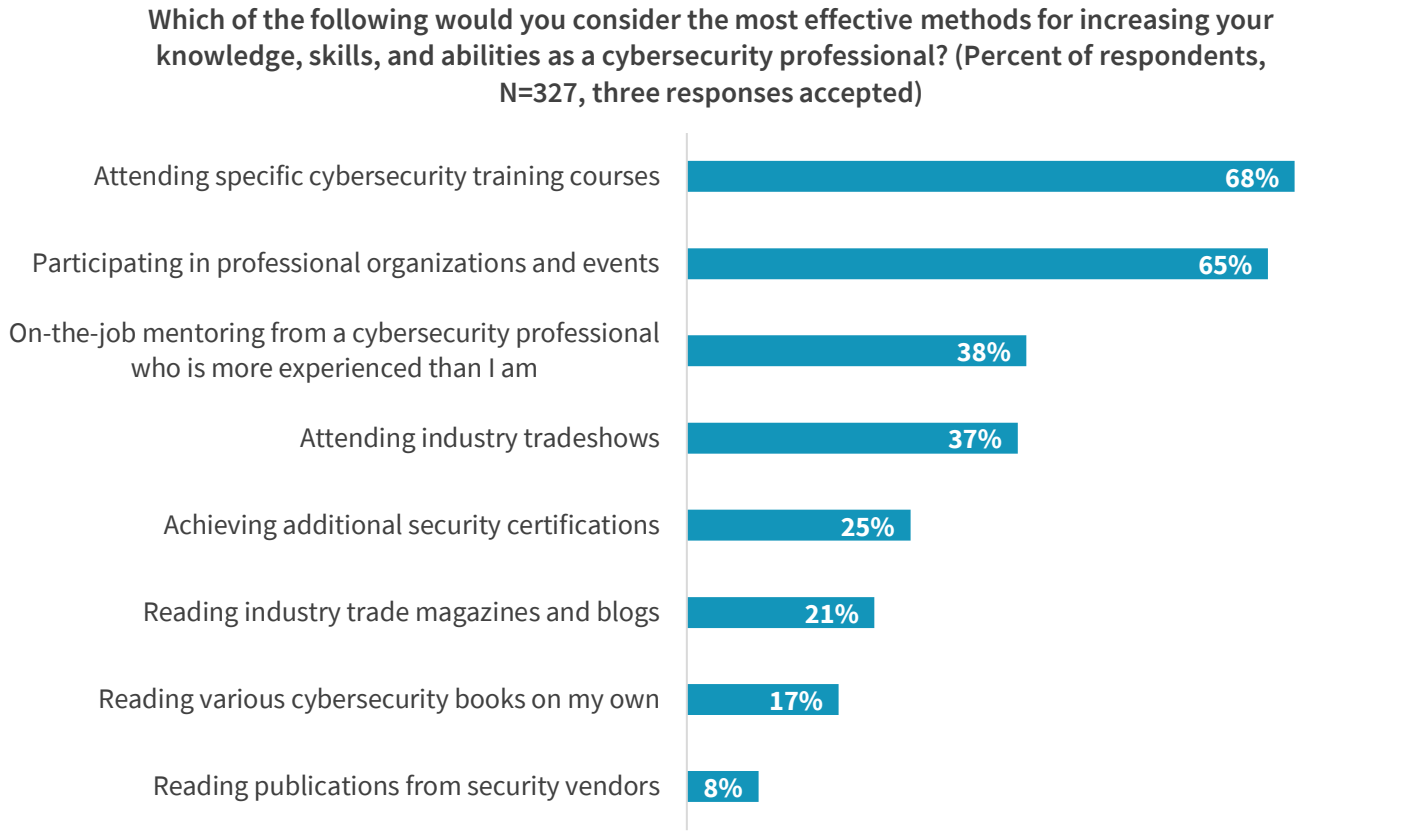
## Figure 9. Most Helpful Factors in Progressing a Cybersecurity Career




*Source: Enterprise Strategy Group*

Respondents were then asked their opinions on the most effective methods for increasing their cybersecurity knowledge, skills, and abilities (KSAs). Among the top activities for increasing KSAs, more than two-thirds (68%) attended specific cybersecurity training courses, and another 65% cited participation in professional organizations (see Figure 10). These top two responses have been consistent for all four years.

**Figure 10. Most Effective Methods for Increasing KSAs**




*Source: Enterprise Strategy Group*

## Career Aspirations

The CISO position is a difficult one, requiring a diverse combination of business, managerial, and technical skills. Do cybersecurity professionals strive to achieve this position, or would they rather remain as part of the cybersecurity team rank-and-file?

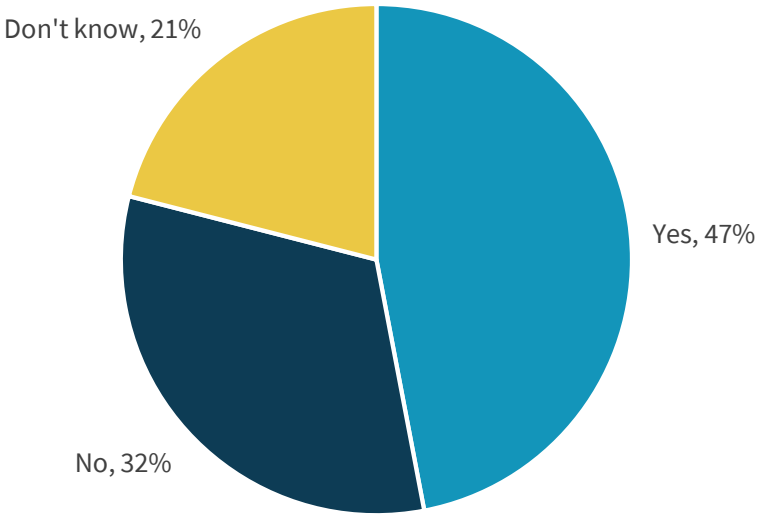
ESG/ISSA explored this area for the first time in this year's survey. Just under half (47%) of respondents have the CISO position as a career goal while 53% are either opposed to an eventual CISO position or don't know (see Figure 11).

ISSA members interested in becoming a CISO were then asked which skills they need to develop to achieve this position. The data is skewed toward non-technical areas like leadership skills, business skills, and communication skills (see Figure 12).

Current CISOs (along with business executives) can help here by identifying strong internal candidates, creating mentoring programs, building career maps, and providing resources for continuous education. These investments will not only benefit individual organizations but also the cybersecurity community at large.

## Figure 11. Aspiration to Become a CISO

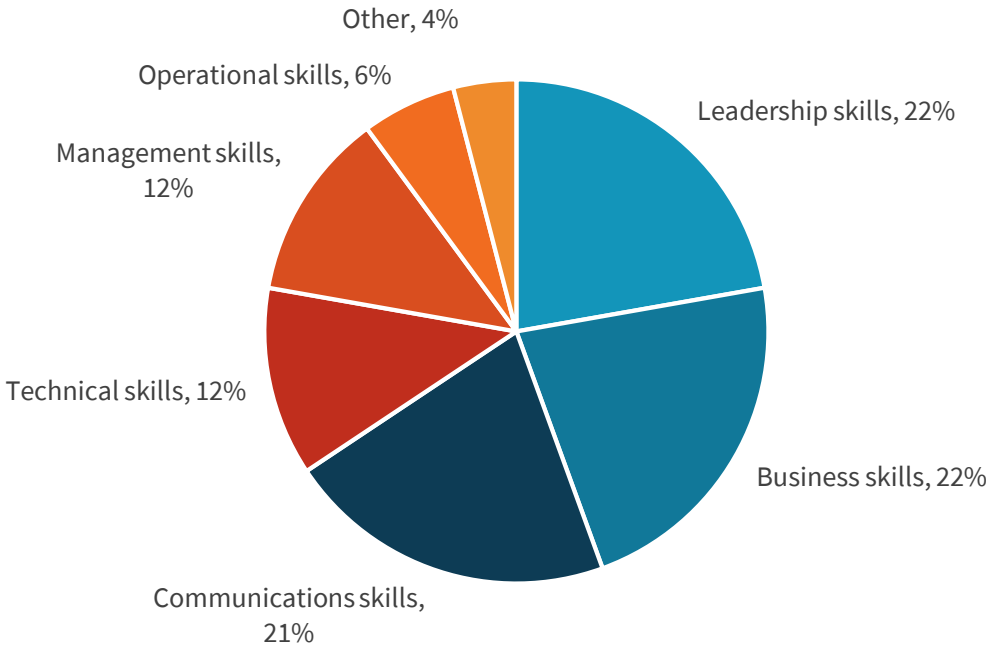
**Do you want to eventually become a CSO/CISO? (Percent of respondents, N=276)**




*Source: Enterprise Strategy Group*

## Figure 12. Skills Development Needed to Become a CISO

**Which skill do you think you'll have to develop most to take on a CSO/CISO role? (Percent of respondents, N=130)**



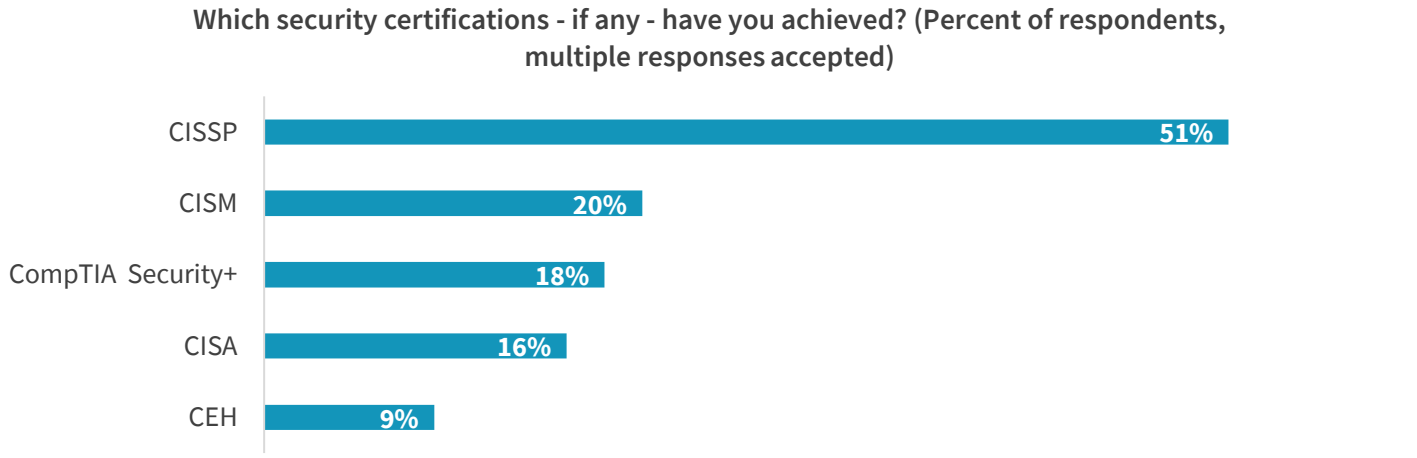

*Source: Enterprise Strategy Group*

## Cybersecurity Certifications

Which certifications have ISSA members achieved? As in years past, survey respondents were asked to write in the answer to this question and the top responses are listed in the figure below (see Figure 13). Of those certifications achieved, the most useful ones for getting a job are graphed in Figure 14 and compared to the results from the past two years. In both graphics, CISSP stands out—it's the most popular certification and the one that's most important for getting a cybersecurity job. Other certifications should be viewed as vehicles for career advancement (in some cases) or to help cybersecurity professionals gain general knowledge in a cybersecurity sub-discipline (for example, certified ethical hacker).

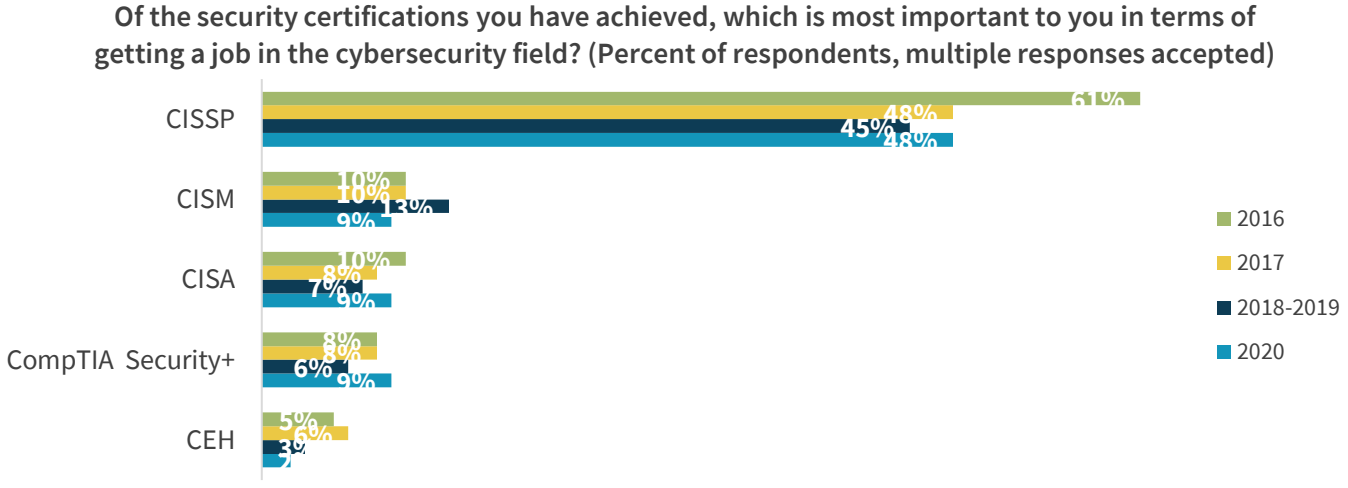
Cybersecurity professionals pursue a CISSP certification after accruing the requisite number of years of experience, as this certification is a requirement for most available jobs. Beyond the CISSP, however, ISSA members take a more tactical approach to additional certifications based upon their skills, interests, and career plans. ESG/ISSA believe this is the right approach for certifications and career development. Rather than fill their resumes with acronyms, cybersecurity professionals should focus on hands-on training, mentoring, and professional networking as primary means for skills development. Rather, certifications should supplement these activities.

### Figure 13. Cybersecurity Certifications Achieved




*Source: Enterprise Strategy Group*

### Figure 14. Most Important Certification Necessary to Get a Job




*Source: Enterprise Strategy Group*

ESG and ISSA have long held the belief that hands-on experience is the most important factor in cybersecurity career development, but this assumption was based on anecdotal data. In the 2020 research project, ESG/ISSA tested this hypothesis by including a question on this topic in this year's survey.

The data supports this long-held belief. Only 2% of respondents believe security certifications are more important than hands-on experience. Alternatively, 52% believe that hands-on experience is more important than certifications while 44% place equal value on hands-on experience and certification achievement (see Figure 15).

Based upon this data, aspiring and growing cybersecurity professionals should take a balanced approach to skills development. Hands-on experience should be supplemented with the appropriate security certifications on an as-needed basis.

**Figure 15. Hands-on Experience versus Cybersecurity Certifications for Skills Development**


*Source: Enterprise Strategy Group*

## Cybersecurity Jobs

What are the most important factors that distinguish a satisfactory and unsatisfactory cybersecurity job? This question about what determines cybersecurity job satisfaction has been a constant in the ESG/ISSA research study for 4 years. Interestingly, the results have also been consistent. The top three priorities in 2020, as well as past years, are 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 16). Organizations looking to hire cybersecurity FTEs should be sure to emphasize these 3 attributes as part of their recruitment efforts.

## Figure 16. Factors Determining Job Satisfaction

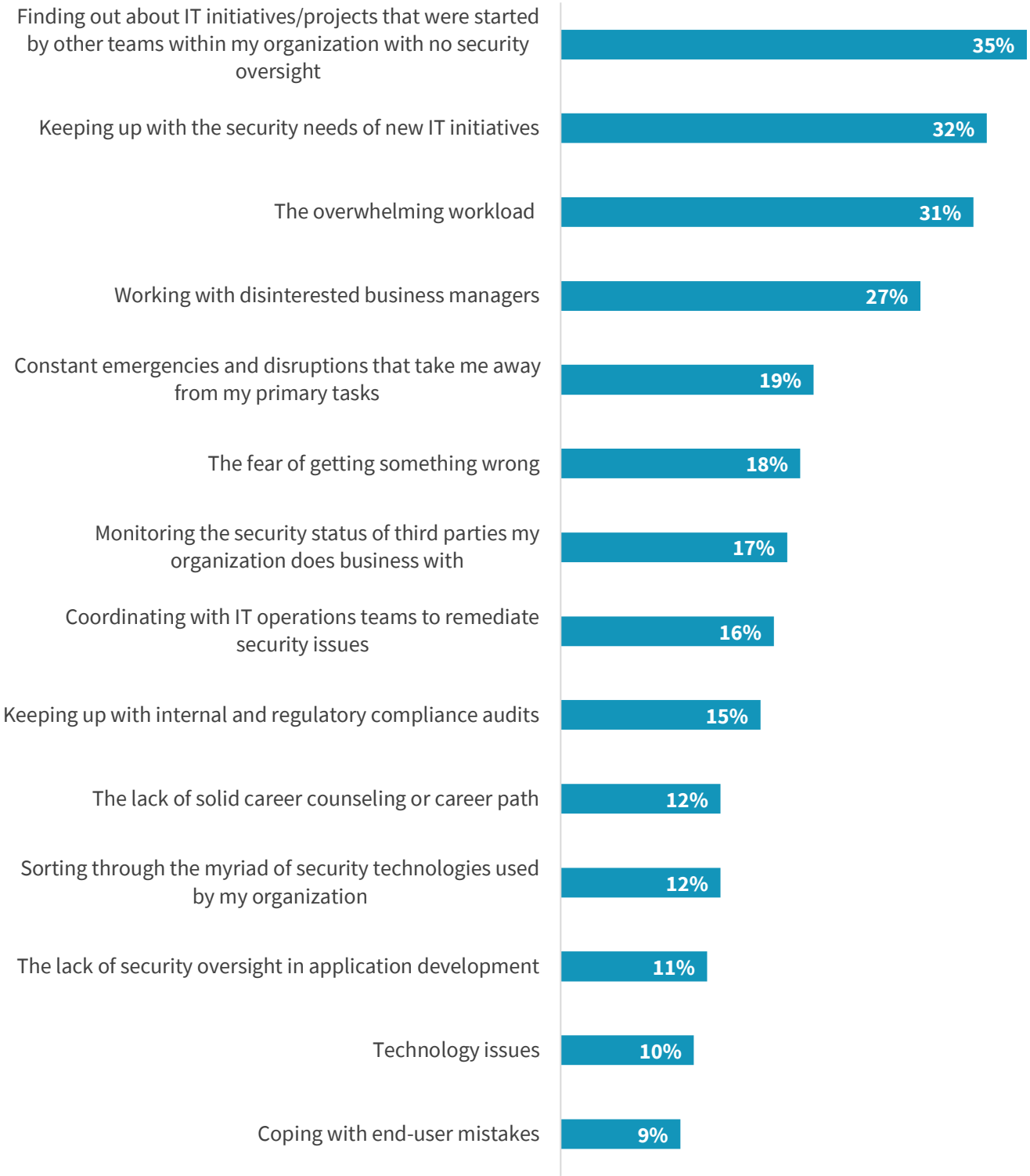
**Which of the following are the biggest factors determining job satisfaction for you? (Percent of respondents, N=327, three responses accepted)**


*Source: Enterprise Strategy Group*

What are the most stressful aspects of a cybersecurity job? Thirty-five percent of ISSA members claim it is finding out about IT/initiatives/projects that were started by other teams (within the organization) with no security oversight (see Figure 17). This makes sense. Security professionals want to be engaged in projects from the start so they can "bake in" rather than "bolt on" security. Similarly, nearly one-third (32%) of respondents believe it is stressful keeping up with the security needs of new IT initiatives while 31% point to the overwhelming workload. It is also noteworthy that 27% of security professionals believe it is stressful working with disinterested business managers. This situation often leads to high rates of cybersecurity employee attrition.

## Figure 17. Most Stressful Aspects of Cybersecurity Jobs

**What are the most stressful aspects of your job as a cybersecurity professional? (Percent of respondents, N=327, three responses accepted)**

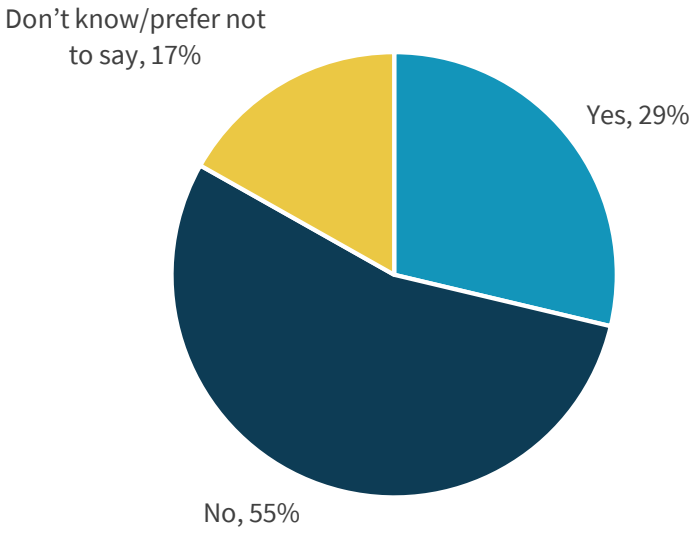



*Source: Enterprise Strategy Group*

The pace and pressure of a cybersecurity job can be difficult at times. Indeed, cybersecurity professionals sometimes struggle with issues like depression, alcoholism, and drug addiction, in reaction to cybersecurity job stress. ESG/ISSA asked a question about this topic in this year's research survey. Alarmingly, 29% of respondents say that they've either experienced significant personal issues as a result of cybersecurity job stress or they know someone else who has (see Figure 18). This percentage may be even higher, as 17% either don't know or prefer not to say. CISOs must team with HR managers to monitor and address this mental health issue on a proactive and ongoing basis.

**Figure 18. Cybersecurity Job Stress Can Lead to Significant Personal Issues**

**Have you or any other cybersecurity professionals you've worked with experienced any significant personal issues as a result of stress associated with the cybersecurity profession? (Percent of respondents, N=327)**



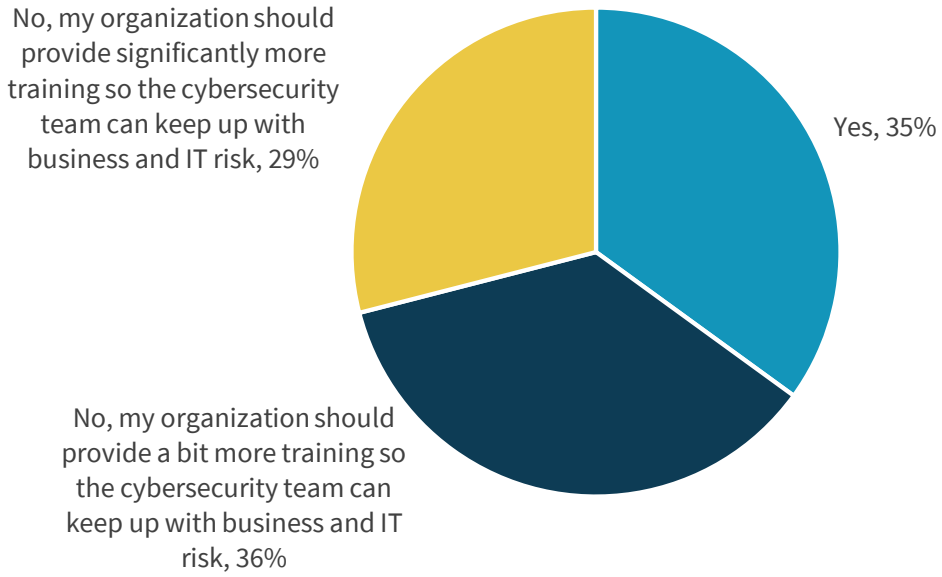

*Source: Enterprise Strategy Group*

The ESG/ISSA research has exposed an alarming trend for four years running—organizations are not providing enough cybersecurity training to help them keep up with business and IT risk. In 2020, most survey respondents don't believe their organization provides the right level of cybersecurity training. In this year's survey, 36% of respondents reported that they thought that their organizations should provide a bit more cybersecurity training, while 29% believe their organizations should provide significantly more training (see Figure 19).

In a new question for 2020, ESG/ISSA asked survey respondents to speculate on how long it takes a cybersecurity professional to become proficient at their job. The highest percentage of respondents (39%) believe it takes anywhere from 3 to 5 years to develop real cybersecurity proficiency, while 22% say 2 to 3 years and 18% claim it takes more than 5 years (see Figure 20). Three to five years is a long time. CISOs should do everything they can to accelerate staff skills development. This can be accomplished by following the advice described by survey respondents (as seen previously in Figure 7, Figure 9, and Figure 10).

## Figure 19. Training Provided to Keep Up with Business and IT Risk

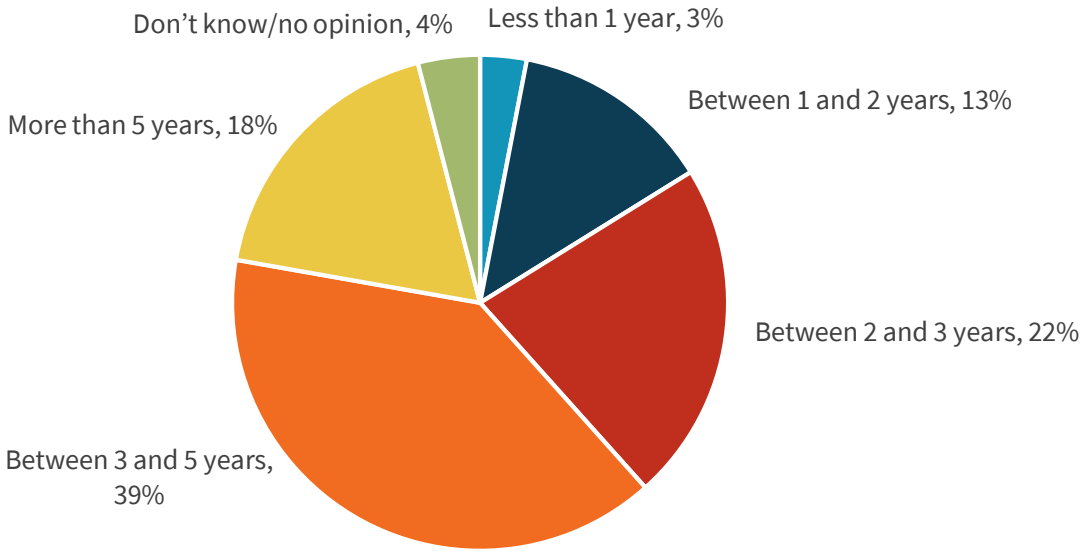
**In your opinion, does your current employer provide the cybersecurity team with the right level of training in order for them to keep up with business and IT risk? (Percent of respondents, N=327)**




*Source: Enterprise Strategy Group*

## Figure 20. Length of Time Required to Develop Cybersecurity Proficiency

**In your opinion, how long does it take a cybersecurity professional to become proficient (i.e., knowledgeable, productive, etc.)? (Percent of respondents, N=327)**

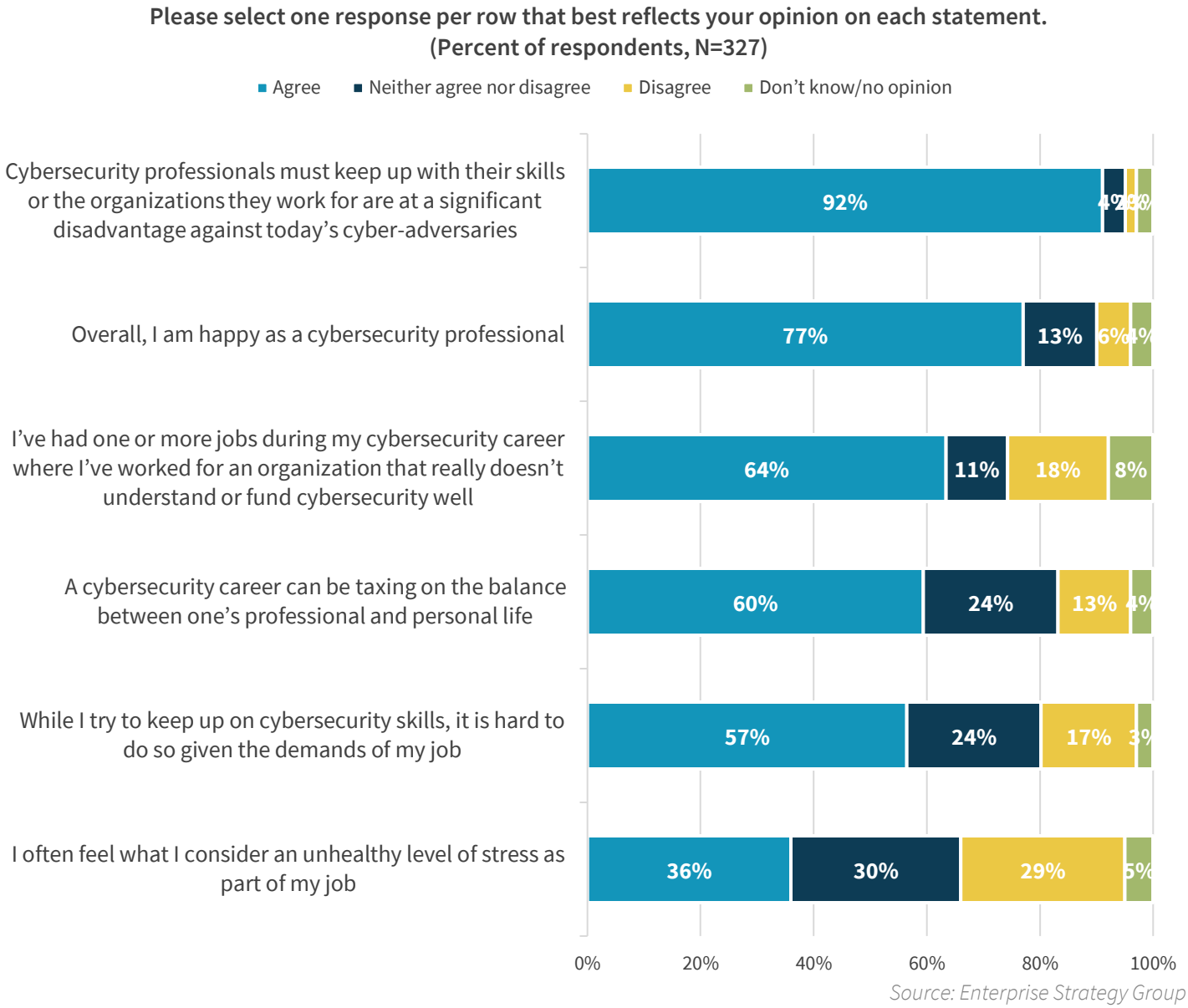



*Source: Enterprise Strategy Group*

Survey respondents were presented with many statements and asked whether they agreed or disagreed with each (see Figure 21). The good news is that 77% of respondents say that they are happy as a cybersecurity professional. Unfortunately, the rest of the data is fraught with problems. For example:

- While 92% of respondents believe that cybersecurity professionals must keep up with their skills or the organizations they work for are at a significant disadvantage against today's cyber-adversaries, 57% agree with the statement, "While I try to keep up on cybersecurity skills, it is hard to do so given the demands of my job." This, combined with the previous data point, indicate an alarming trend—many cybersecurity professionals don't receive the right level of training from their employers and are simply too busy to seek out training on their own.
- Sixty percent of respondents claim that a cybersecurity job can be taxing on the balance between one's professional and personal life. This and the unhealthy levels of stress of a cybersecurity job (36%) may be a leading cause of the significant personal issues described above.

## Figure 21. Respondents' Opinions on Cybersecurity Topics

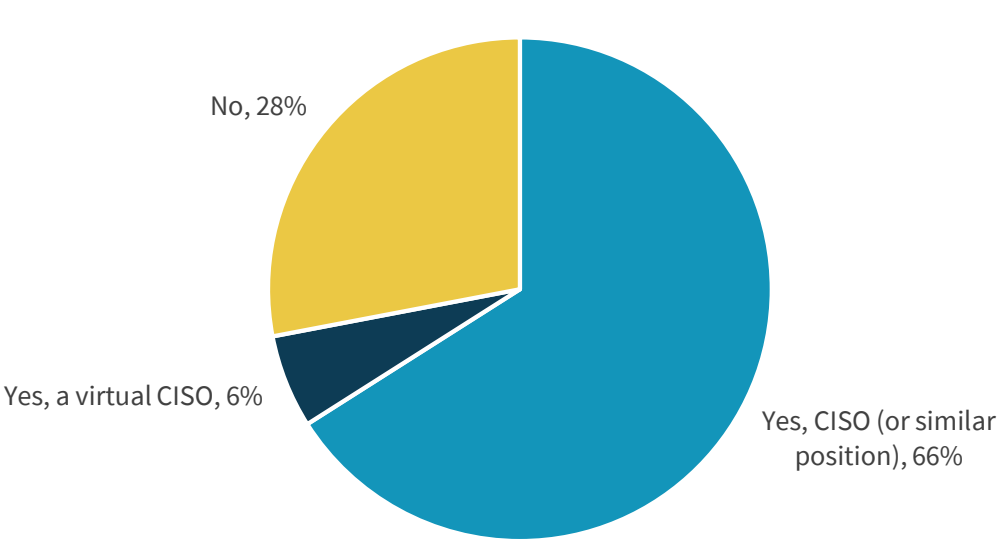



*Source: Enterprise Strategy Group*

## Cybersecurity Leadership

Once again, the majority of respondents work at an organization employing a CISO (66%) while 6% work at an organization with a virtual CISO (see Figure 22).

**Figure 22. Does Organization Have a CSO/CISO?**

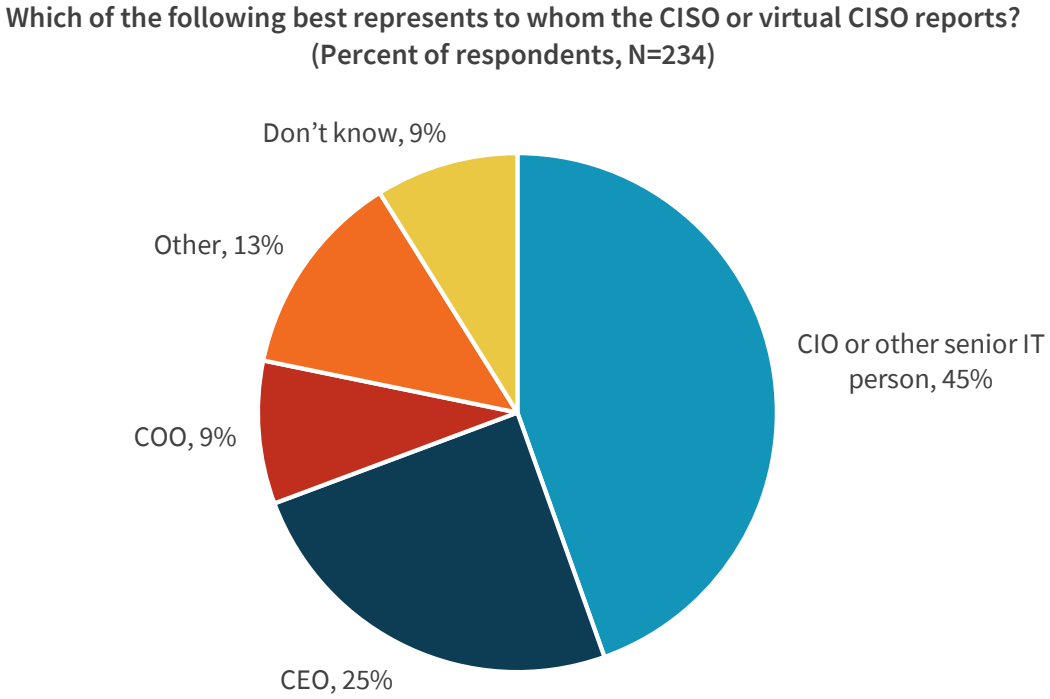



*Source: Enterprise Strategy Group*

Reporting structures for CISOs have remained consistent throughout the 4 years of the ESG/ISSA research projects. Just under half (45%) of CISOs report into IT as compared with 48% last year. In both 2020 and 2019, 25% of CISOs reported directly to CEOs (see Figure 23).

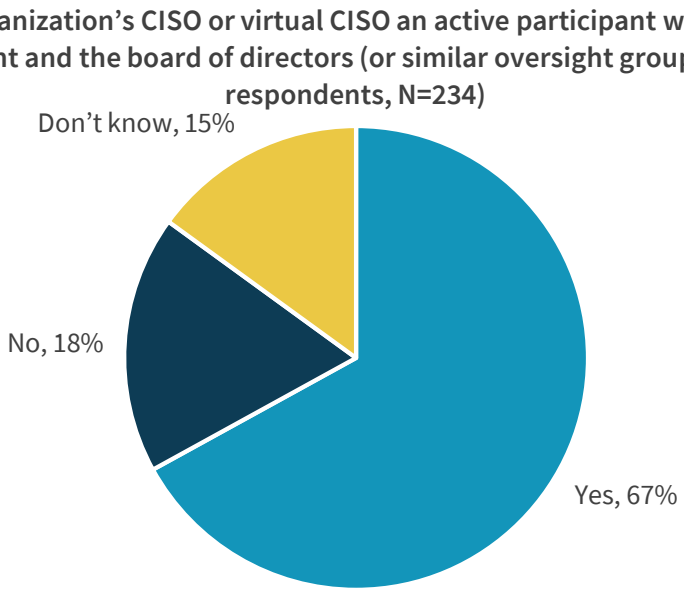
Survey respondents were then asked if the organization's CISO is an active participant with executives and boards. There's a bit of a positive trend over the last few years. In 2020. 67% said "yes," up from 64% in 2019 and 59% in 2018. This incremental progress illustrates that cybersecurity is an increasingly important boardroom-level issue (see Figure 24).

Figure 23. To Whom Does the CSO/CISO Report?




*Source: Enterprise Strategy Group*

Figure 24. Level of CISO Participation with Business Management

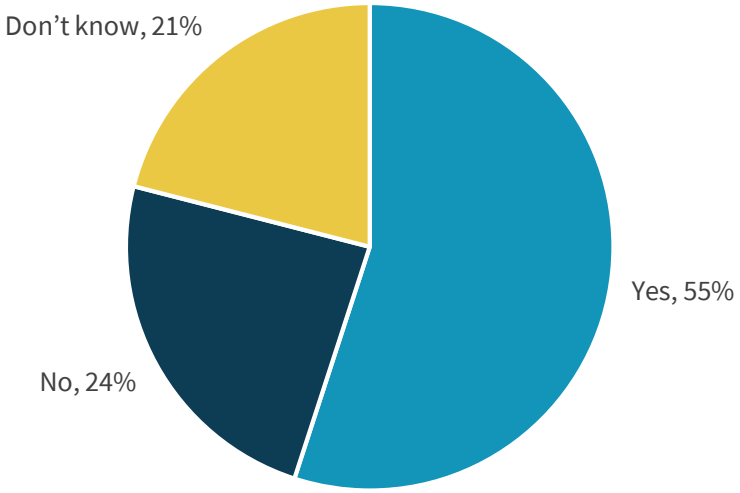



*Source: Enterprise Strategy Group*

Fifty-five percent of respondents believe there is adequate CISO participation with executives and corporate boards in 2020 (see Figure 25). Once again, this is trending upward slightly, as just under half (49%) of respondents believed CISOs' participation was at the right level in 2019. Still, 24% think that CISOs and business executives could do more together.

## Figure 25. 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=234)**

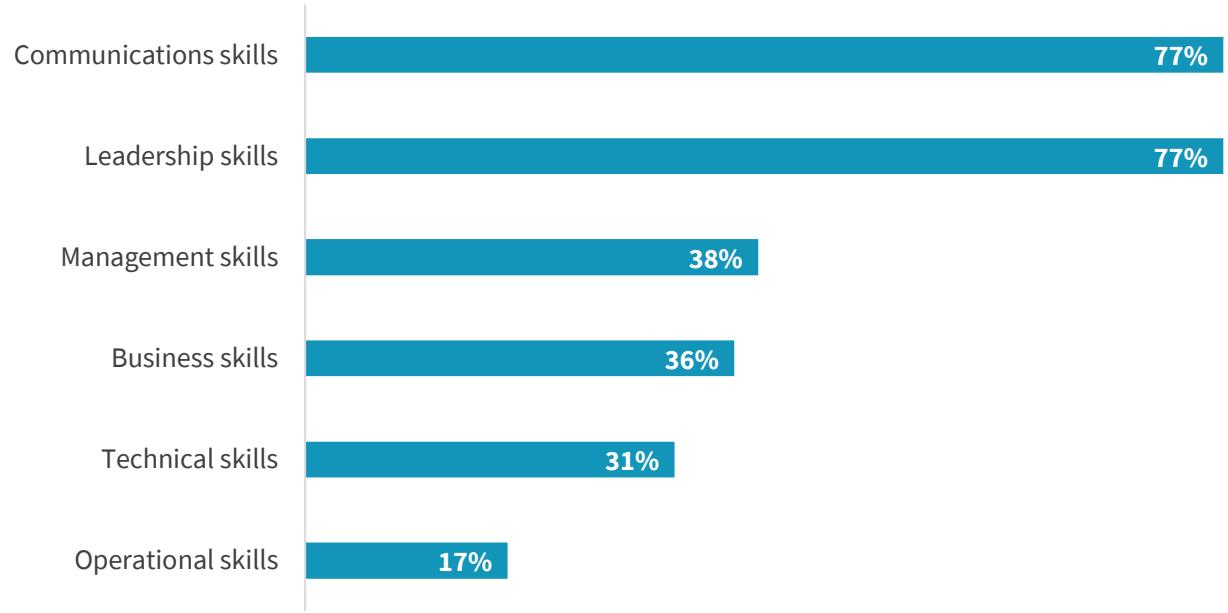



*Source: Enterprise Strategy Group*

When asked to identify the most important qualities of a successful CISO, two characteristics stood out above all else: communications skills and leadership skills (see Figure 26). This list clearly exemplifies the current state of the CISO position as it is dominated by skills necessary for business rather than technical leadership. It also aligns well with the skills development requirements defined by junior cybersecurity professionals with CISO aspirations (see Figure 12).

## Figure 26. Most Important Qualities of a Successful CISO

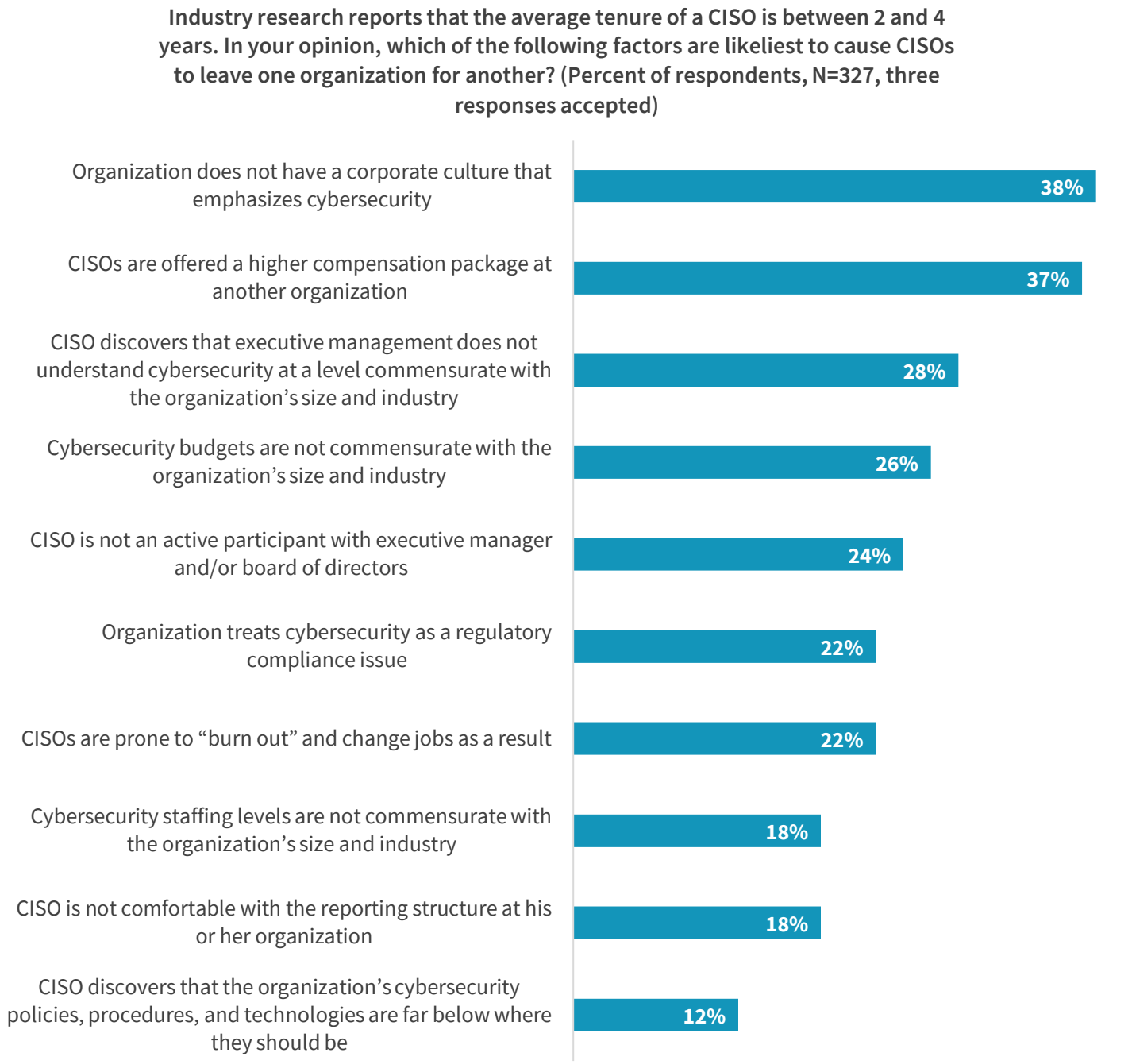
**In your opinion, which of the following are the most important qualities of a successful CISO or virtual CISO? (Percent of respondents, N=327, three responses accepted)**




*Source: Enterprise Strategy Group*

CISO attrition is common, with the average tenure of each job around 24 to 48 months in length. Why do CISOs move on so quickly? Once again, ISSA members believe the main reasons CISOs leave one organizations for another are a corporate culture that doesn't include cybersecurity, higher compensation elsewhere, and an inadequate level of cybersecurity commitment (see Figure 27). These results are consistent with past years.

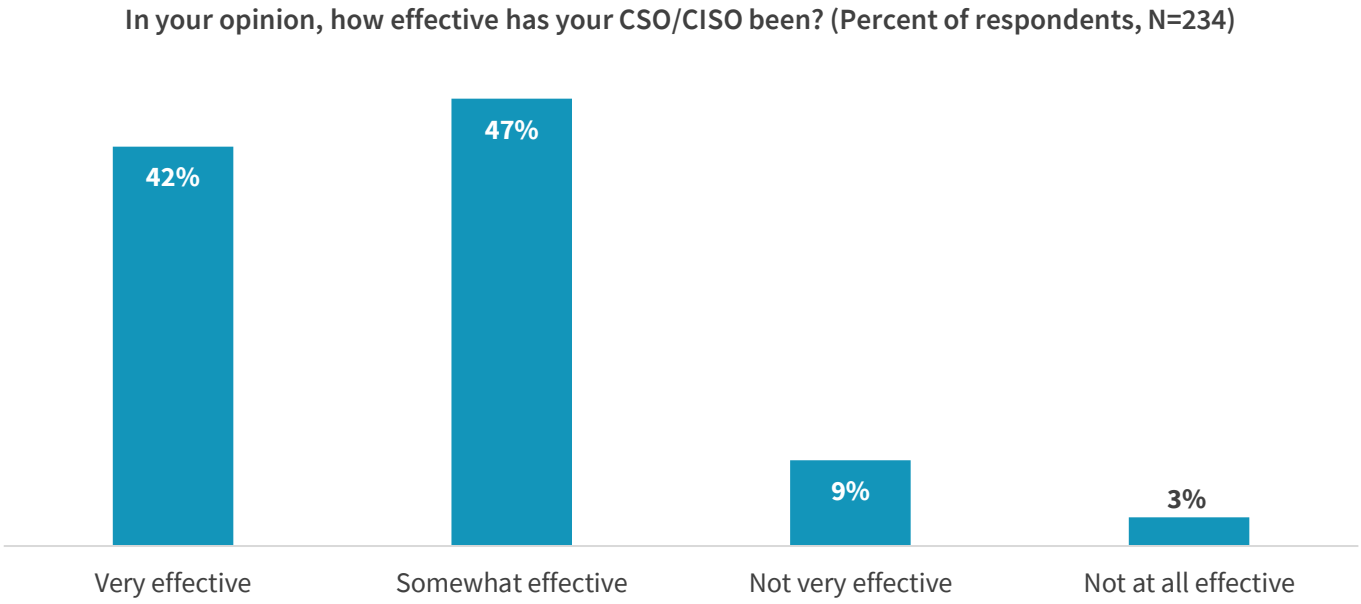
**Figure 27. Most Likely Factors to Cause a CISO to Leave an Organization**




*Source: Enterprise Strategy Group*

For the first time, ESG/ISSA asked survey respondents to provide feedback on their CISOs' effectiveness. While 42% rated the CISO as very effective, it's somewhat concerning that a larger percentage (47%) responded somewhat effective, while 12% said not very effective or not at all effective (see Figure 28). Overall, there is room for improvement.

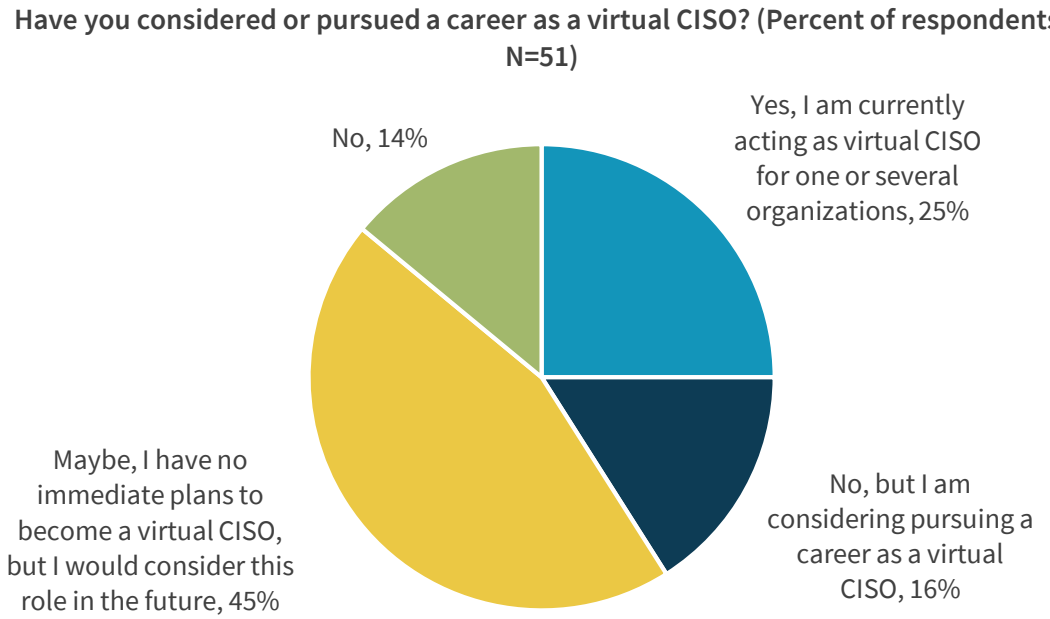
## Figure 28. Rating CISO Effectiveness




*Source: Enterprise Strategy Group*

For the second year running, ESG/ISSA asked CISO respondents whether they've considered or pursued a virtual CISO (vCISO) position. The data is consistent in 2019 and 2020, as 25% are currently acting as a virtual CISO for one or more organizations (compared to 29% last year). In 2020, 16% are considering pursuing a virtual CISO career path, and 45% are open to becoming a virtual CISO sometime in the future (see Figure 29). These percentages are somewhat higher than 2019, indicating that the vCISO position is more established, driving more interest in this role.

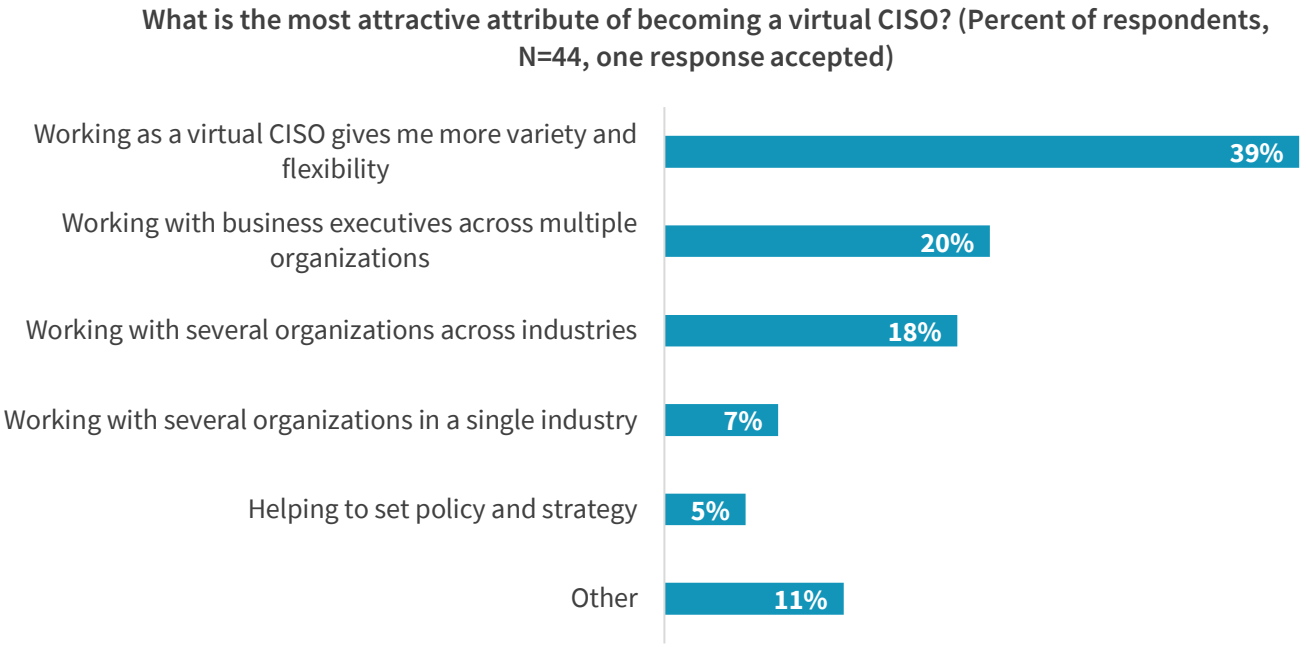
## Figure 29. Consideration of a Virtual CISO Position




*Source: Enterprise Strategy Group*

Why become a virtual CISO? Once again, the top answers included variety/flexibility, working with business executives across multiple organizations, and the opportunity to span across industries (see Figure 30).

**Figure 30. Attractive Attributes of a Virtual CISO Position**

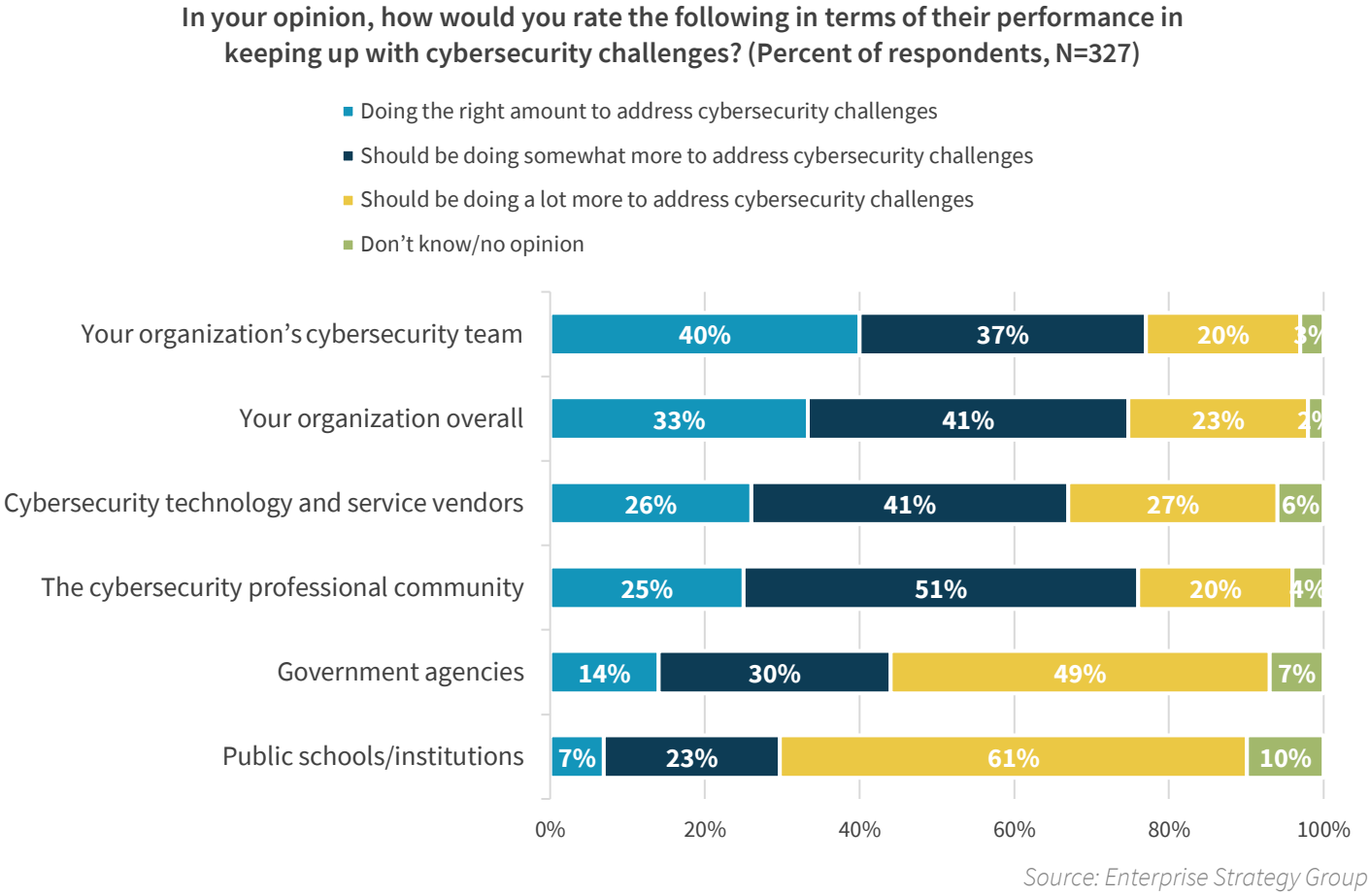



*Source: Enterprise Strategy Group*

In 2020, ESG/ISSA added a new survey question, asking respondents to rate several constituencies in terms of their ability to keep up with cybersecurity challenges. The results are not encouraging. Forty percent of ISSA members say that their organization's cybersecurity team is doing the right amount to address cybersecurity challenges, but 57% believe the cybersecurity team should be doing somewhat or a lot more in these areas (see Figure 31). Additionally:

- 64% of respondents believe their organization should be doing somewhat or a lot more to address cybersecurity challenges. This may indicate a disconnect between business, IT, and security teams, or perhaps a lack of cybersecurity knowledge at the board level.
- 68% of respondents believe that cybersecurity technology and service vendors should be doing somewhat or a lot more to address cybersecurity challenges. This negative rating seems to indicate that the cybersecurity industry must eschew marketing rhetoric and work closer with customers.
- 71% of respondents believe the cybersecurity community at large should be doing somewhat or a lot more to address cybersecurity challenges. This indicates the need for more collaboration and communication.
- 79% of respondents believe that government agencies should be doing somewhat or a lot more to address cybersecurity challenges. In other words, voluntary efforts like the NIST cybersecurity framework (CSF) are not enough.
- 84% of respondents believe that public schools/institutions should be doing somewhat or a lot more to address cybersecurity challenges. This could include cybersecurity awareness training at the elementary school level.

Figure 31. Ratings of Cybersecurity Performance in Keeping Up with Challenges



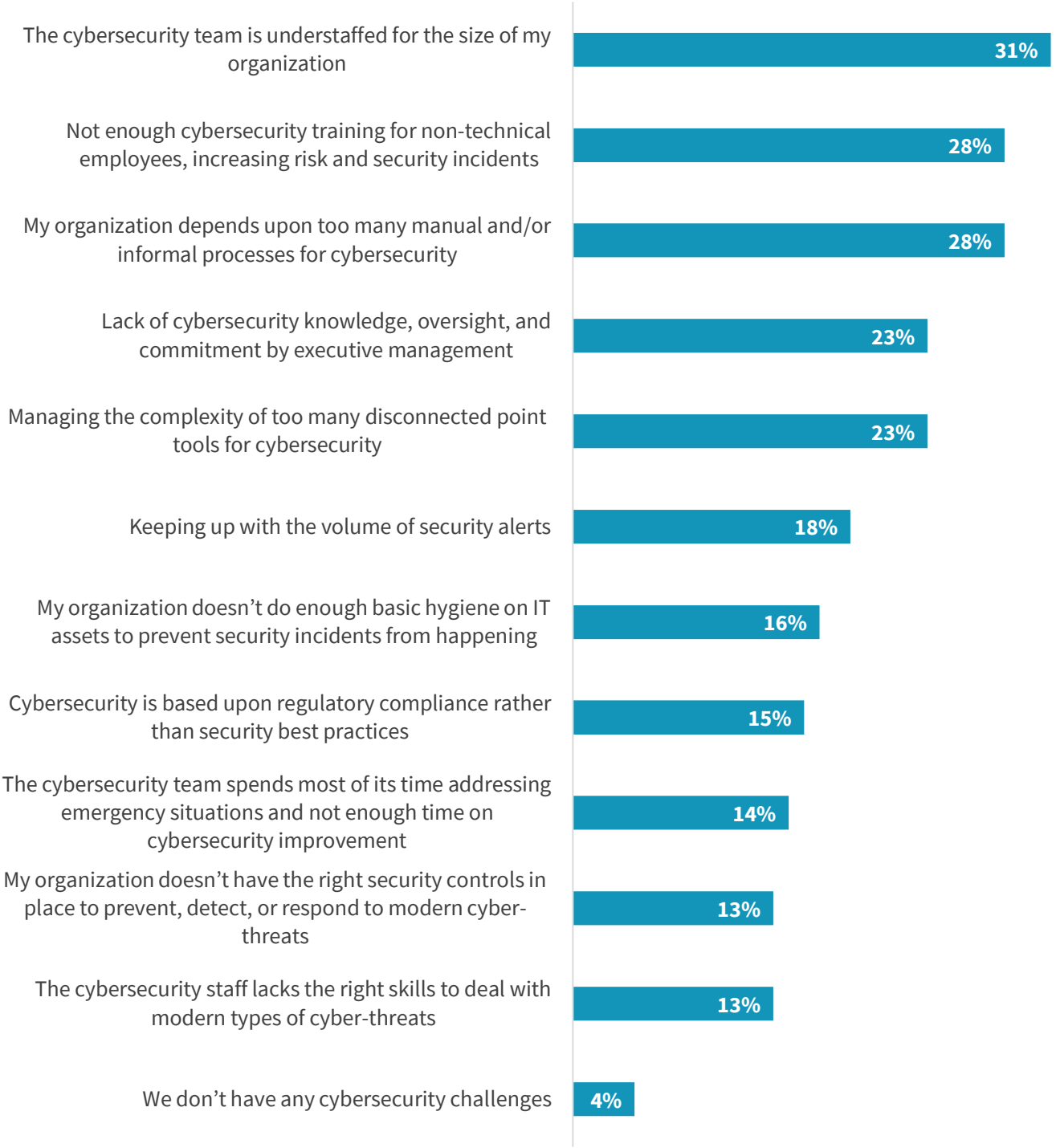

*Source: Enterprise Strategy Group*

As in the past, respondents were asked to identify the top cybersecurity challenges at their organizations (see Figure 32). Similar to last year, the fact that respondents' cybersecurity teams are understaffed for the size of their organizations was the top challenge (31%). This was followed by 28% who claim that their organizations do not provide enough cybersecurity training for non-technical employees, and 28% who say that their organizations depend upon too many manual/informal processes for cybersecurity.

ESG/ISSA find it especially alarming that nearly one-quarter of respondents (23%) say there is a lack of cybersecurity knowledge, oversight, and commitment by executive management. These organizations will serve as cybersecurity career way stations with high attrition rates. High-demand cybersecurity professionals will be actively recruited to leave these organizations for those with a stronger commitment to cyber-risk management.

## Figure 32. Biggest Cybersecurity Challenges

**Which of the following would you say are the biggest cybersecurity challenges at your organization? (Percent of respondents, N=327, three responses accepted)**

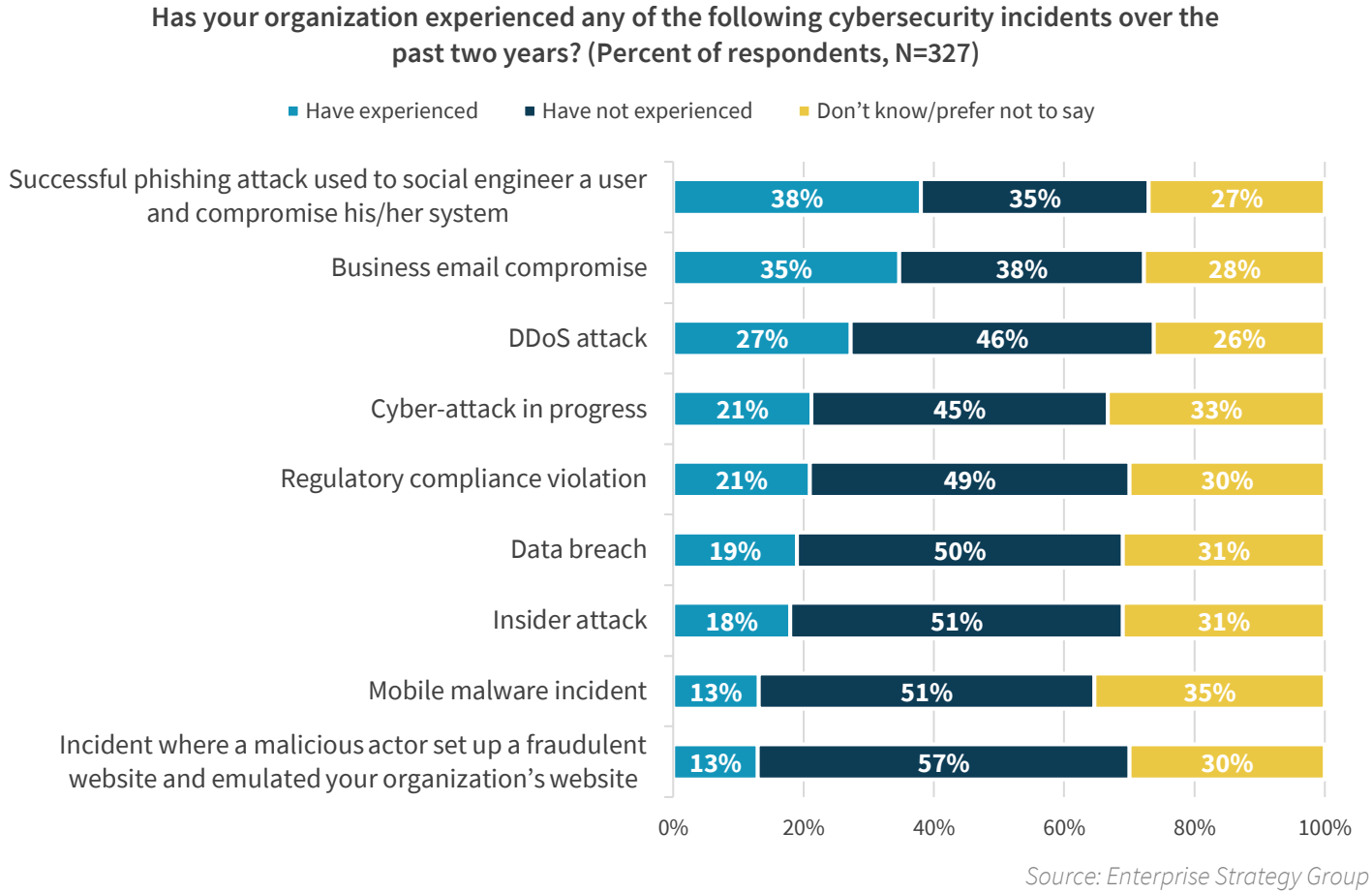



*Source: Enterprise Strategy Group*

In this year's survey, cybersecurity professionals were asked if their organization experienced several different types of cybersecurity incidents over the past two years (see Figure 33). Phishing, business email compromises, and DDoS attacks topped the list of incidents. It is also noteworthy that a large percentage of respondents either didn't know or preferred not

to say. This is understandable—cybersecurity professionals don't like to give details about their defenses, weaknesses, or past failures.

**Figure 33. Cybersecurity Incidents Experienced Over the Past Two Years**




*Source: Enterprise Strategy Group*

ESG/ISSA followed up the last question by asking respondents to identify factors that contributed to these security incidents (see Figure 34). These included:

- A lack of adequate training for non-technical employees. At 33%, this was the top response once again. Given that 38% of organizations experienced phishing attacks over the past two years, it appears that employees can't tell the difference between legitimate emails and social engineering. Clearly, more training is needed—especially considering work-from-home (WFH) initiatives driven by COVID-19.

- New IT initiatives without proper cybersecurity oversight and controls. Nearly one-third (31%) selected this response. To minimize cyber-risk, security professionals prefer to be involved in IT initiatives as early as possible so they can "bake in" rather than "bolt on" security after the fact. Unfortunately, this isn't happening on a regular basis.

- Poor security hygiene associated with IT assets. More than one-quarter (27%) said that poor hygiene leads to security incidents at their organization. This is alarming as security hygiene is a foundational concept—think CIS top 20.

## Figure 34. Biggest Contributors to Security Events Experienced

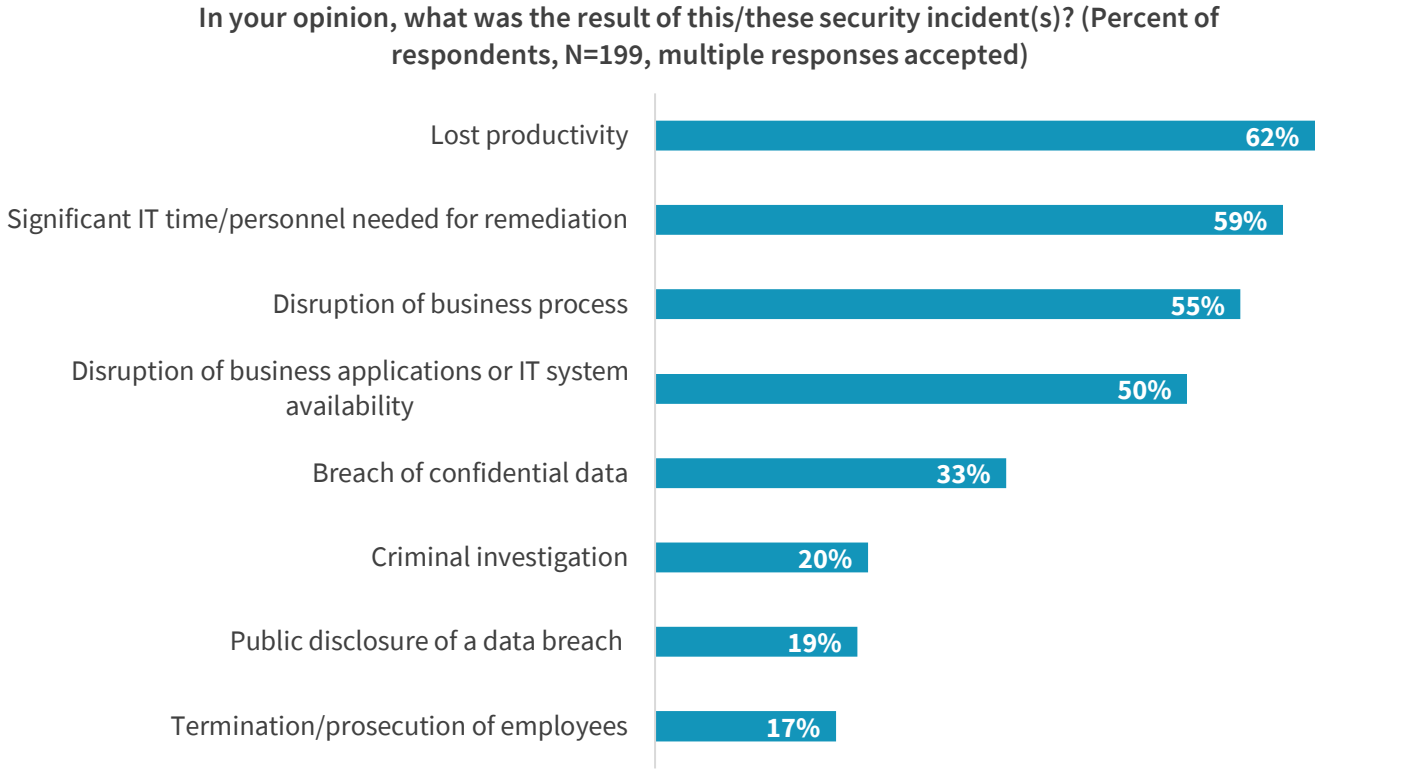
**Which of the following factors were the biggest contributors to the security events your organization experienced in the past two years? (Percent of respondents, N=199, three responses accepted)**


*Source: Enterprise Strategy Group*

The top three ramifications of security incidents were the same for the last three years—lost productivity, significant IT time/personnel for remediation, and disruption of business process (see Figure 35).

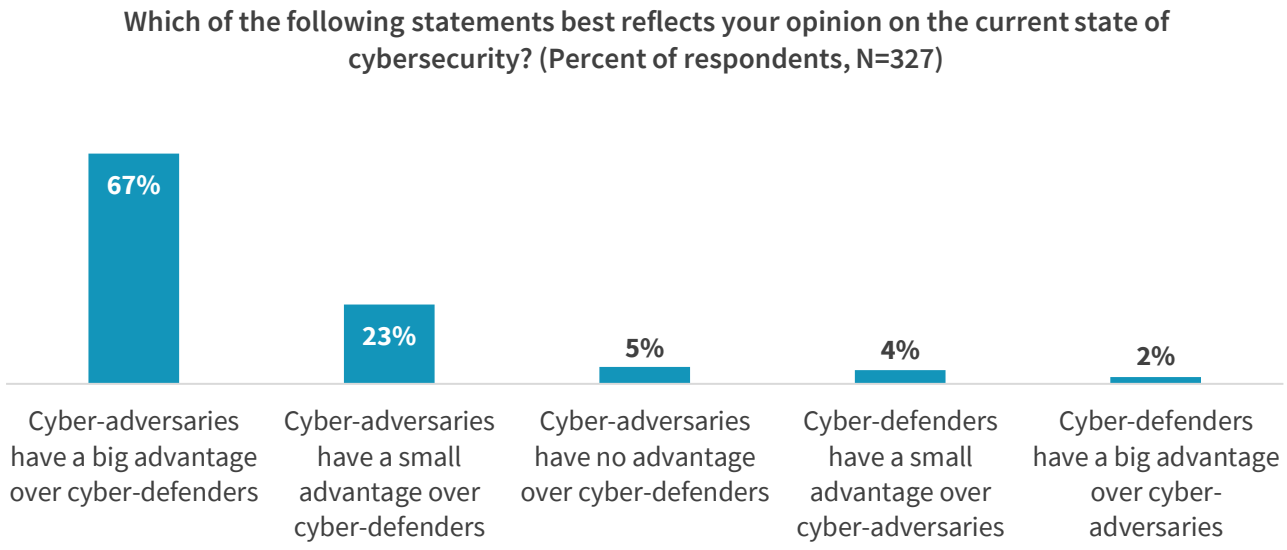
For the second year in a row, ISSA members were asked to compare the status of cyber-adversaries with that of cyber-defenders. The results are even more alarming than last year, as 67% of respondents believe that cyber-adversaries have a big advantage over cyber-defenders as compared to 59% in the 2018-2019 project (see Figure 36).

Figure 35. Results of Security Incidents




*Source: Enterprise Strategy Group*

Figure 36. Cyber-adversaries Have a Distinct Advantage over Cyber-defenders




*Source: Enterprise Strategy Group*

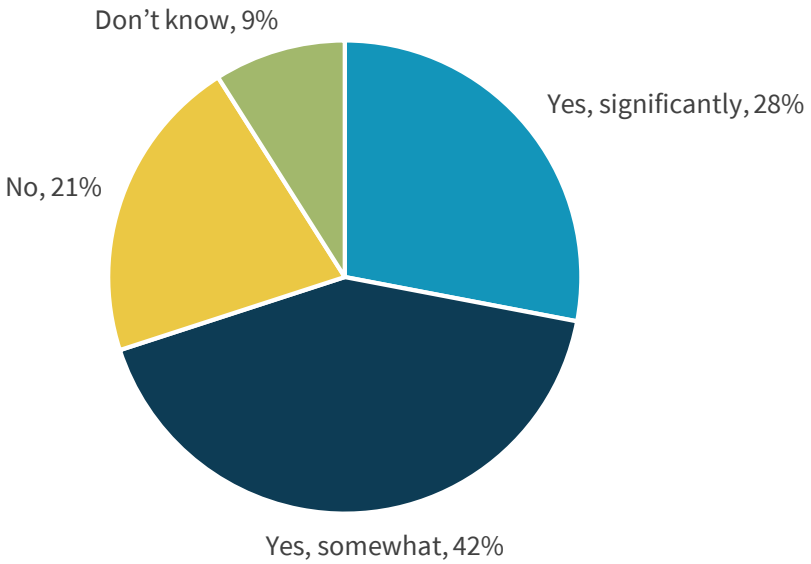
In aggregate, cybersecurity professionals appear to be fighting uphill. They don't believe they have adequate support from their organizations (or the cybersecurity industry, government agencies, or public education), and are forced to defend against a superior adversary. Little wonder then why so many organizations experience a variety of cyber-attacks and system compromises.

## The Cybersecurity Skills Shortage

As in past years, ESG and ISSA wanted to understand the implications of the global cybersecurity skills shortage and how it is affecting organizations. The data indicates that the situation remains static, as 28% of cybersecurity professionals say that the cybersecurity skills shortage has had a significant impact on their organizations, while 42% claim that their organizations have been impacted somewhat by the global cybersecurity skills shortage (see Figure 37).

**Figure 37. 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 organization you work for? (Percent of respondents, N=327)**

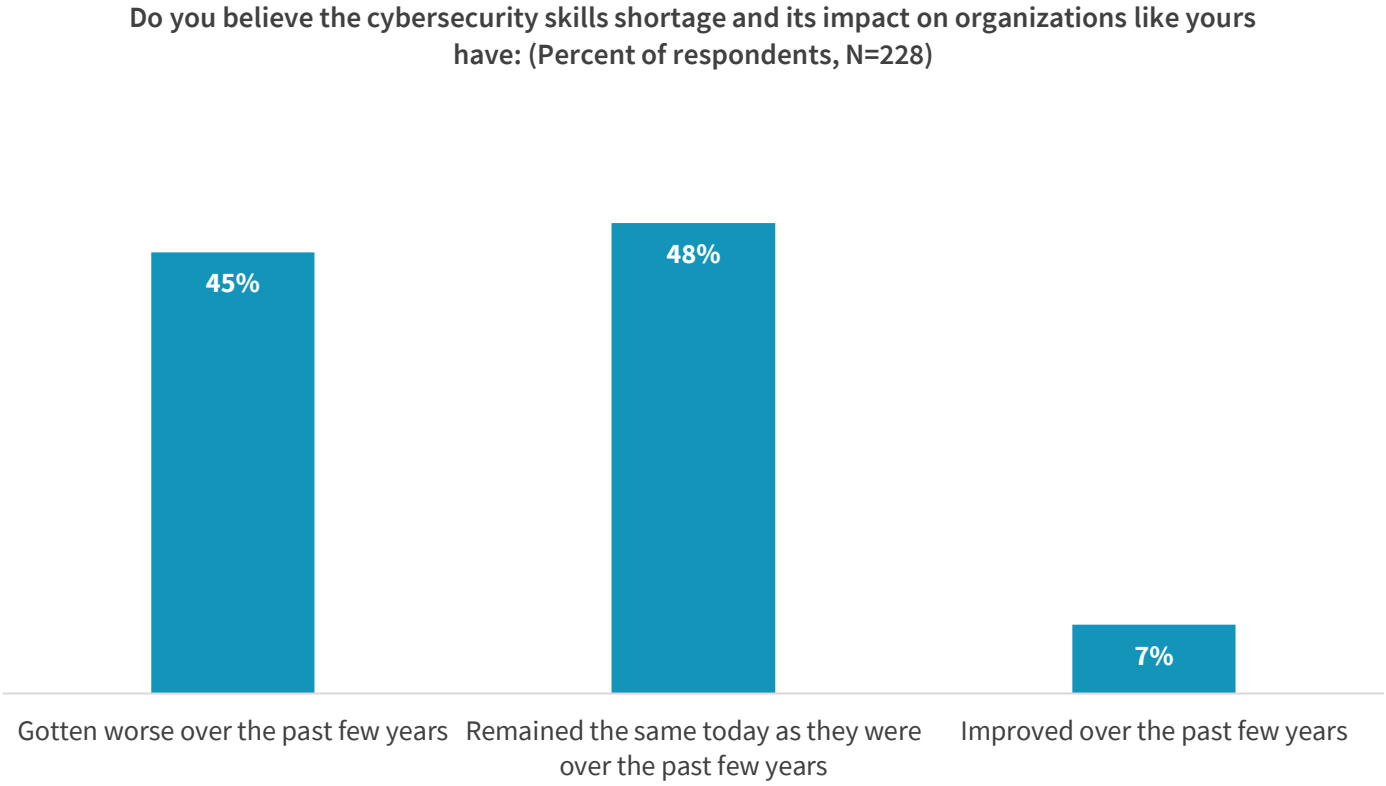



*Source: Enterprise Strategy Group*

In 2020, 70% of respondents claim that their organization has been impacted significantly or somewhat by the global cybersecurity skills shortage. These percentages are similar to those of the past 4 years, which ranged from a low of 69% to a high of 74%. The data demonstrates that things aren't improving, but are they getting worse? ESG/ISSA added a question to this year's survey to answer this question. The results are distressing—45% believe the cybersecurity skills shortage (and its impact) have gotten worse over the past few years while 48% say it's about the same today as it was over the past few years (see Figure 38). Only 7% believe things have gotten better.

This is an important data point that should be of concern to business executives, CISOs, educators, and government agencies. There's been plenty of talk about the cybersecurity skills shortage over the past 5 to 10 years but few results. Security leaders, educators, and legislators must brainstorm on new and creative ways to address this problem as common wisdom approaches aren't working.

Figure 38. The Cybersecurity Skills Shortage Is Not Improving

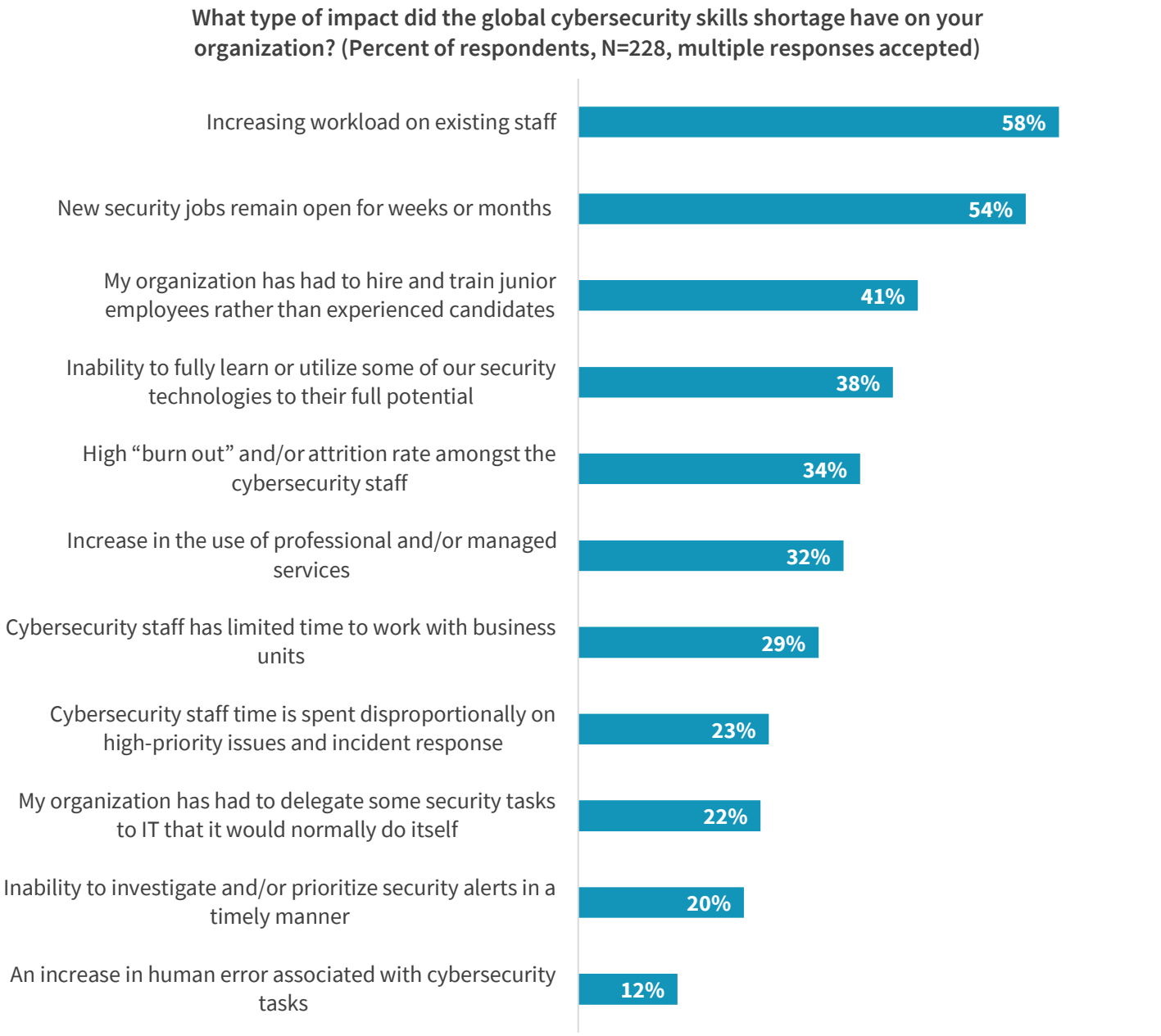



*Source: Enterprise Strategy Group*

Seventy percent of organizations say that the global cybersecurity skills shortage has had an impact. What type of impact (see Figure 39)? Once again, the top response (58%) was that it has increased the workload on existing staff, which is similar to last year's results (66%). In 2020, 54% of respondents also indicated that the skills shortage has led to new security jobs remaining open for weeks or months. This may be one reason why 41% of organizations must hire and train junior employees rather than experienced candidates.

It is also noteworthy that 38% of respondents say that the skills shortage has led to a situation where the cybersecurity team is unable to learn or utilize some security technologies to their full potential. This data point should set off alarms within the security technology industry. Smart vendors will bridge this gap with customer success programs and services to help customers improve security technology configuration, customization, and ongoing operations.

Figure 39. How the Cybersecurity Skills Shortage Has Impacted Organizations

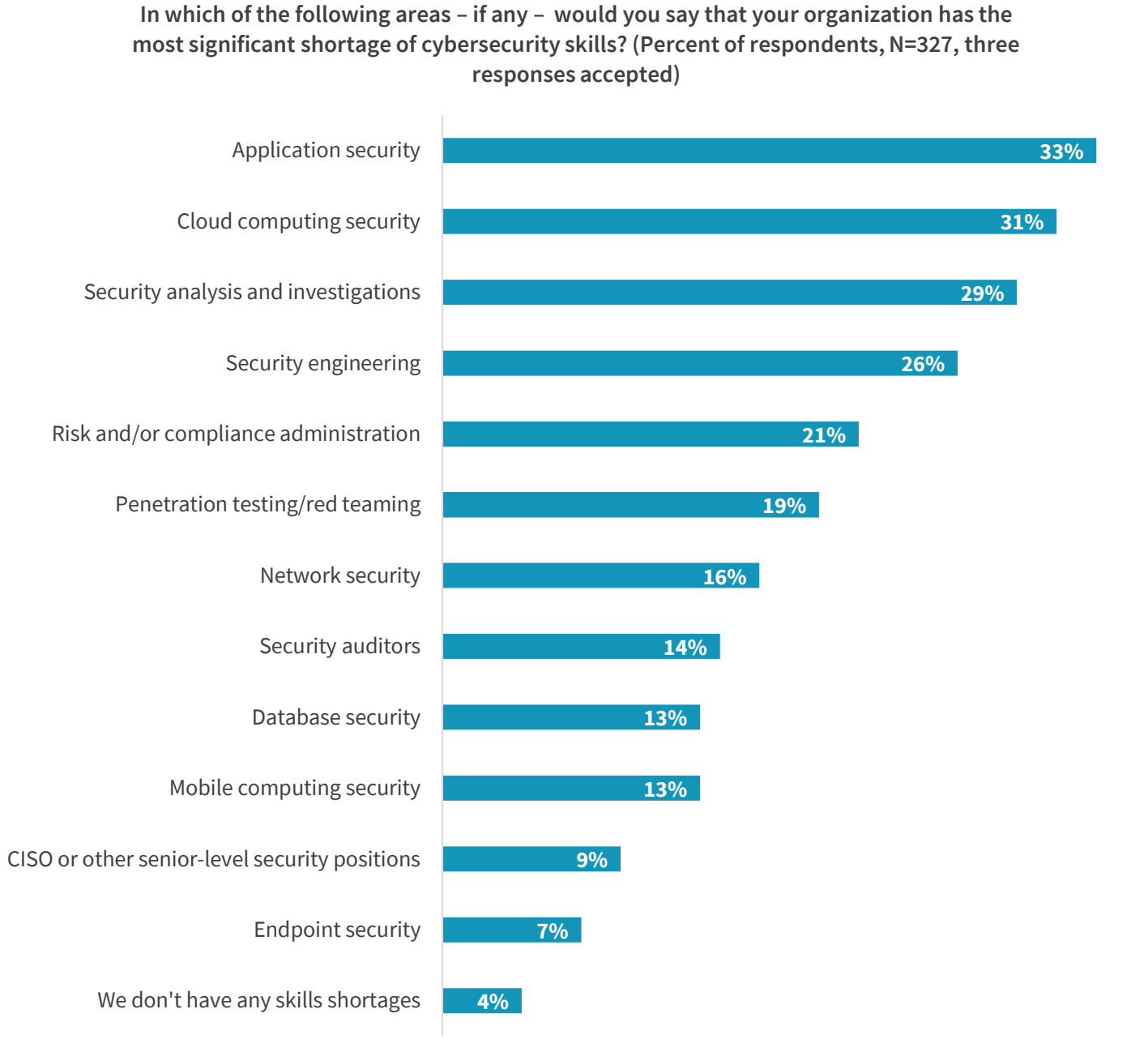



*Source: Enterprise Strategy Group*

Survey respondents were asked to identify areas with the most acute skills shortages. The two top spots flipped in 2020 with application security topping cloud computing security, but the percentages were almost identical to last year's results (application security: 33% in 2020 and 32% in 2018-2019, cloud computing security: 31% in 2020 and 33% in 2018-2019). Security analysis and investigations finished third in both years at 29% in 2020 and 30% in 2018-2019 (see Figure 40).

CISOs must understand the level of competition for candidates with these skill sets. It may be worthwhile to craft backup plans if recruitment efforts languish or fail completely. Examples include training software developers and DevOps personnel on application security, recruiting and training server virtualization administrators as cloud computing security specialists, and working with experienced managed services providers.

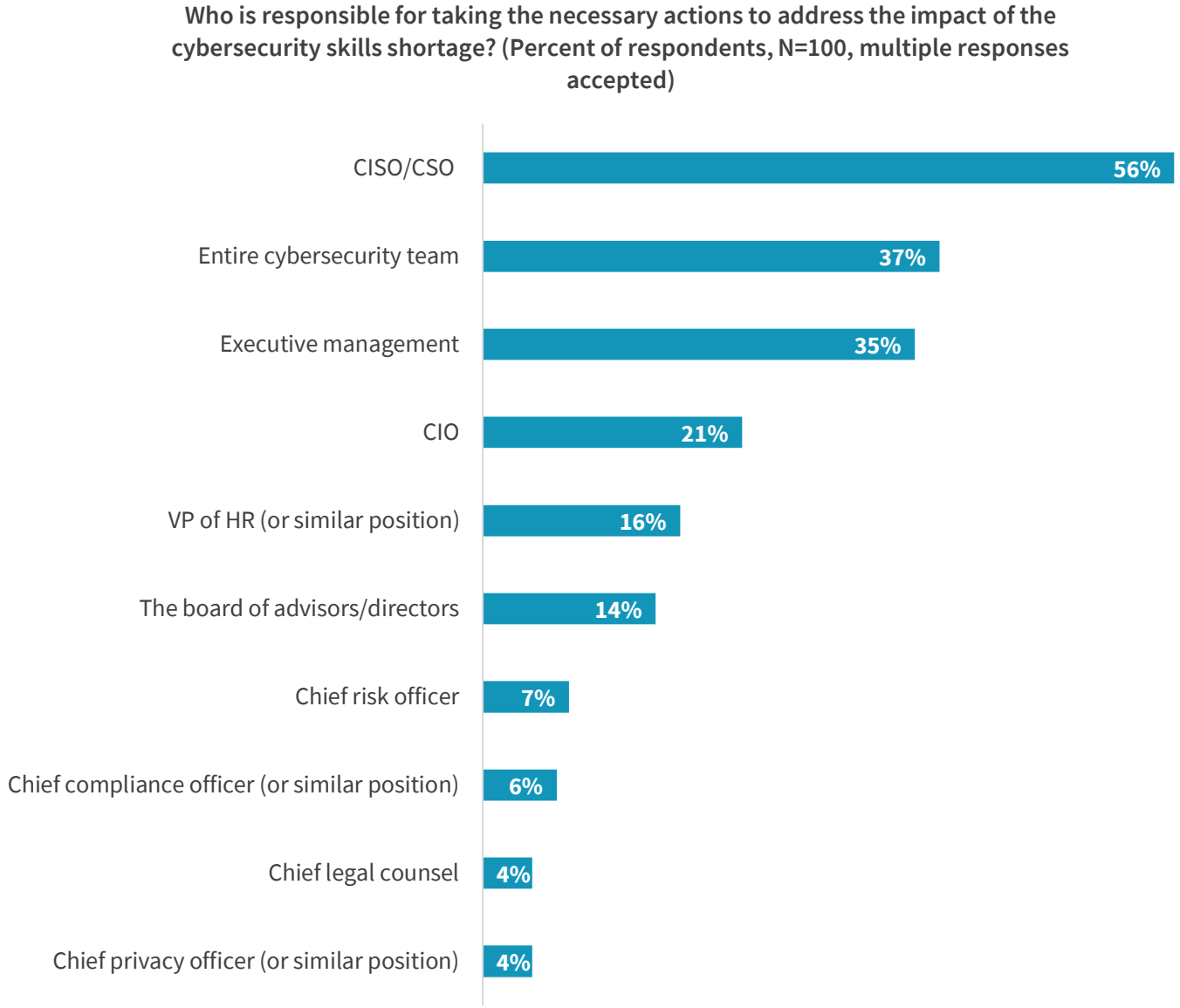
Figure 40. Area(s) with Biggest Shortage of Cybersecurity Skills




*Source: Enterprise Strategy Group*

In a new question for 2020, ISSA members were asked to identify who is responsible for addressing the cybersecurity skills shortage. Respondents indicate that CISOs/CSOs really own this problem (see Figure 41).

Figure 41. Responsibilities for Addressing the Impact of the Cybersecurity Skills Shortage



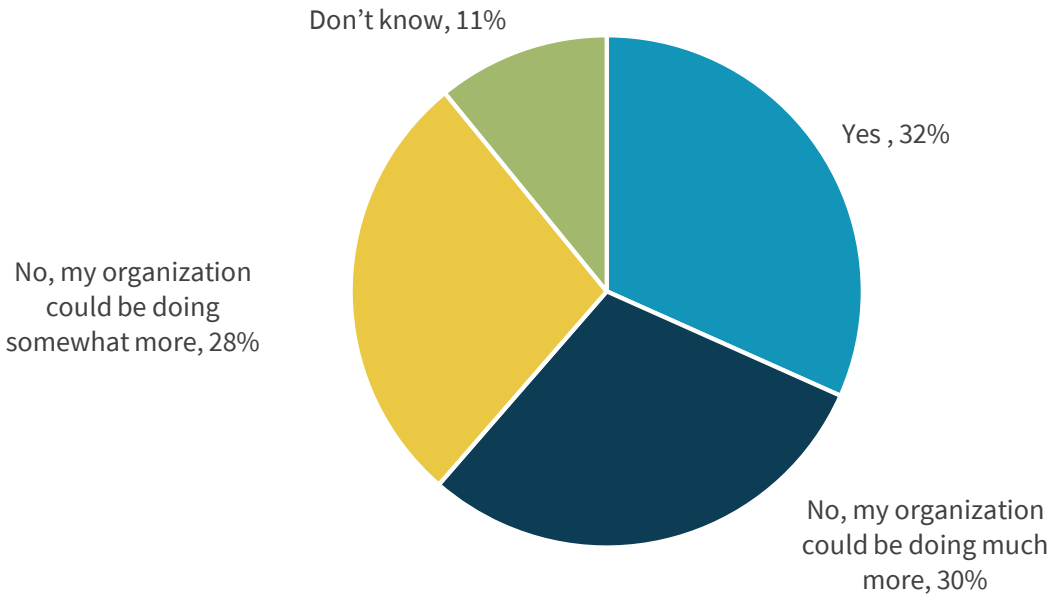

*Source: Enterprise Strategy Group*

Recall that nearly half of respondents (49%) believe the cybersecurity skills shortage hasn't improved while 43% say that things have gotten worse. The research indicates that this issue goes beyond global trends alone—organizations should be creating their own plans for addressing this situation.

How are they doing in this regard? Not too well—28% of respondents say that their organization could be doing somewhat more to address the impact of the cybersecurity skills shortage while 30% claim that their organization could be doing much more to address the cybersecurity skills shortage (see Figure 42).

## Figure 42. Organizational Response to the Cybersecurity Skills Shortage

**Do you believe your organization is taking the necessary actions to address the impact of the cybersecurity skills shortage? (Percent of respondents, N=314)**

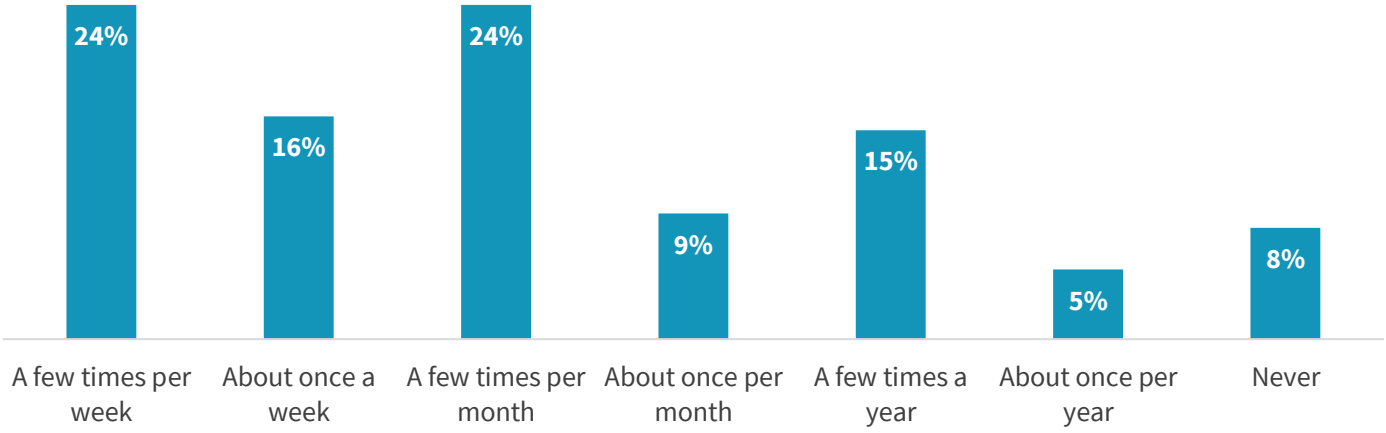



*Source: Enterprise Strategy Group*

One of the byproducts of the cybersecurity skills shortage is an extremely competitive market for talent. This has created a "seller's market" where skilled and experienced cybersecurity professionals are in high demand. In fact, 40% of the cybersecurity professionals responding to the ESG/ISSA survey say they are solicited by recruiters at least once per week while 72% are recruited at least once per month (see Figure 43). Aggressive recruitment efforts like these have been consistent for all four years of this project.

## Figure 43. Frequency of Solicitation by Job Recruiters

**About how often are you solicited to consider other cybersecurity jobs by various types of recruiters? (Percent of respondents, N=327)**




*Source: Enterprise Strategy Group*

After years of studying this issue, ESG believes that addressing the cybersecurity skills shortage effectively requires a combination of:

- Process automation. This means assessing and documenting processes, developing runbooks, and automating manual tasks that act as bottlenecks. In this way, organizations can decrease process time while improving employee productivity.
- Increasing the use of advanced analytics. CISOs should carefully evaluate emerging analytics technologies that can help improve alert fidelity, enrich security data, provide risk scores, and accurately pinpoint the root causes of problems. This is an evolving but promising area.
- Offloading of tasks to managed security service providers. CISOs understand that there will always be more work than staff capacity. These individuals tend to take a portfolio approach to their responsibilities, looking for pedestrian tasks to outsource and high skills areas for staff augmentation.
- Continuous progress for employees. Cybersecurity staff must be given a continuous opportunity for skills development and career advancement.

Organizations can also develop reputations within the cybersecurity community as great places to work. This effort includes:

- Competitive compensation.
- Continuous training and career development as described previously. CISOs can also encourage staff to work on open source projects, speak at conferences, work with leading vendors, etc.
- Strong mentoring programs.
- "Thought leadership" in areas like experimenting with emerging technologies, conducting threat research and analysis, participating in industry events, etc.

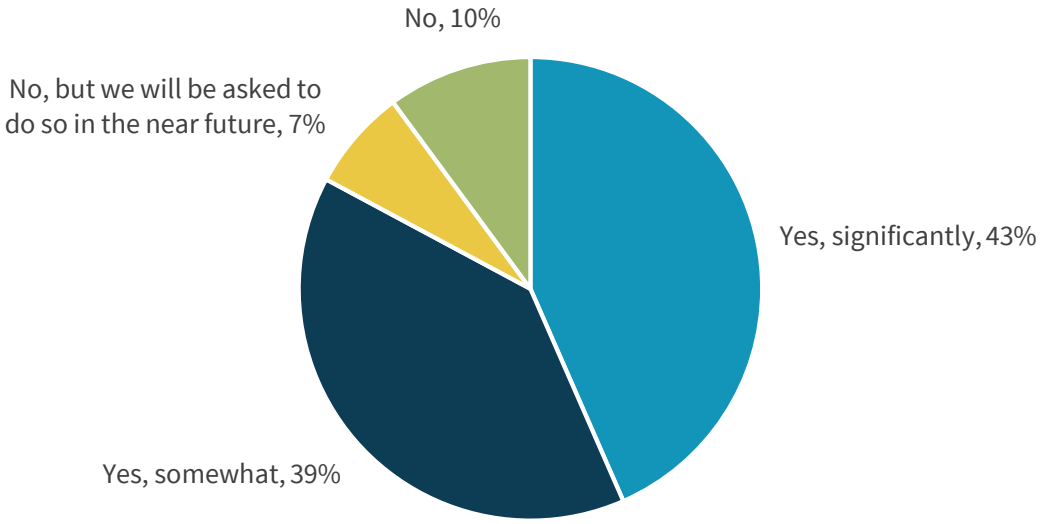
## The Quest for Cybersecurity Improvement

For the second year, ESG/ISSA asked respondents several questions about data privacy. The research reveals that 82% of respondents claim that the cybersecurity team at their organization has taken a more active role in data security while 7% expect to be asked to do so in the future (see Figure 44). The data is almost identical to last year.

Who owns data privacy? Under half (42%) of organizations have a data privacy officer, slightly higher than last year's response of 37%. More than one-quarter (28%) don't have a chief privacy officer but rather delegate these responsibilities to others (see Figure 45). Based upon the ESG/ISSA research, it's fair to assume that CISOs are often called upon to fill this role. Typically, they work hand-in-hand with legal and compliance teams. In these cases, legal/compliance personnel own data privacy policy creation while CISOs are called upon to operationalize the plan.

## Figure 44. Cybersecurity Teams Are More Active in Data Privacy

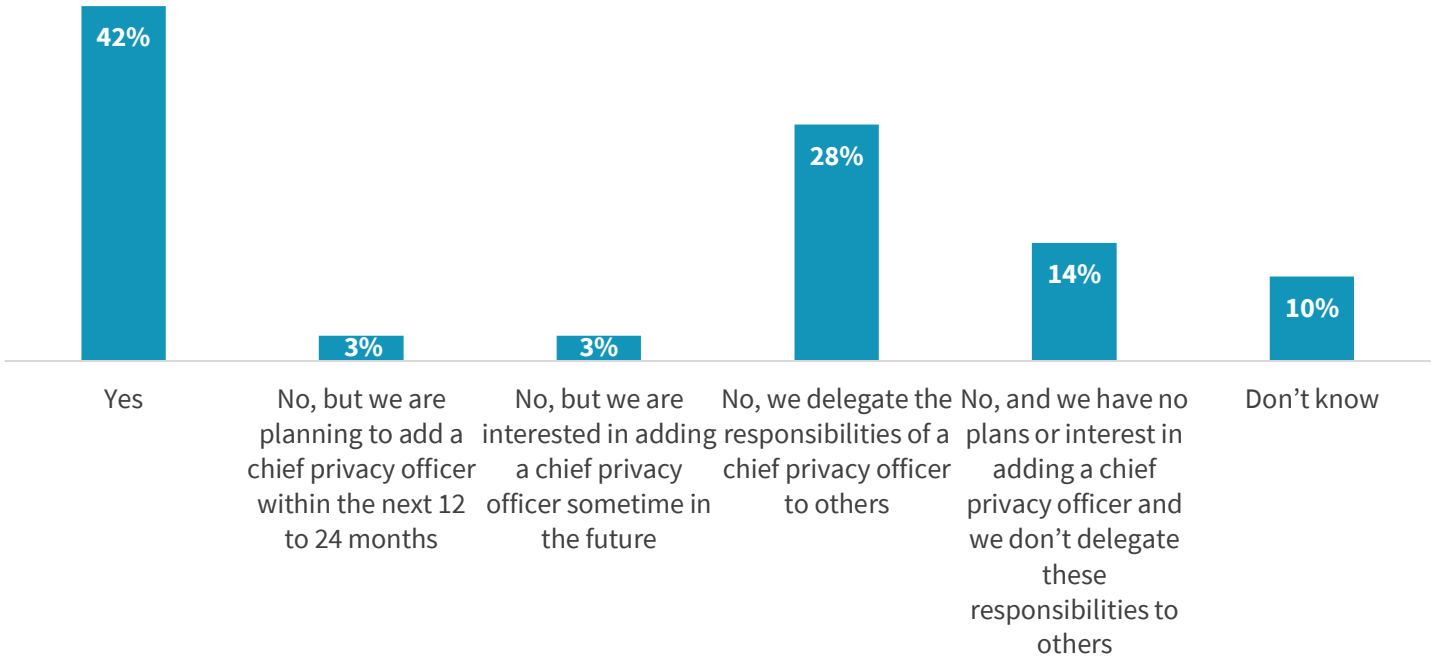
**Has your cybersecurity team taken a more active role with data privacy over the past 12 months? (Percent of respondents, N=327)**




*Source: Enterprise Strategy Group*

## Figure 45. Does Organization Have a Chief Privacy Officer?

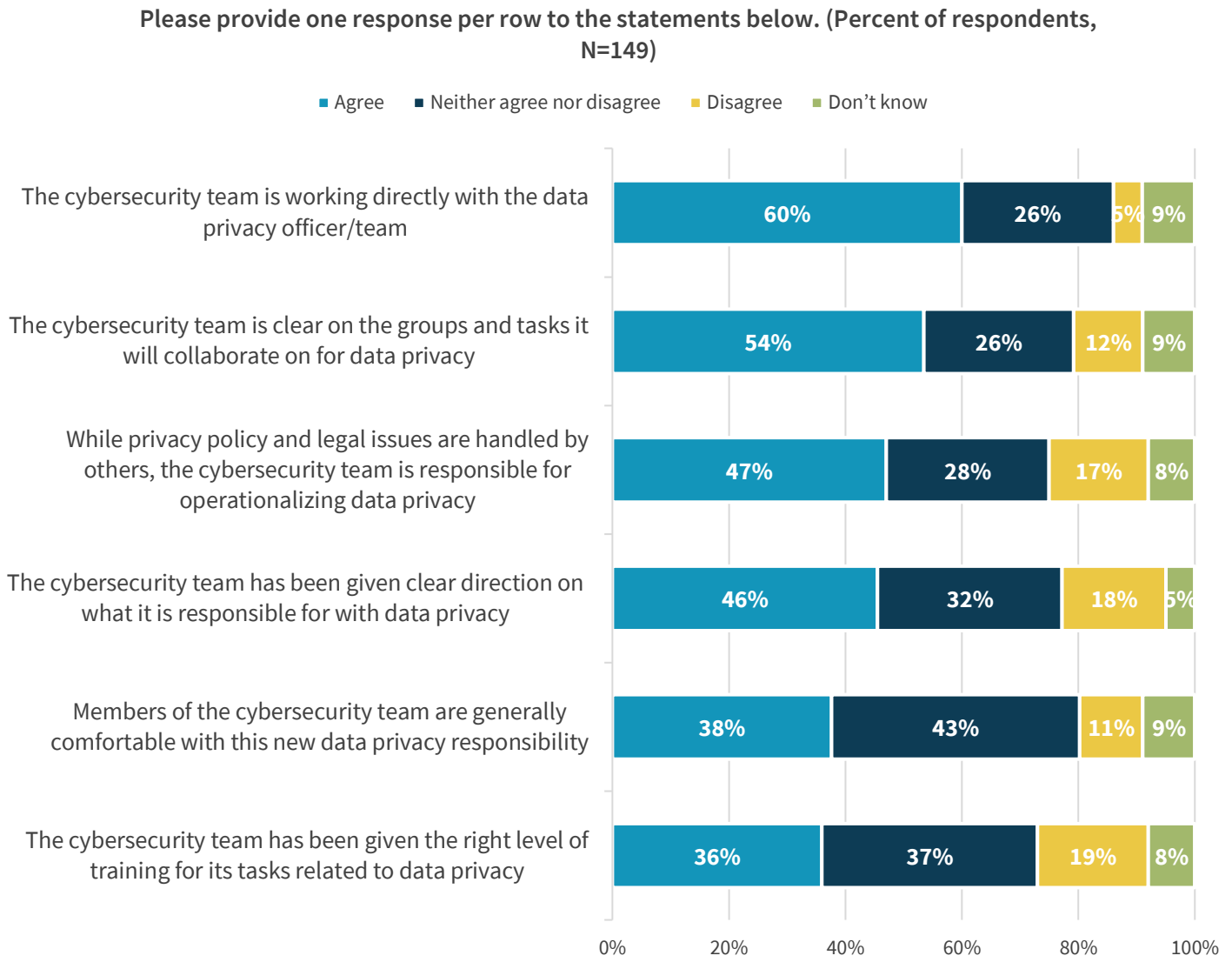
**Does your organization have a chief privacy officer (or an individual/group with a similar role)? (Percent of respondents, N=327)**




*Source: Enterprise Strategy Group*

Survey respondents were then asked a series of opinion questions about their data privacy programs (see Figure 46). While most of the data shows cybersecurity support for data privacy, it is worth noting that 18% disagree with the statement: The cybersecurity team has been given clear direction on what it is responsible for with data privacy. CISOs should investigate this lack of clarity within their organization and resource efforts to align policy with data privacy operations where it exists.

**Figure 46. Data Privacy Opinions**




*Source: Enterprise Strategy Group*

## Conclusions

Cybersecurity professionals continue to manage their careers in a tactical manner with little long-term planning. This is especially problematic for inexperienced cybersecurity professionals seeking a career path toward a CISO position. Many cybersecurity professionals believe that their organizations, governments, and school systems need to do more to keep up with cybersecurity requirements. They also remain bearish about the current balance of cybersecurity power and give a distinct advantage to adversaries over defenders.

The cybersecurity skills shortage seems to be getting worse, forcing overwhelmed cybersecurity professionals into constant firefighting. Despite these ongoing problems, many organizations have been able to manage through the global pandemic, providing basic connectivity, network access, and security to employees. This points to good planning, strong collaboration with IT operations, and cybersecurity professional perseverance.

### Takeaways for Cybersecurity Professionals

As with past reports, cybersecurity professionals—especially those in the early stages of a cybersecurity career or individuals seeking to enter the field—should use this research for career planning. Therefore, cybersecurity professionals should:

1. Explore future career options and then craft and manage a career plan; job shop if you must but be extremely selective when contemplating new job opportunities. Work with a transformation coach, a group of peer advisors, and a career mentor to build and pivot the career plan as you discover what you love most about your career in cybersecurity.

2. Seek out opportunities for hands-on experience and network with other cybersecurity pros as much as possible. Move beyond your comfort zone to reach out and build your network of support through online and in-person networking events.

3. Plan for continuous education and training to develop business, communications, leadership, and management skills as much as possible, especially improving knowledge and skills around data privacy and security. Understand the importance and balance of knowledge skills and abilities—technical knowledge, business acumen, ability to develop and set security strategy, and capability to impart this knowledge to your executive team, your business unit, and your employees at levels that they can absorb. Find ways to strengthen these KSAs as you move through your career path.

4. Manage job-related stress and seek help if necessary.

5. Know and think like the enemy. In other words, understand their motivations; skills; and tactics, techniques, and procedures (TTPs). This will help you develop better countermeasures.

### Takeaways for CISOs and Organizations

This research should be used as a guideline for building a strong and happy cybersecurity team. CISOs and their organizations should:

1. Work with the cybersecurity staff on career development.

2. Anticipate the cybersecurity skills shortage impact on every aspect of your cybersecurity program by getting creative with cybersecurity recruitment and engaging non-technical candidates with the right underlying skills.

3. Make cybersecurity awareness training a priority rather than a checkbox exercise, invest in continuous training for the cybersecurity staff, and develop mentoring and staff rotation programs. Teach security awareness and advocate for security accountability programs as a necessary part of each employee's performance and responsibility in the organization

4. Encourage the cybersecurity staff to network with peers and participate in research, development, and innovation. Understand the goals of your staff and help them to devise a career plan based on what they are interested in and what you see in them.

5. Get business executives and corporate directors more involved in cybersecurity program management, especially when it comes to operationalizing data privacy. Help the executives to understand the importance of the role of cybersecurity in the overall strategic mission and business goals.

## Research Methodology

To gather data for the main part of 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 December 10, 2019 and January 20, 2020.

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 327 security and IT professionals.

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

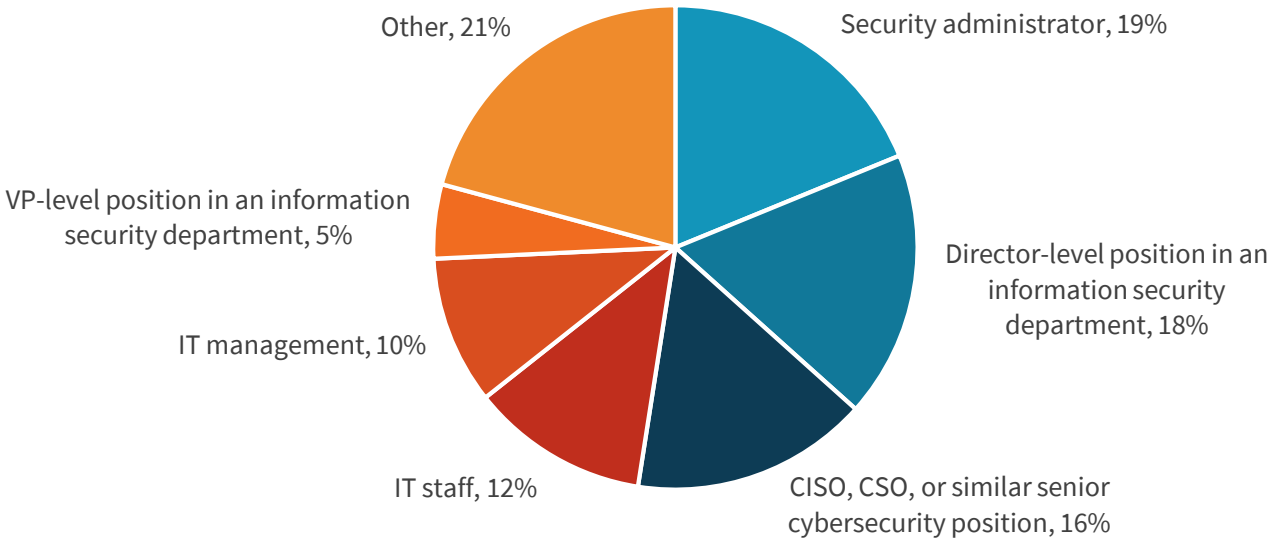
Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

## Respondent Demographics

The data presented in this report is based on a survey of 327 qualified respondents and cybersecurity professionals. Figure 47 through Figure 50 detail the demographics of the respondent base at an individual and organizational level.

### Figure 47. Respondents by Current Position

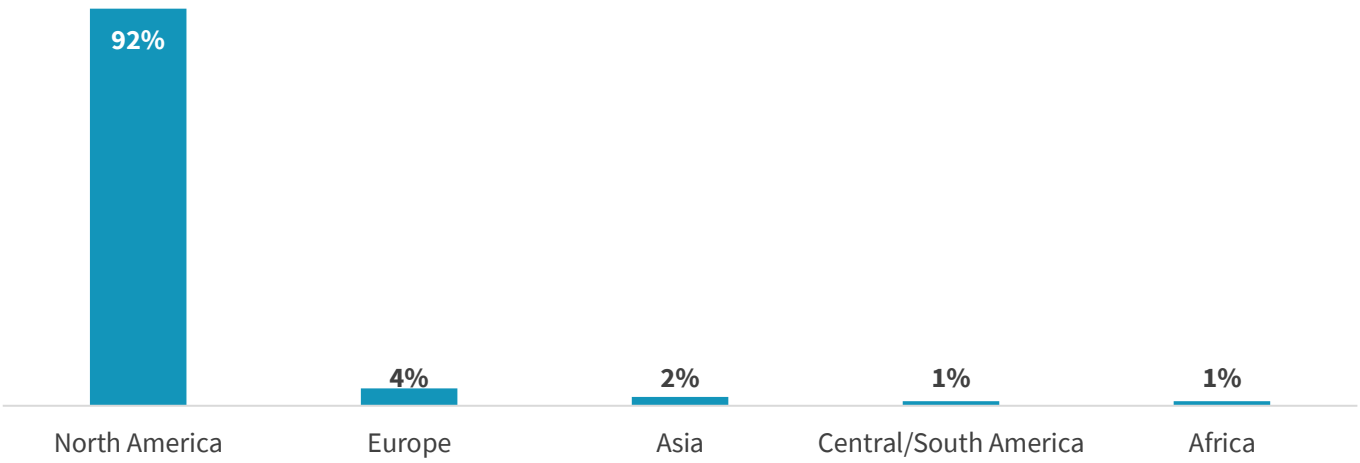
**Which of the following best describes your current position within your organization? (Percent of respondents, N=327)**




*Source: Enterprise Strategy Group*

### Figure 48. Respondents by Region

**Please indicate where you are based (i.e., where you live and work). (Percent of respondents, N=327)**



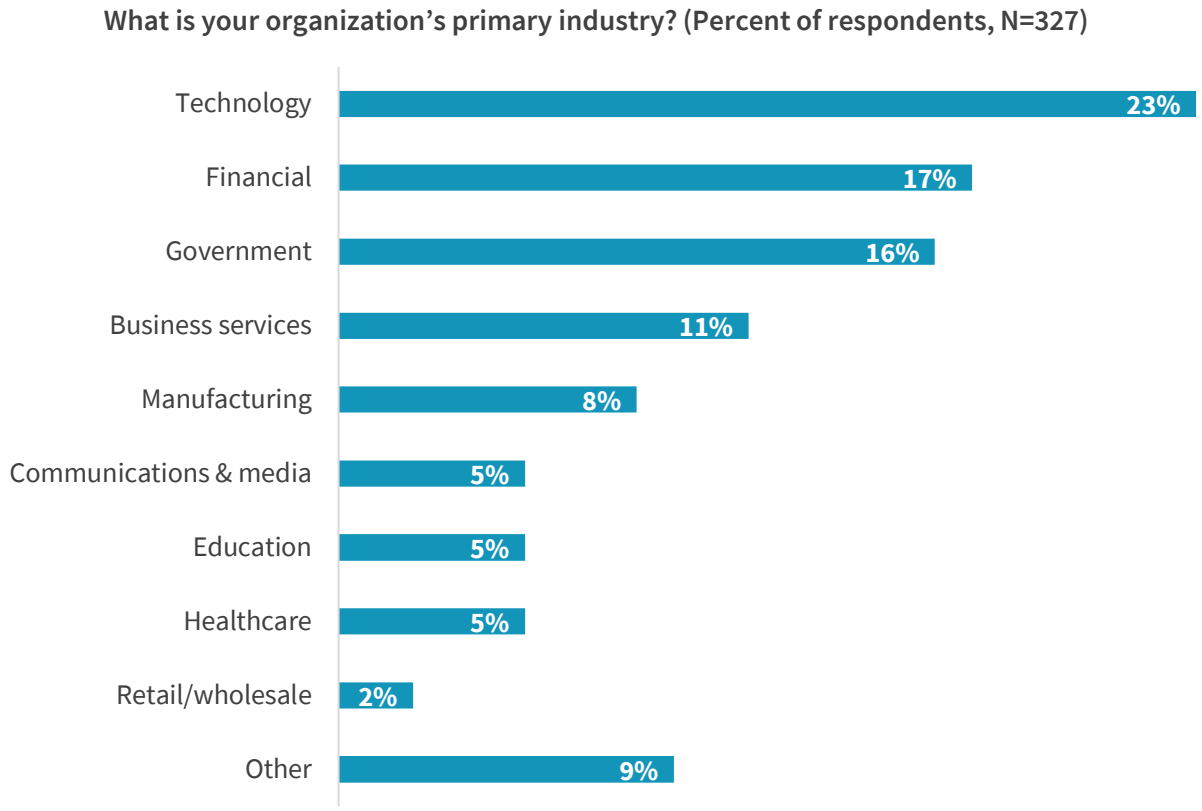

*Source: Enterprise Strategy Group*

Figure 49. Respondents by Number of Employees


*Source: Enterprise Strategy Group*

Respondents were asked to identify their organization's primary industry. In total, ESG received completed, qualified responses from individuals in 19 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 50.

Figure 50. Respondents by Industry




*Source: Enterprise Strategy Group*

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


www.esg-global.com


contact@esg-global.com


508.482.0188