RESEARCH REPORT

The Life and Times of Cybersecurity Professionals

By Jon Oltsik, ESG Senior Principal Analyst

November 2017

A Cooperative Research Project by ESG and ISSA

Contents

List of Figures

List of Tables

Executive Summary

Report Conclusions

In 2017, the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA) teamed up for the second year in a row to look at the lives and experiences of cybersecurity professionals. This year's report is based on data from a survey of 343 cybersecurity professionals and ISSA members. Eighty-five percent of survey respondents resided in North America, 7% came from Europe, 3% from Central/South America, 3% from Asia, and 1% from Africa.

Like 2016, this year has been eventful in terms of cybersecurity events. For example:

- As of the writing of this report, there have been 416 publicly disclosed data breaches, exposing more than 156 million records (source: privacyrights.org). Visible breaches occurred at organizations like SVR Tracking (540,000 records exposed), Equals3 (590,000+ records exposed), BroadSoft (4,000,000 records exposed), and Equifax (143,000,000 records exposed).

- Ransomware variants like WannaCry, Petya, and Bad Rabbit continue to proliferate. According to a report from Cybersecurity Ventures, ransomware damage is up 15x in two years as global damages are expected to exceed $5 billion in 2017, up from $325 million in 2015.

- Recent threat intelligence from Check Point Software and Qihoo identified a new IoT botnet dubbed "reaper." Researchers claim that reaper is much more sophisticated than the Mirai IoT botnet used to attack DNS services at Dyn that rendered many Internet sites inaccessible in 2016. Some researchers believe that reaper could grow much larger than Mirai and harness enough network bandwidth to take down critical services or large parts of the Internet.

The continuing cycle of threats and visible data breaches motivates organizations to bolster their cybersecurity defenses. ESG's annual IT spending intentions data for 2017 reveals:

- Sixty-nine percent of organizations planned to increase cybersecurity spending in 2017. This percentage is almost identical to the percentage of organizations that increased cybersecurity spending in 2016 (70%).

- Thirty-nine percent of organizations say that increasing cybersecurity protection is one of their highest *business* initiatives driving IT spending in 2017.

- Thirty-two percent of organizations say that strengthening cybersecurity tools and processes is one of their most important IT initiatives in 2017.[1]

As in the 2016 report, the data presented here illustrates an escalating and dangerous game of cybersecurity "cat and mouse." Cyber-adversaries continue to develop creative tactics, techniques, and procedures (TTPs) for attacks. Recognizing the risk, large and small organizations are prioritizing and investing in cybersecurity defenses and oversight.

Cybersecurity professionals continue to reside on the frontline of this perpetual battle, tasked with applying limited resources as countermeasures and defending their organizations against a constant barrage of cyber-attacks. Many organizations fight this fight with suboptimal forces—ESG research reveals that 45% of organizations claim to have a problematic shortage of cybersecurity skills.[2]

[1] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, March 2017.
[2] Source: ESG Brief, *2017 Cybersecurity Spending Trends*, March 2017.

Given this daunting responsibility, it's natural to wonder just how well cybersecurity professionals are holding up. Are they prepared for this perpetual battle or has the pace and intensity of their jobs caused a state of professional burnout within the cybersecurity ranks? What is the impact on the organizations they work for?

To answer these questions, the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA) teamed up once again and initiated a primary research project in 2017 with the goal of capturing the voice and thoughts of cybersecurity professionals on the state of their profession and gaining a perspective on situational analysis from those closest to the fight. In pursuit of this goal, ESG/ISSA surveyed 343 IT and information security professionals (and ISSA members). Survey respondents represented organizations of all sizes located in all parts of the world (see the demographics section of this report for more details).

Based upon the data collected, the big change from last year is that the cybersecurity skills crisis is getting worse and causing a rapidly widening business problem. Consistent with last year, the majority of respondents continue to believe that the cybersecurity skills shortage has had an impact on their organization and confirm that the cybersecurity skills shortage is exacerbating the number of data breaches. However, this year, these same organizations are significantly falling behind in providing an adequate level of training, and a lack of training has taken the lead as the number one contributing factor to security events. This points to an important shift from a staffing gap to a training gap at all levels of the organization, a consistent theme throughout this year's report.

This report concludes (in order of the survey questionnaire):

- Cybersecurity professional career paths follow a common pattern. Nearly half (47%) of survey respondents got into cybersecurity as a chance to use their skills and curiosity to pursue technical challenges, 37% state that a cybersecurity career was a natural progression from an IT position, and 36% were attracted by the morality of the profession. Taken together, this data indicates that many cybersecurity workers come from a subsegment of IT professionals who want to use their technical skills in the fight of good versus evil. While this data is useful for recruiting purposes, it also illustrates the limited pool of potential future cybersecurity professionals today. The cybersecurity industry must reach beyond this traditional base, promote cybersecurity as a career path, and educate a broader population on cybersecurity career opportunities.

- Cybersecurity professionals struggle to define their career paths. Two-thirds (66%) of respondents do not have a clearly defined career path or plan to take their careers to the next level. This is likely due to the diversity of cybersecurity focus areas, the lack of a well-defined, industry-standard cybersecurity career lifecycle map, and the rapid changes in the cybersecurity field itself. Business, IT, and cybersecurity managers, academics, and public policy leaders should take note of today's cybersecurity career morass and develop and promote more formal cybersecurity guidelines and frameworks that can guide cybersecurity professionals in their career development in the future.

- Cybersecurity professionals have solid ideas for skills advancement. When asked how they improve their knowledge, skills, and abilities (KSAs), 76% of cybersecurity professionals pointed to things like attending specific cybersecurity training courses, participating in professional organizations (71%), and attending industry trade shows (53%). Clearly, survey respondents believe that interacting with other cybersecurity professionals is the best way to move ahead.

- Technical certifications remain a niche. New cybersecurity professionals are often overwhelmed by the number of certification options in the field, and some pursue multiple certifications because they believe that a business card full of acronyms will lead to career success. For the second year running, the ESG/ISSA research disputes this notion. While survey respondents claim that a CISSP is important for finding a job, other certifications aren't nearly as useful. Beyond a CISSP, other certifications are more useful to highlight knowledge around cybersecurity sub-topics.

- **Cybersecurity professional job satisfaction depends upon culture and continuing education.** Beyond leading compensation, cybersecurity professionals find job satisfaction from organizations that provide incentives for career advancement, provide an opportunity to work with other skilled cybersecurity professionals, and support a strong commitment to cybersecurity by business leaders.

- **Most cybersecurity professionals aren't satisfied with their current job.** Alarmingly, 60% of survey respondents are somewhat satisfied, not very satisfied, or not at all satisfied with their current positions. This data hints at a future with high attrition rates. To avoid this, CISOs must assess staff satisfaction and make necessary changes to retain employees for the long term.

- **Most organizations are not providing the cybersecurity staff with adequate training.** While 96% of survey respondents agree that keeping their skill set up to date is a cybersecurity career requirement, only 38% of those surveyed believe that their organization is providing an appropriate level of training for them to keep up with business and IT risks. This training gap should be concerning to business, IT, and cybersecurity executives alike.

- **Cybersecurity pros are in high demand.** Nearly half (49%) of those surveyed are solicited to consider other cybersecurity jobs at least once per week. This isn't surprising given the global cybersecurity skills shortage and high demand for top talent. This situation may be good for job applicants but high employee attrition and salary inflation should be a top concern for all CISOs.

- **CISOs are not always getting boardroom-level attention.** Nearly one-third (31%) of survey respondents working at organizations that employ a CISO (or equal position) believe that their CISO does not have an adequate level of participation with executive management or the board of directors. This data is consistent with a sub-theme throughout the report. Despite the continuous cycle of cyber-threats and data breaches, some organizations continue to treat cybersecurity as a necessary evil or compliance mandate alone.

- **Most organizations experience security incidents for a number of reasons.** The majority of organizations have experienced one or several security incidents over the past two years. There are many contributing factors to these incidents, including a lack of training, a sub-optimally sized cybersecurity staff, and business management that treats cybersecurity as a low priority. Security incidents tend to result in lost productivity or even disruption of a critical business service.

- **The majority of organizations are vulnerable to a damaging cyber-attack.** Ninety-one percent of survey respondents believe that most organizations are extremely vulnerable or somewhat vulnerable to a damaging cyber-attack. This is a frightening data point since these ISSA professionals have direct and hands-on knowledge of their organizations' cybersecurity status.

- **Organizations face numerous cybersecurity challenges**. When asked to identify their organizations' top security challenges, survey respondents pointed to a sub-optimal cybersecurity staff, too many manual cybersecurity processes, and business managers' lack of cybersecurity knowledge. The data points to the reality that most organizations have a wide range of cybersecurity challenges to address.

- **The cybersecurity skills shortage impact is widespread**. Seventy percent of survey respondents say that the cybersecurity skills shortage has had an impact on their organization. This impact includes an increasing workload for the cybersecurity staff, the need to recruit junior employees in lieu of more experienced cybersecurity professionals, and the need to focus on high-priority security events rather than security planning, strategy, or training. When asked

to identify acute areas of cybersecurity skills shortages, respondents identified security analysts, application security specialists, and cloud security experts.

- **ISSA members have suggestions to improve cybersecurity.** When asked what would be most beneficial for their organizations' overall cybersecurity, survey respondents suggested adding cybersecurity goals and metrics for business and IT managers, documenting and formalizing cybersecurity processes, and hiring additional staff. This data points to an overall desire to make cybersecurity a more structured and critical component of the overall organizational mission.

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 actually 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?

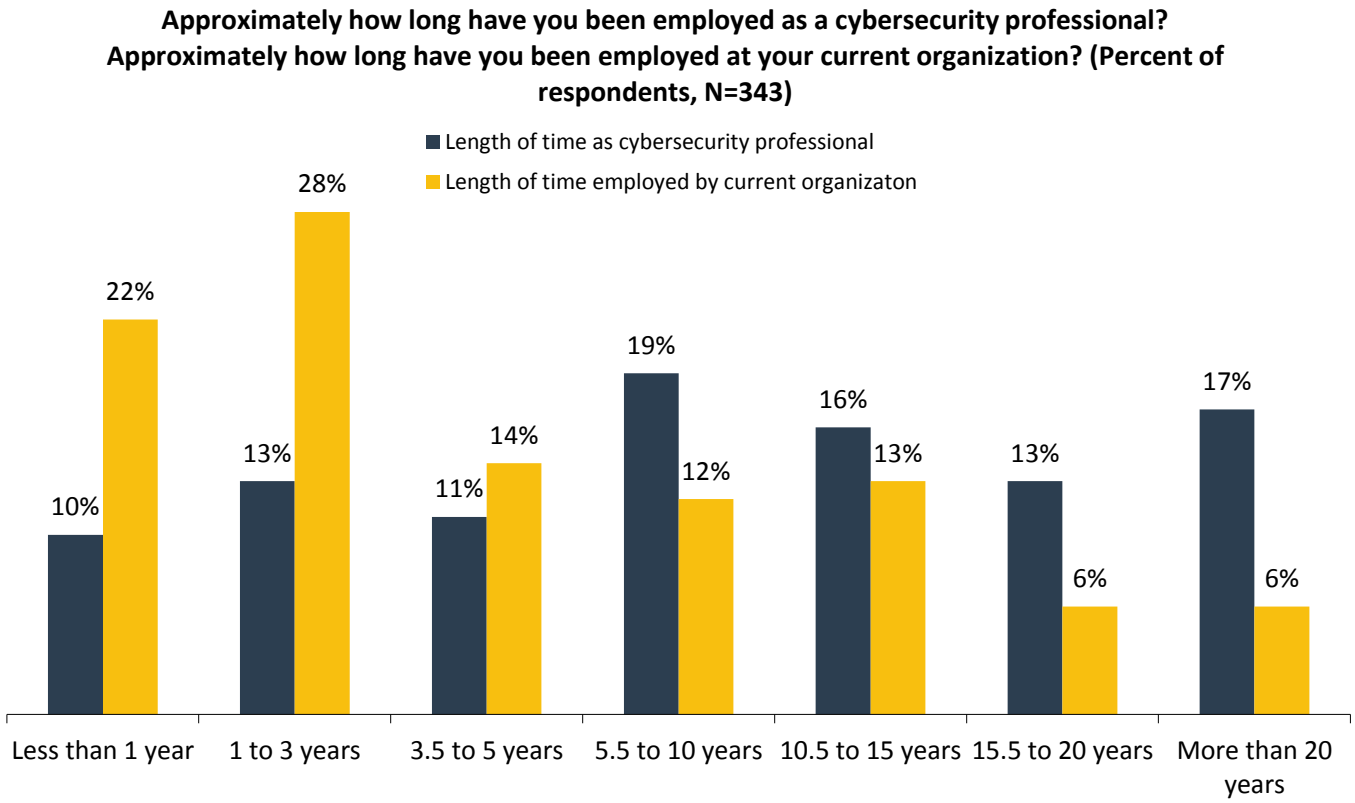
Survey participants represented a wide range of industries including health care, IT, financial services, manufacturing, business services, communications and media, and government. For more details, please see the *Research Methodology* and *Respondent Demographics* sections of this report.

Research Findings

The ISSA Survey Respondents

The ESG/ISSA research study is based upon a survey of a diverse group of cybersecurity professionals ranging from entry-level to senior positions. According to Figure 1, more than one-third (34%) have less than 3 years' experience while 30% have been cybersecurity professionals for at least 15 years. Most of the cybersecurity professionals surveyed for this project have been employed at their current organization for a relatively short timeframe—50% have been employed at their current organization for 3 years or less.

Figure 1. Length of Time Employed as a Cybersecurity Professional and at Current Organization/Job

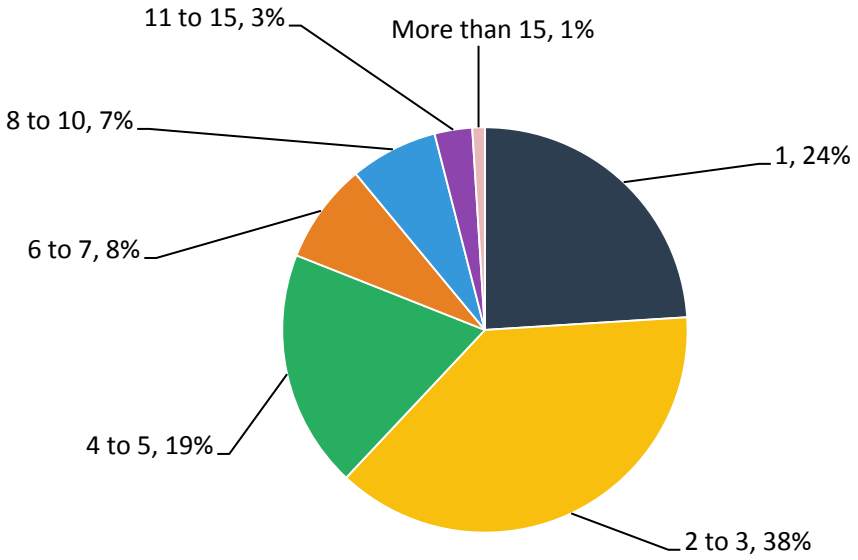


Source: Enterprise Strategy Group and ISSA, 2017

The ESG/ISSA research data indicates that 62% of cybersecurity professionals have worked at one or two jobs in their entire career (see Figure 2). ESG/ISSA also wanted to align respondents' experience with the phases of the ISSA cybersecurity career lifecycle. Twenty-two percent of respondents consider themselves "senior," while 45% rank themselves as "leaders" (see Figure 3).

Figure 2. Number of Different Organizations Respondents Have Worked for as a Cybersecurity Professional

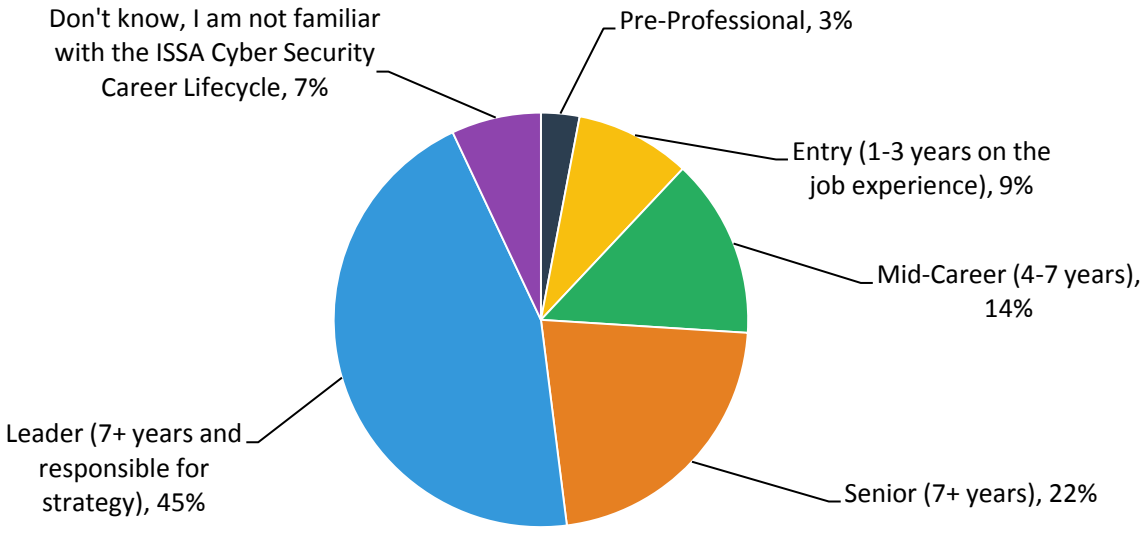
Approximately how many different organizations have you worked for during the span of your cybersecurity career? (Percent of respondents, N=343)



Source: Enterprise Strategy Group and ISSA, 2017

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=316)

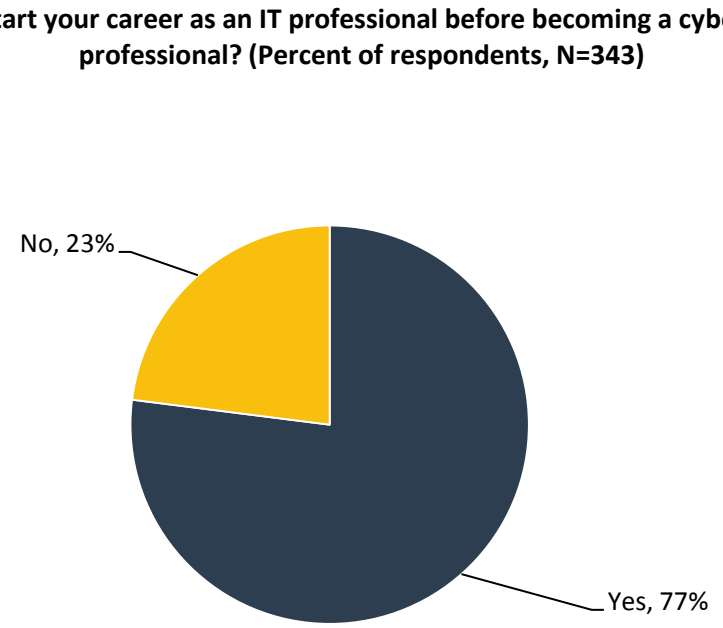


Source: Enterprise Strategy Group and ISSA, 2017

The Cybersecurity Professional

A vast majority of cybersecurity professionals (77%) 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 last year's project (78% started their career in IT, 22% did not).

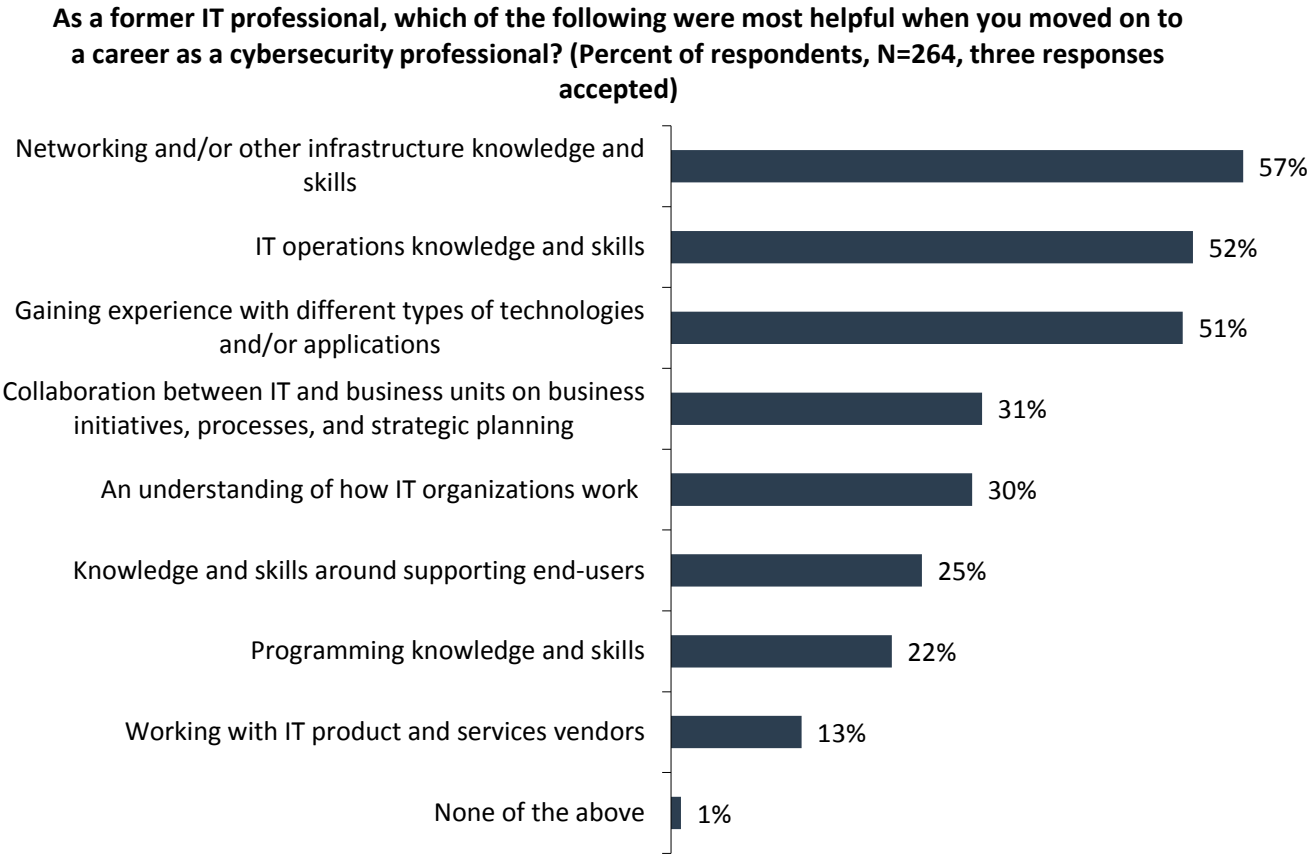
Figure 4. Did Respondents Start Career as an IT Professional?



Source: Enterprise Strategy Group and ISSA, 2017

IT professionals transitioning to a cybersecurity career come with a host of technical and organizational skills. Survey respondents point to the most important of these skills: More than half (57%) point to networking and/or other infrastructure knowledge, 52% say IT operations knowledge and skills, and 51% indicate gaining experience with different types of technologies (see Figure 7). Note the steep drop off from these 3 responses. It appears that IT technical and process experience is most important for a successful cybersecurity career. In this case, results varied from 2016 to 2017 (note that some responses were slightly modified between 2016 and 2017, see Table 1).

Figure 5. Factors Most Helpful in Moving to a Cybersecurity Career



Source: Enterprise Strategy Group and ISSA, 2017

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

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

Source: Enterprise Strategy Group and ISSA, 2017

Why do individuals choose to become cybersecurity professionals? Nearly half (47%) claim that a cybersecurity career presents them with the chance to use their skills and curiosity to address technical challenges, 37% say that a cybersecurity career was a natural career move from an IT job, and 36% indicate that they were attracted by the morality of the (cybersecurity) profession (see Figure 6). Note that financial opportunities associated with cybersecurity careers is far down the list. Clearly, most cybersecurity professionals aren't looking to get rich. Instead, they wanted a career choice that appealed to them from a technical and ethical perspective. Note that the top choices were consistent in 2016 and 2017.

Figure 6. Reasons for Becoming a Cybersecurity Professional

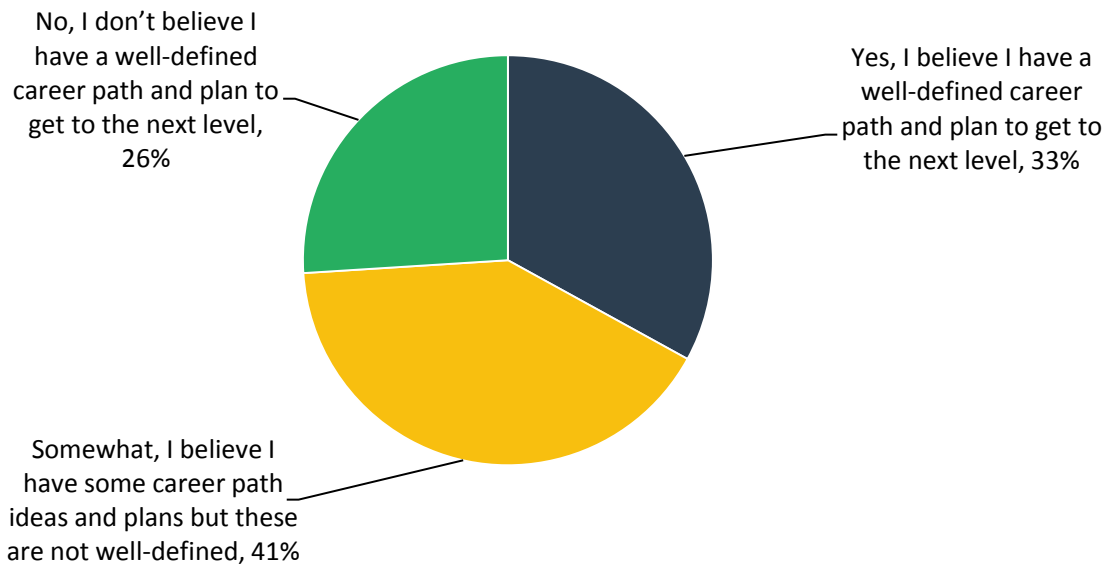
Source: Enterprise Strategy Group and ISSA, 2017

Cybersecurity careers can veer in many directions—toward business, compliance, operations, technology, etc. As a function of these choices and the day-to-day pace of their jobs, cybersecurity professionals can struggle with their career paths. While one-third of respondents claim to have a well-defined career path, two thirds remain confused about taking their career paths to the next level (see Figure 7).

Of those cybersecurity professionals looking for guidance, 42% believe that their career path would benefit from a combination of mentoring, a standardized career map, and additional technical training (see Figure 8). Note that the results were consistent in 2016 and 2017.

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

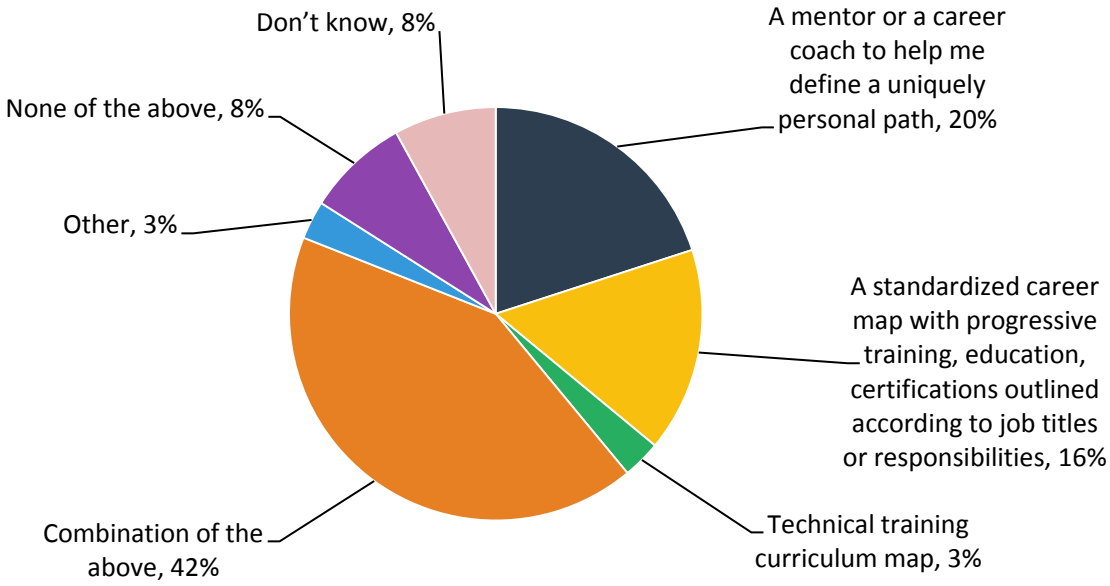
Do you believe you have a well-defined career path and plan to get to the next level?
(Percent of respondents, N=343)



Source: Enterprise Strategy Group and ISSA, 2017

Figure 8. Most Helpful Factors in Getting to the Next Level Career-wise

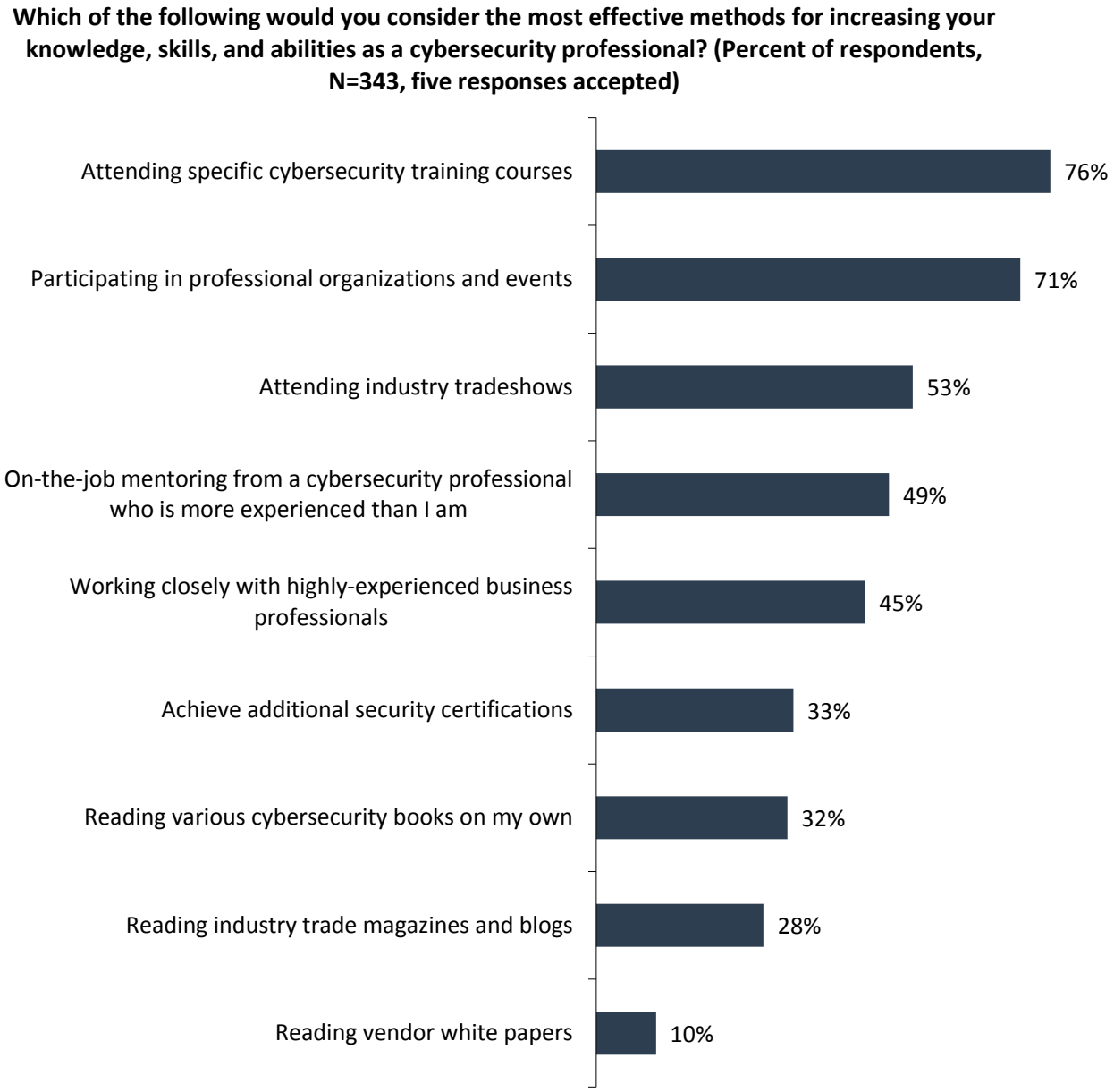
Which of the following would be the most helpful in getting to the next level career-wise?
(Percent of respondents, N=231)



Source: Enterprise Strategy Group and ISSA, 2017

Respondents were also asked their opinions on the most effective methods for increasing their cybersecurity knowledge, skills, and abilities (KSAs). More than three-quarters of the cybersecurity professionals surveyed equated KSA development to attending specific cybersecurity training courses (76%) while 71% thought participating in professional organizations would be helpful (see Figure 9). These two responses stood out from others. Note that the results were fairly consistent between 2016 and 2017.

Figure 9. Most Effective Methods for Increasing KSAs



Source: Enterprise Strategy Group and ISSA, 2017

Cybersecurity Certifications

As stated in Figure 15, 61% of ISSA members surveyed for this report believe that cybersecurity certifications are far more useful for getting a job than they are for doing a job. In other words, certifications get individuals in the door but once they are employed they rely on other KSAs, as described in Figure 9.

Which certifications have ISSA members achieved? In this year's survey, respondents were asked to write-in the answer to this question and the top responses are listed in Figure 10.

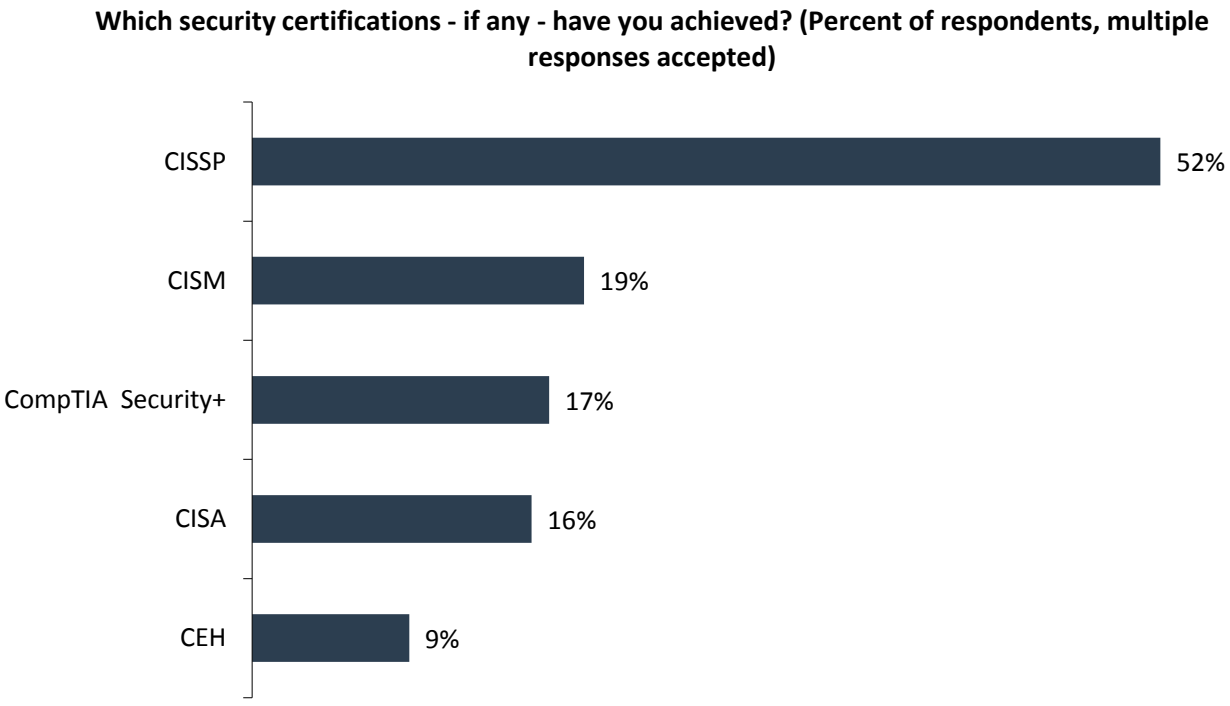
Of those certifications achieved, the most useful ones for getting a job are graphed in the figure below and compared to the results from 2016 (see Figure 11).

Once again, the data demonstrates a consistent conclusion. Cybersecurity professionals invest in CISSP certification as part of their career development. This appears to be a good investment as it helps them get a job and move forward with a cybersecurity career. What's troubling, however, is the decrease in value associated with all other certifications. In each case, the percentage of respondents claiming that an individual certification was useful for getting a job was lower than the percentage of respondents who'd achieved this certification.

Of course, specific certifications can demonstrate the end results of learning a new body of knowledge. For example, a cybersecurity professional with a CISSP may decide to pursue training in ethical hacking and then conclude this training by passing a Certified Ethical Hacker (CEH) test. In this case, however, the training and skill set, rather than the certification itself, are really what's important.

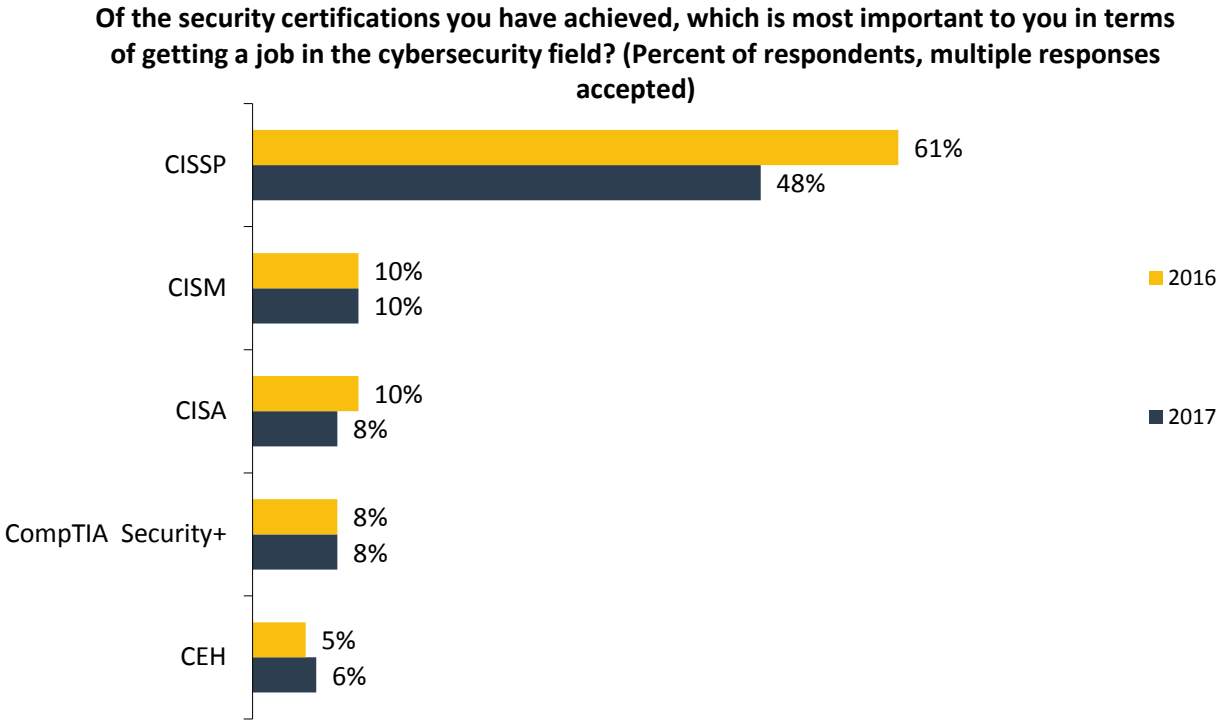
Given the number of certifications and the constant drumbeat of certification marketing, cybersecurity professionals may be tempted to fill their cards with acronyms as they achieve numerous security certifications. The ESG/ISSA data suggests that this is a myopic strategy. Cybersecurity professionals would be 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 and ISSA, 2017

Figure 11. Most Important Certifications to Get a Job

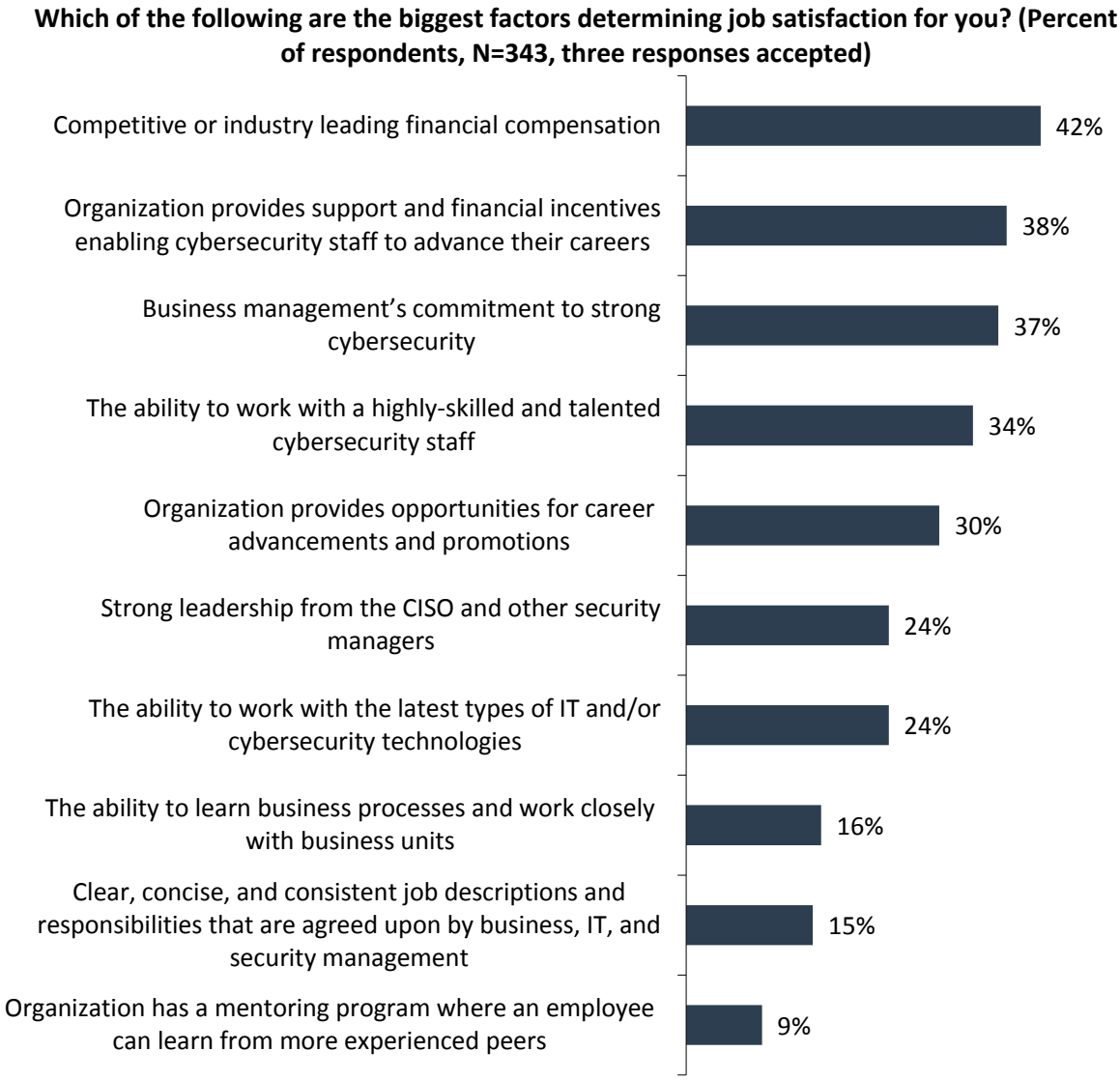


Source: Enterprise Strategy Group and ISSA, 2017

Cybersecurity Jobs

As described above, individuals become cybersecurity professionals to build upon their IT knowledge, satisfy their technical curiosity, and take a stance against cyber-adversaries. What do they look for when they join the cybersecurity ranks? Leading financial compensation is important, but cybersecurity pros also look for financial incentives for training and career development, an organization with a commitment to strong cybersecurity, and the ability to work with a highly skilled and talented cybersecurity staff (see Figure 12).

Figure 12. Factors Determining Job Satisfaction



Source: Enterprise Strategy Group and ISSA, 2017

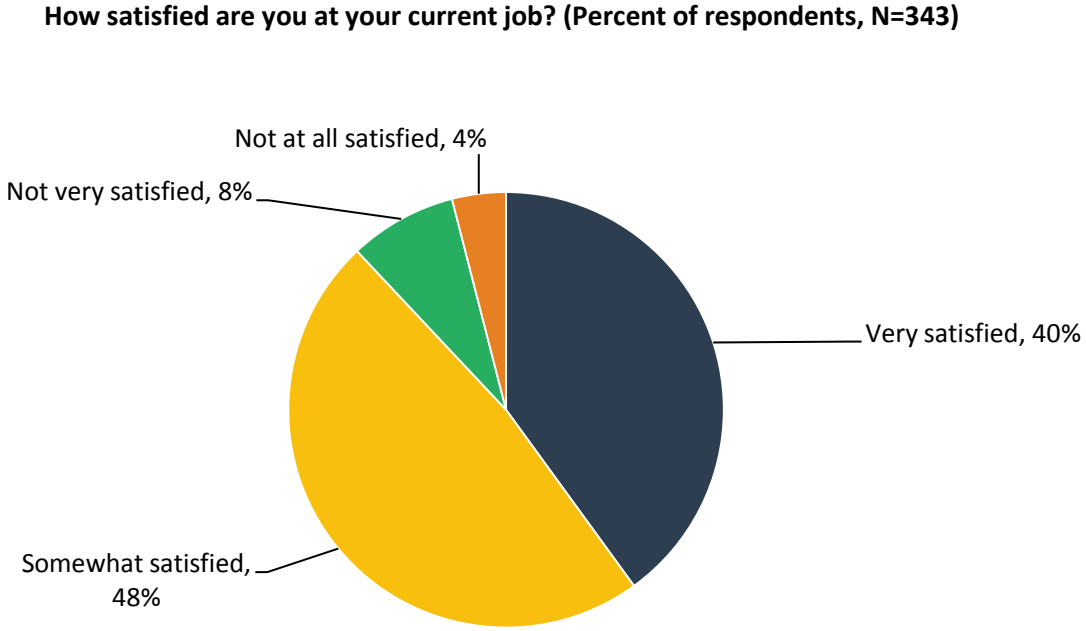
While many cybersecurity professionals remain enthusiastic about their career choice, they may not be as bullish about their current jobs. The ESG/ISSA report reveals that only 40% of survey respondents are very satisfied with their current job while 48% are somewhat satisfied, 8% are not very satisfied, and 4% are not at all satisfied (see Figure 13).

Based upon this data, it's safe to assume that most cybersecurity professional jobs lack some of the positive attributes described above. In other words, cybersecurity professionals are not receiving adequate incentives for career

development, business management does not have an appropriate commitment to cybersecurity, and cybersecurity professionals are not given ample opportunities to work with other highly skilled cybersecurity professionals.

Smart CISOs will survey the cybersecurity staff to gauge their level of job satisfaction and strive for continuous improvement in these and other areas.

Figure 13. Level of Satisfaction with Current Job



Source: Enterprise Strategy Group and ISSA, 2017

As previously discussed, cybersecurity career professionals depend upon a regimen of continuous training for three reasons:

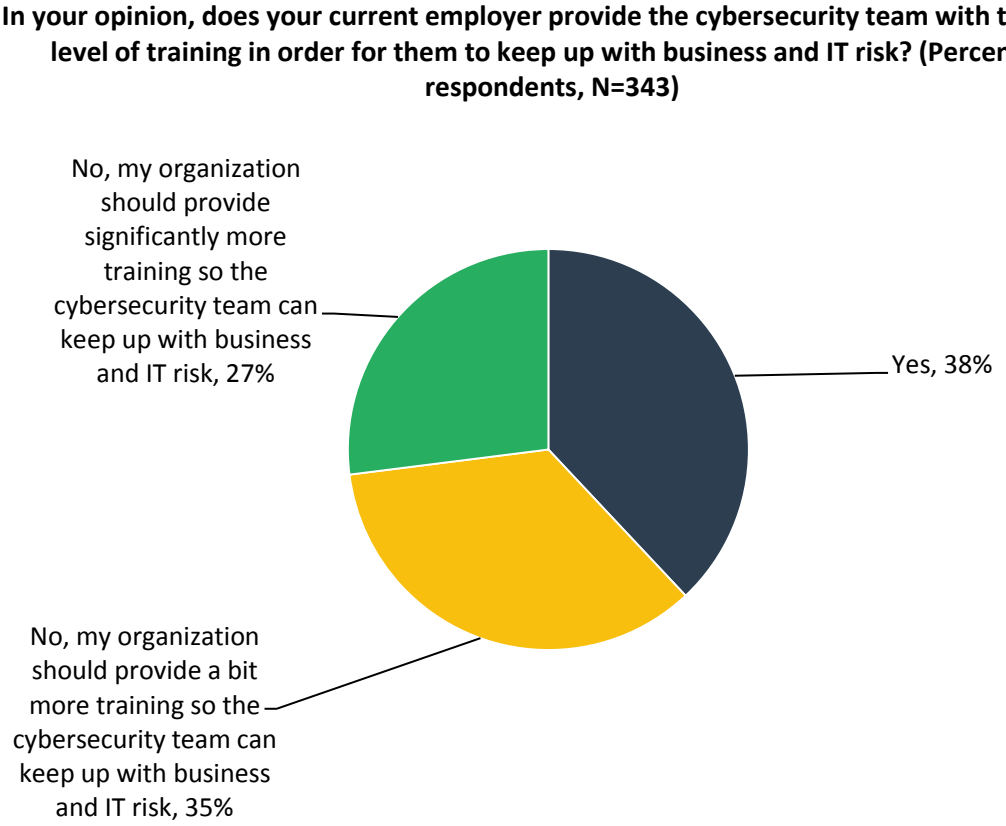
1. To align their skill sets with a constantly changing threat landscape
2. To develop their careers
3. To maintain job satisfaction

As previously described, skills development is also a critical component of overall job satisfaction.

Unfortunately, many organizations are not keeping up with an adequate level of cybersecurity training. More than one-third (35%) of ISSA members surveyed claim that their organizations should provide a bit more cybersecurity training while 27% believe their organizations should provide significantly more training (see Figure 14). Note that the results are consistent between 2016 and 2017.

Alarmingly, this data indicates that 62% of organizations are not providing the proper amount of training to keep up with business and IT risks. This should set off "red flags" for CEOs and corporate boards tasked with managing overall risk. Executives should assess whether their organizations fall into this category and then adjust their training investments and risk management strategies accordingly.

Figure 14. Training Provided to Keep Up with Business and IT Risk



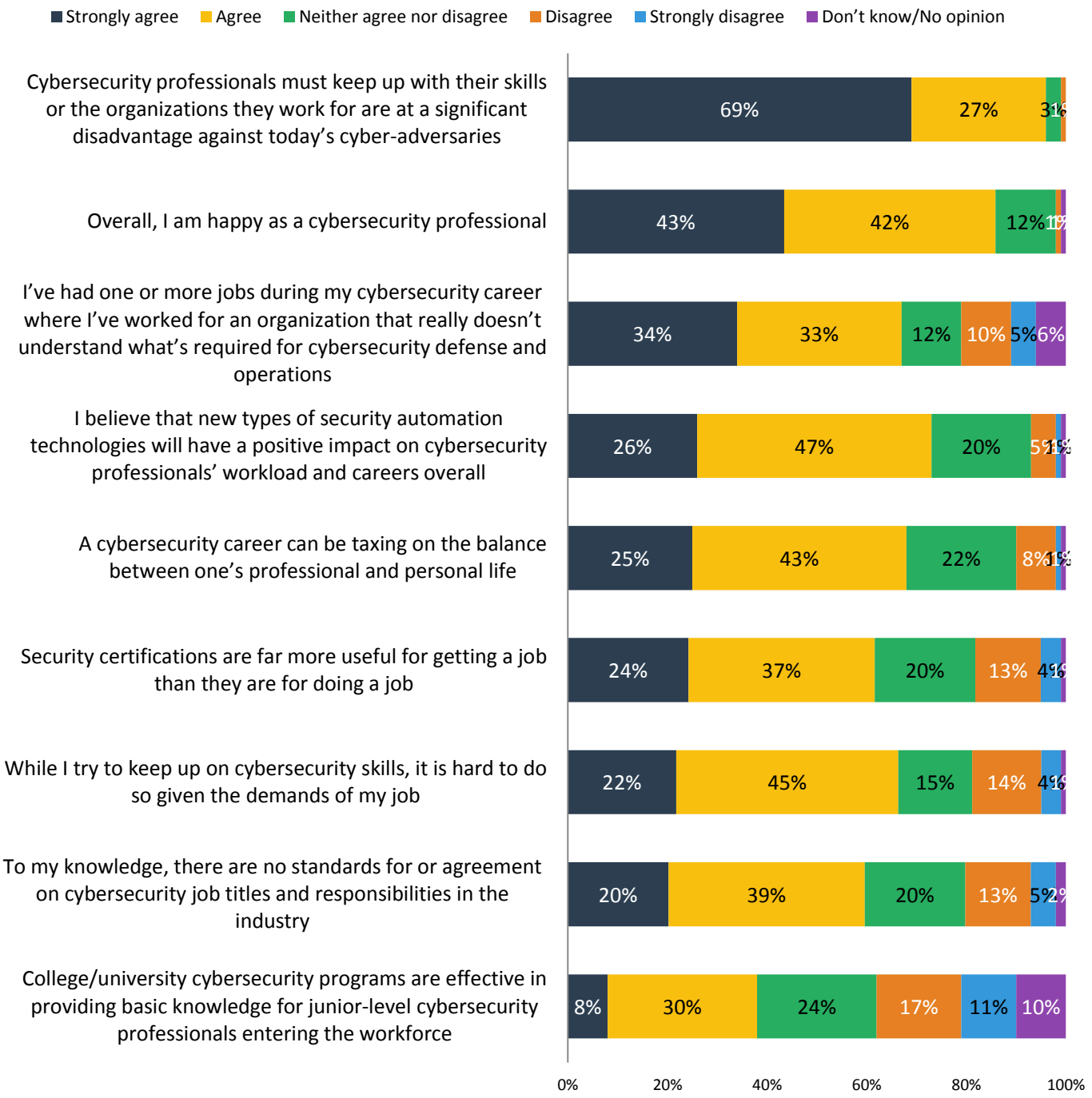
Source: Enterprise Strategy Group and ISSA, 2017

Survey respondents were presented with many statements and asked whether they agreed or disagreed with each (see Figure 15). This data provides some strong opinions on the state of cybersecurity professional careers. For example:

- 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. In other words, continuous staff training is a requirement for effective cyber-risk management.
- 85% of survey respondents strongly agree or agree that they are happy being cybersecurity professionals. This demonstrates their dedication and commitment to their role as network defenders.
- 73% of survey respondents strongly agree or agree that new types of security automation technologies will have a positive impact on cybersecurity workload and career development. This optimism is noteworthy as it represents a technical solution to help address the global cybersecurity skills shortage.
- 68% of survey respondents strongly agree or agree that a cybersecurity career can be taxing on the balance between one's professional and personal life. CISOs should monitor this situation to protect against employee burnout.
- 67% of survey respondents strongly agree or agree that while they try to keep up with their cybersecurity skills, it is hard to do so given their job's demands. This data point is troubling because 96% of cybersecurity professionals agree that keeping up with skills development is an essential countermeasure for addressing the evolving threat landscape. To mitigate this risk, CISOs must help key staff members find the time for advanced training.

Figure 15. Respondents' Sentiment on Various Cybersecurity Topics

Please select one response per row that best reflects your opinion on each statement.
(Percent of respondents, N=343)



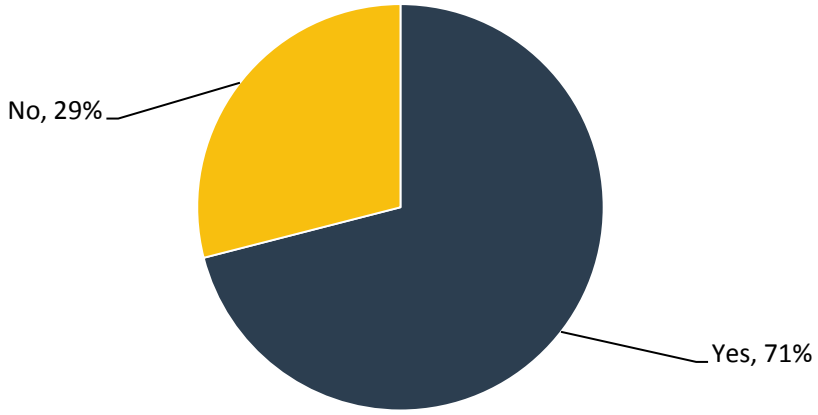
Source: Enterprise Strategy Group and ISSA, 2017

Cybersecurity Leadership

The majority of ISSA members surveyed work at organizations with a CISO (or equal position) employed (see Figure 16). Note that the results are consistent between 2016 and 2017. In most cases (55%), the CISO reports to a CIO or other senior IT person. Only 23% of CISOs report directly to a CEO, which is consistent with last year's survey results (22%, see Figure 17). Note that the results are consistent between 2016 and 2017.

Figure 16. Do Organizations Have a CISO/CSO?

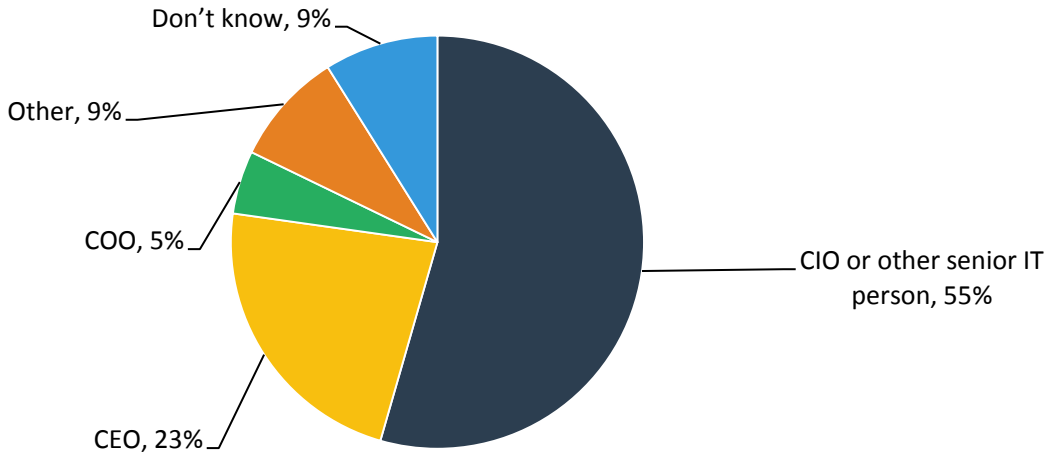
Does your organization have a Chief Information Security Officer (or similar position) in place today? (Percent of respondents, N=343)



Source: Enterprise Strategy Group and ISSA, 2017

Figure 17. To Whom Does the CISO/CSO Report?

Which of the following best represents to whom the CISO reports? (Percent of respondents, N=244)

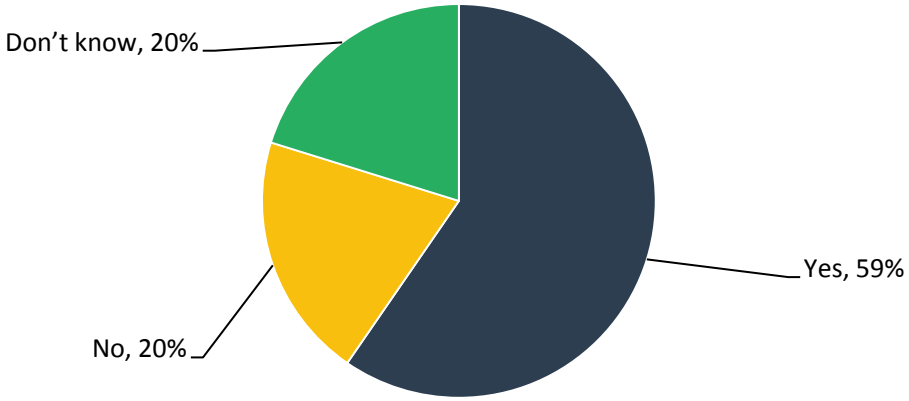


Source: Enterprise Strategy Group and ISSA, 2017

The CISO is an active participant with executive management and corporate boards in a majority of cases (59%, see Figure 18). Still, 20% of organizations seem to view the CISO as a technical manager and keep this person separated from business executives. Note that the results are consistent between 2016 and 2017.

Figure 18. Is CISO an Active Participant with Executive Management and Board of Directors?

Is your organization's CISO an active participant with executive management and the board of directors (or similar oversight group)? (Percent of respondents, N=244)

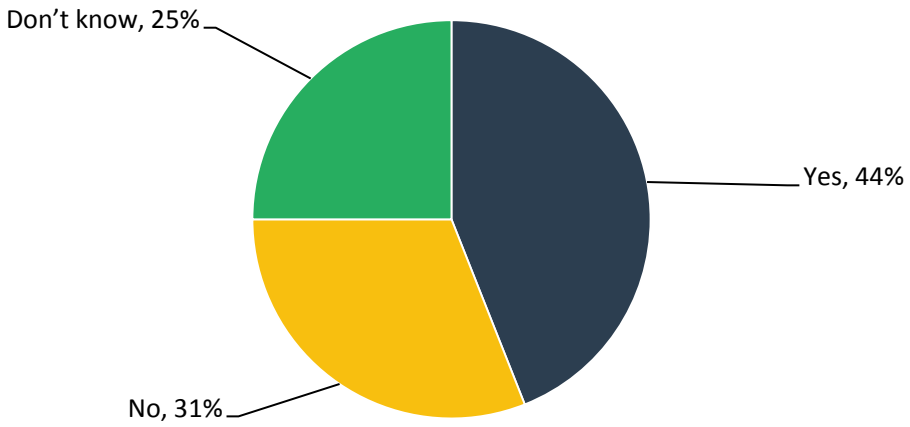


Source: Enterprise Strategy Group and ISSA, 2017

Over the past few years, cybersecurity has become a boardroom issue, making it noteworthy that less than half of survey respondents (44%) believe that their organization's CISO has an adequate level of participation with executive management and the board of directors (see Figure 19). Perhaps some CISOs don't have the right communications skills to address the board or, alternatively, some boards don't seek out counsel from CISOs as often as they should. Either of these situations is suboptimal and can lead to increased cyber-risk.

Figure 19. Is CISO Level of Participation with Executive Management and Board of Directors Adequate?

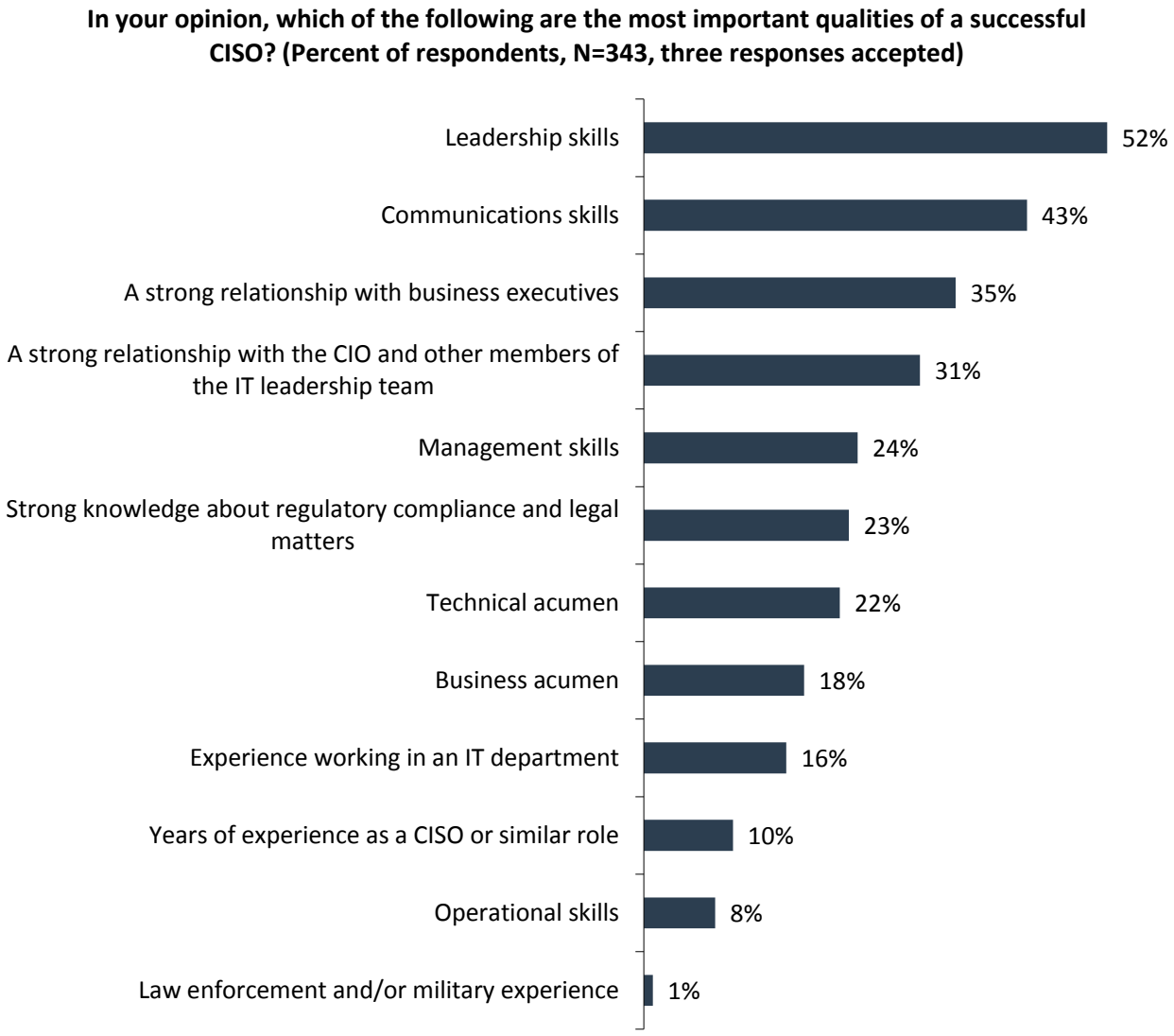
Do you think your CISO's level of participation with executive management and the board of directors is adequate? (Percent of respondents, N=244)



Source: Enterprise Strategy Group and ISSA, 2017

What qualities make a CISO successful? The top responses in 2017 align with those of 2016 ESG/ISSA research—namely, leadership skills, communications skills, a strong relationship with business executives, and a strong relationship with the CIO and IT leadership team (see Figure 20). Note that the results are consistent between 2016 and 2017.

Figure 20. Most Important Qualities of a Successful CISO

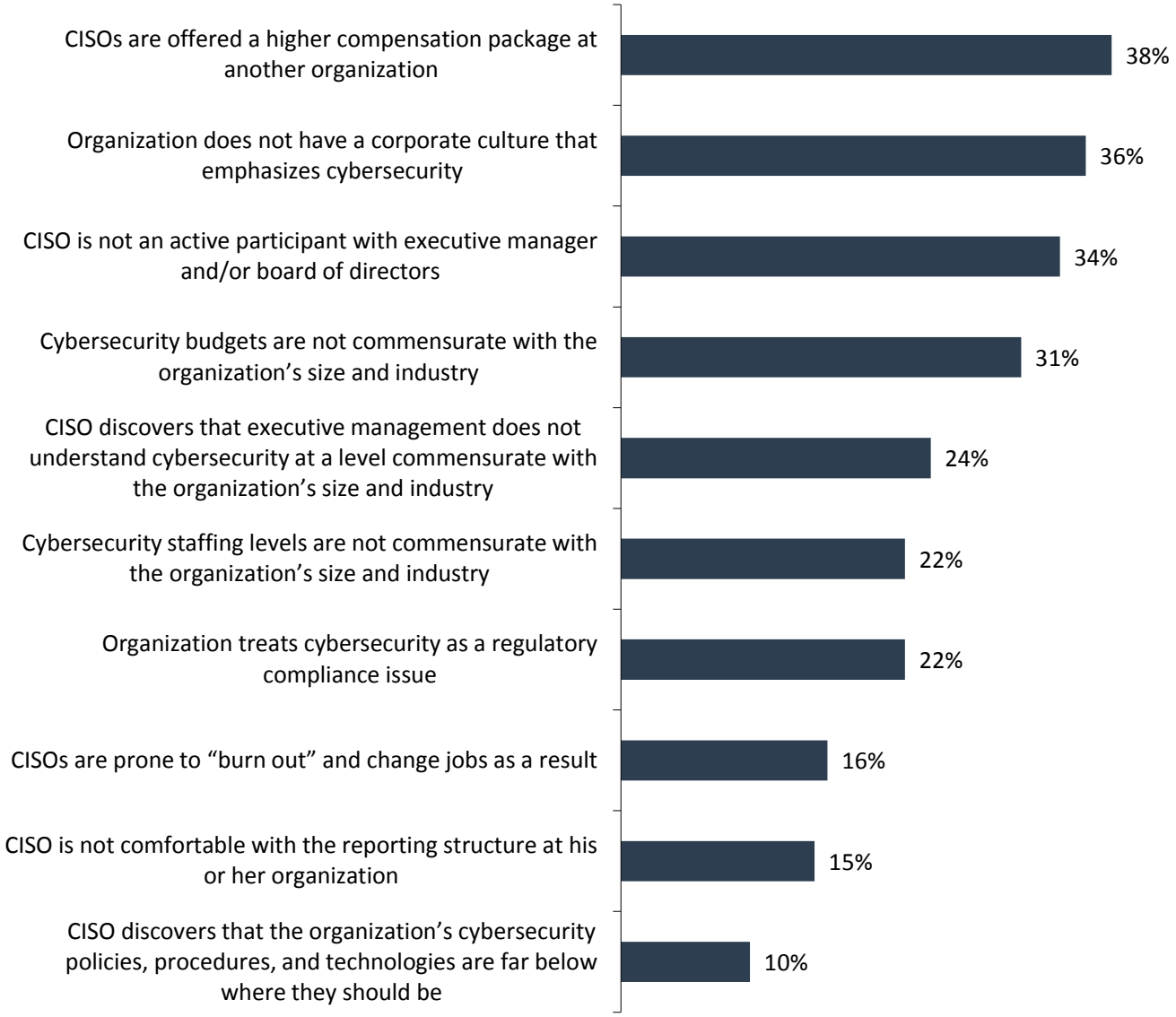


Source: Enterprise Strategy Group and ISSA, 2017

It is estimated that the average tenure of a CISO is approximately 24 to 48 months. Why is there such high attrition with security executives? Survey respondents were asked this question. Thirty-eight percent believe that CISOs leave for higher compensation packages, 36% say CISOs change jobs when their organizations do not have a corporate culture that emphasizes cybersecurity, and 34% say CISOs exit when he or she is not an active participant with executive management and/or the board of directors (see Figure 21). Note that the results are consistent between 2016 and 2017.

Figure 21. Factors Likely to Cause CISOs 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=343, three responses accepted)

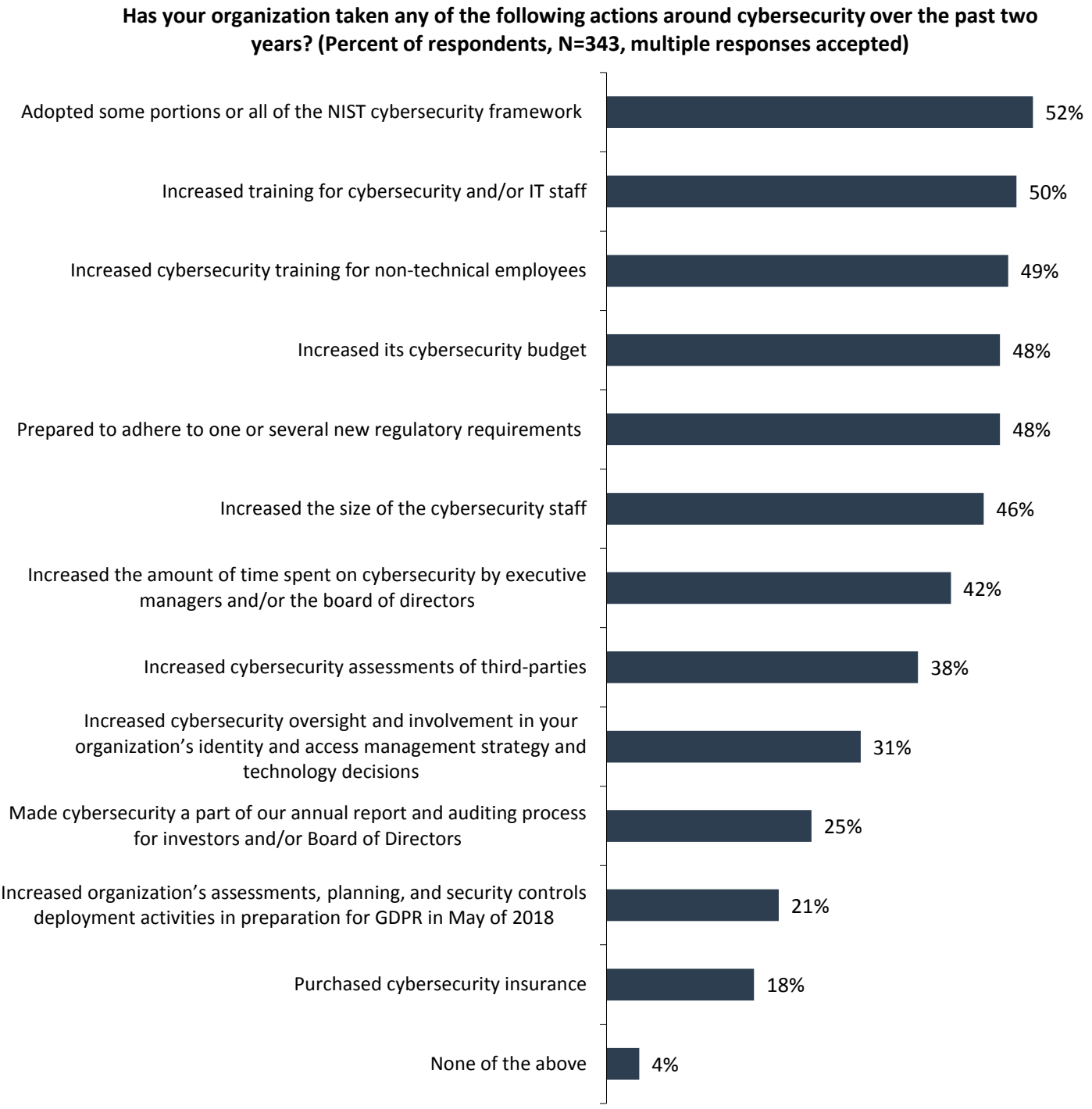


Source: Enterprise Strategy Group and ISSA, 2017

The State of Cybersecurity

Survey respondents were asked to identify cybersecurity actions taken over the past two years. Nearly half of all organizations have adopted some portion of the NIST cybersecurity framework (CSF), increased training for cybersecurity and/or IT staff, increased cybersecurity training for non-technical employees, increased their cybersecurity budget, and prepared to adhere to one or several new regulatory requirements (see Figure 22).

Figure 22. Actions Taken around Cybersecurity Over the Past Two Years



Source: Enterprise Strategy Group and ISSA, 2017

It is worth noting that the list of actions in 2017 differed from those of 2016 (see Table 2). It's likely that many organizations have taken all of these actions over the past 24 months.

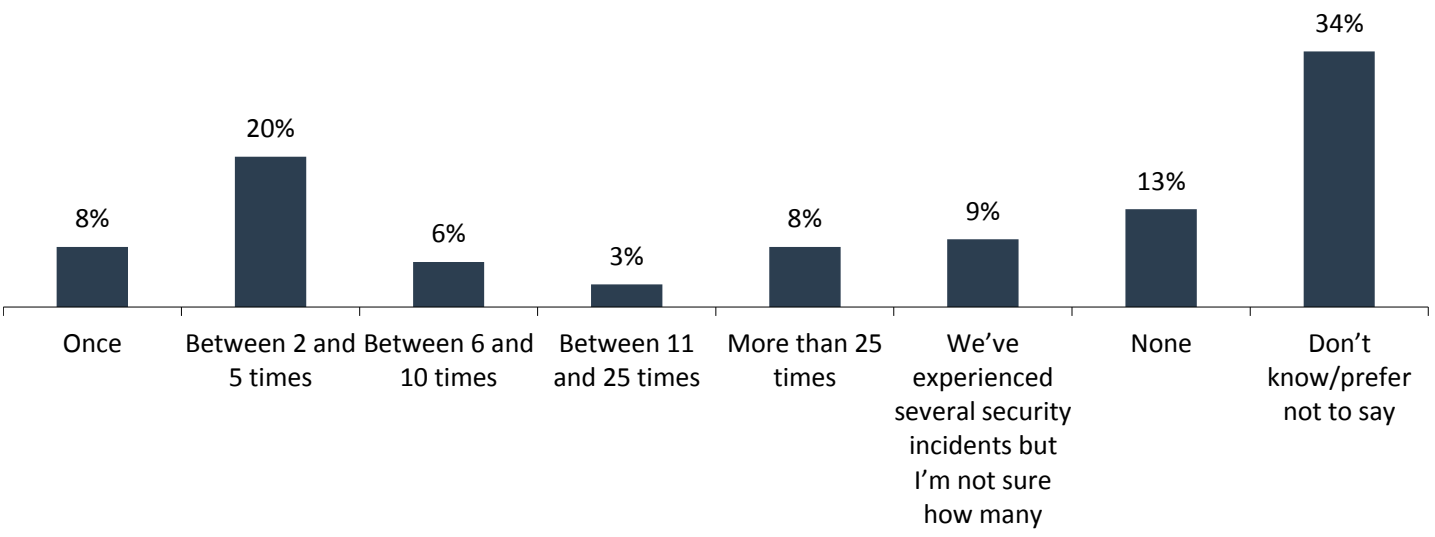
Table 2. Actions Taken around Cybersecurity by Year

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

Source: Enterprise Strategy Group and ISSA, 2017

Only 13% of organizations claim that they haven't experienced any security incidents over the past 2 years. Alternatively, 46% have experienced more than one incident (see Figure 23). It is interesting that more than one-third (34%) of respondents selected "don't know/prefer not to say," but security professionals often err on the side of discretion.

Figure 23. Frequency of Security Incidents over the Past Two Years



Source: Enterprise Strategy Group and ISSA, 2017

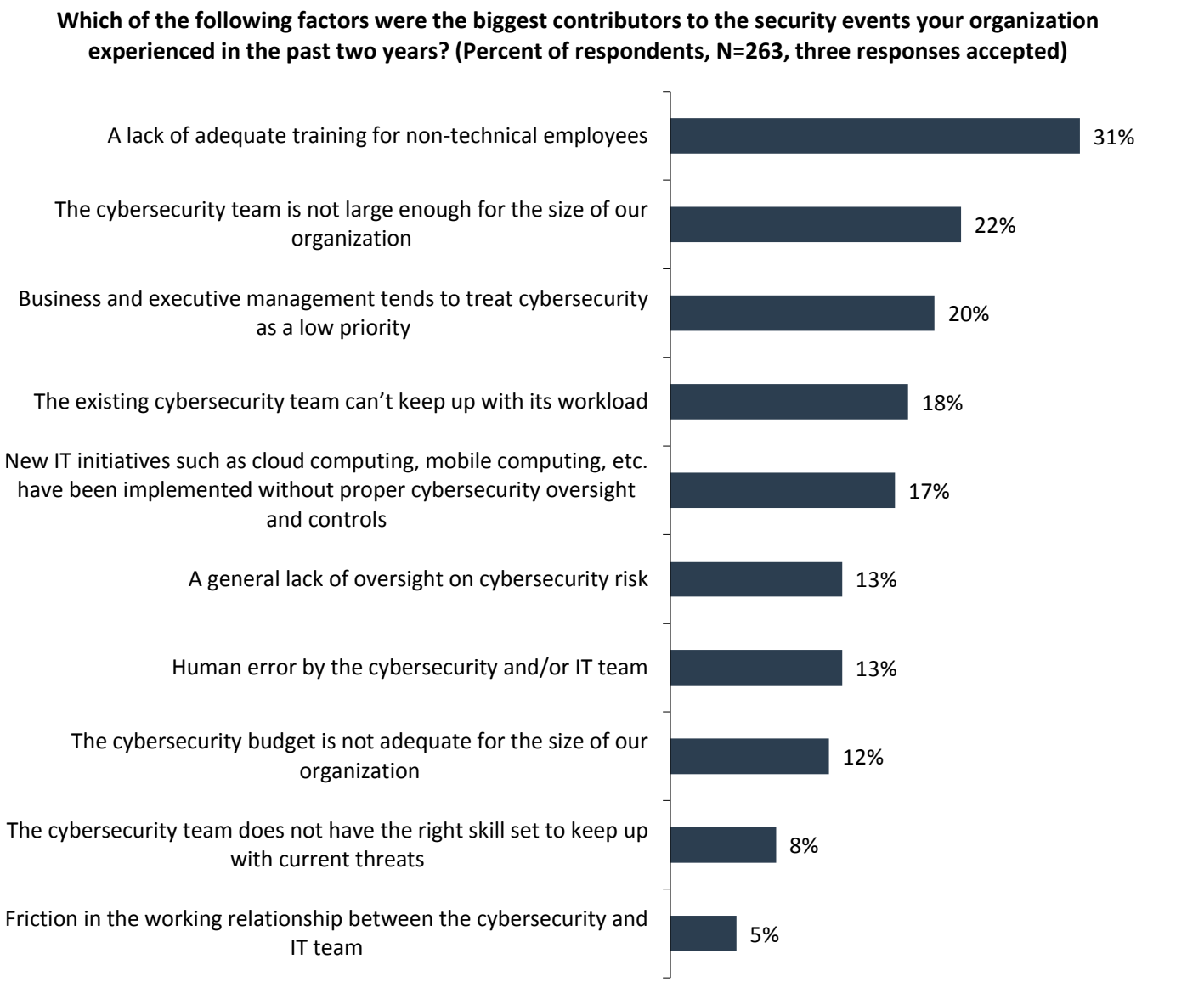
Respondents whose organization experienced at least one security incident were then asked to identify the biggest contributors to these events (see Figure 24). Cybersecurity professionals pointed to:

- A lack of adequate training for non-technical employees. This indicates that non-technical employees are doing things like downloading malicious files, clicking on malicious links, and falling for social engineering schemes like phishing

emails. CISOs should quantify the number of incidents occurring, the cost to remediate those incidents, and potential damages related to the incidents. These costs may more than offset the cost of more thorough end-user training.

- **An inadequately sized security team.** This data point is consistent with the global cybersecurity skills shortage impacting organizations of all sizes and across all industries. CISOs should assess skills and staffing gaps and look for services partners who can augment cybersecurity staff.
- **The fact that business and executive management tend to treat cybersecurity as a low priority.** This situation is especially demoralizing for cybersecurity professionals. As the data from this report indicates, organizations in this camp will likely experience high attrition rates as security staff members find other more fulfilling jobs elsewhere.

Figure 24. Biggest Contributors to Security Events Experienced



Source: Enterprise Strategy Group and ISSA, 2017

It is also worth noting that the list of contributing factors to security events in 2017 was consistent with the list from 2016 (see Table 3).

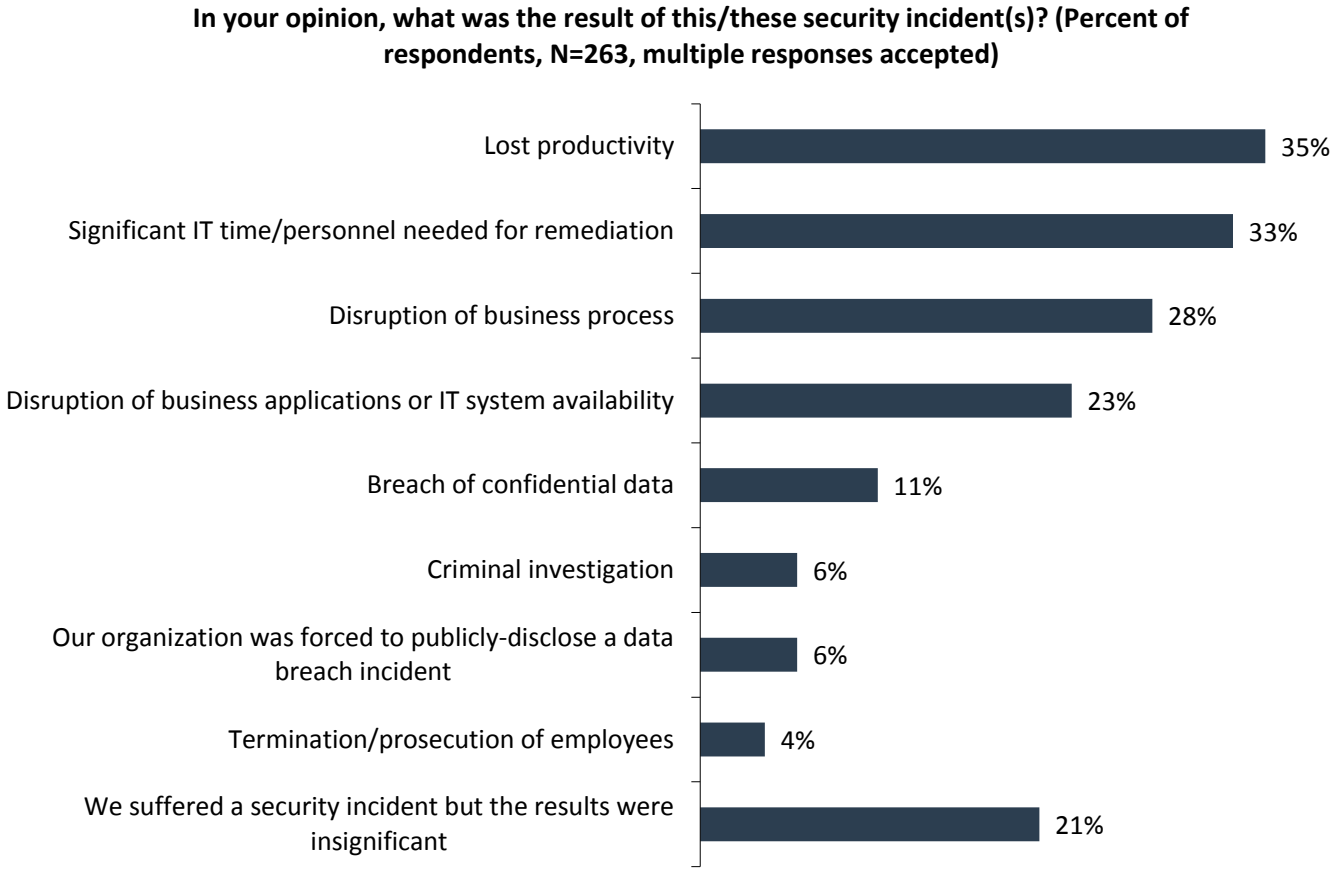
Table 3. Biggest Contributors to Security Events Experienced by Year

Top Four Contributing Factors in 2017	Top Four Contributing Factors in 2016
A lack of adequate training for non-technical employees	The cybersecurity team is not large enough for the size of our organization
The cybersecurity team is not large enough for the size of our organization	A lack of adequate training for non-technical employees
Business and executive management tend to treat cybersecurity as a low priority	Business and executive management tend to treat cybersecurity as a low priority
The existing cybersecurity team can't keep up with its workload	The cybersecurity budget is not adequate for the size of our organization

Source: Enterprise Strategy Group and ISSA, 2017

Even a single security incident can cause significant damage. Survey respondents pointed to ramifications from security incidents such as lost productivity, significant IT time/personnel needed for remediation, and disruption of a business process (see Figure 25).

Figure 25. Results of Security Incidents

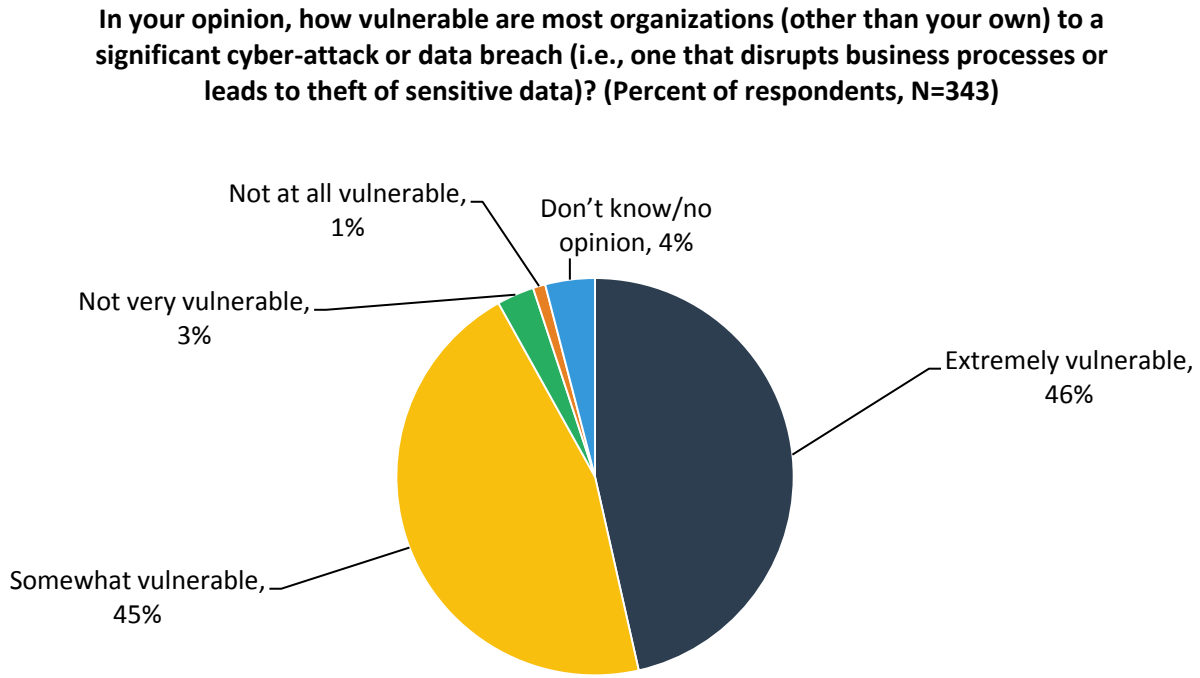


Source: Enterprise Strategy Group and ISSA, 2017

Cyber-attacks and data breaches at organizations like Adobe, Deloitte, Equifax, and Yahoo have become commonplace and cybersecurity professionals are on the frontline of this activity. Little wonder then why nearly half (46%) of survey respondents believe that most organizations are extremely vulnerable to a significant cyber-attack or data breach, while

another 45% believe that most organizations are somewhat vulnerable (see Figure 26). Note that the results are consistent between 2016 and 2017.

Figure 26. Vulnerability of Most Organizations to a Significant Cyber-attack or Data Breach

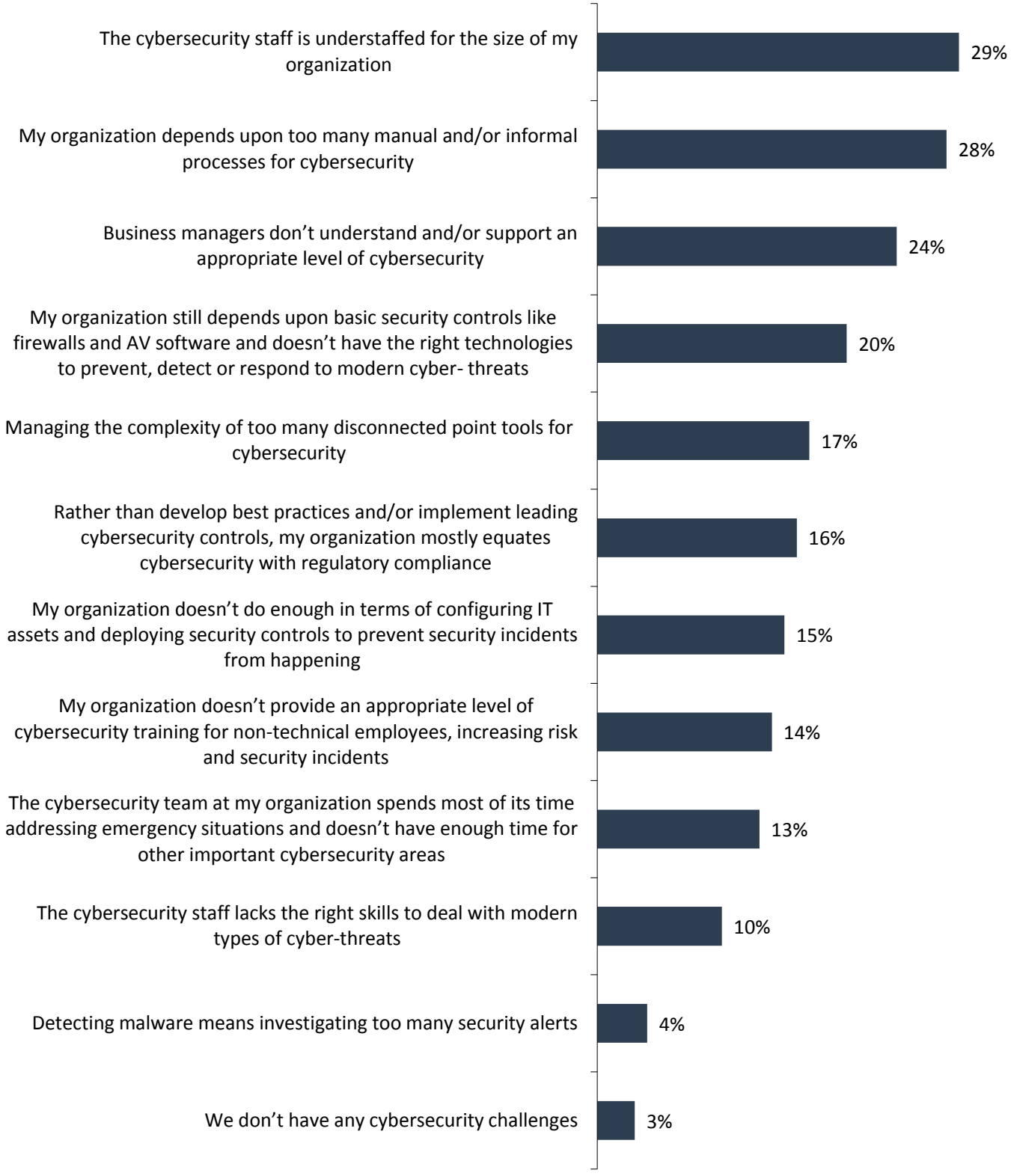


Source: Enterprise Strategy Group and ISSA, 2017

Cyber-attacks, data breaches, and security incidents are the product of a long list of cybersecurity challenges faced by all organizations. What are the biggest of these challenges? Once again, the data reveals problems associated with an undersized security staff but ISSA members surveyed also pointed to other challenges such as a reliance on manual processes, a lack of support from the business, and a dependence on basic security controls (see Figure 27).

Figure 27. Biggest Cybersecurity Challenges

Which of the following would you say are the biggest cybersecurity challenges at your organization? (Percent of respondents, N=343, three responses accepted)



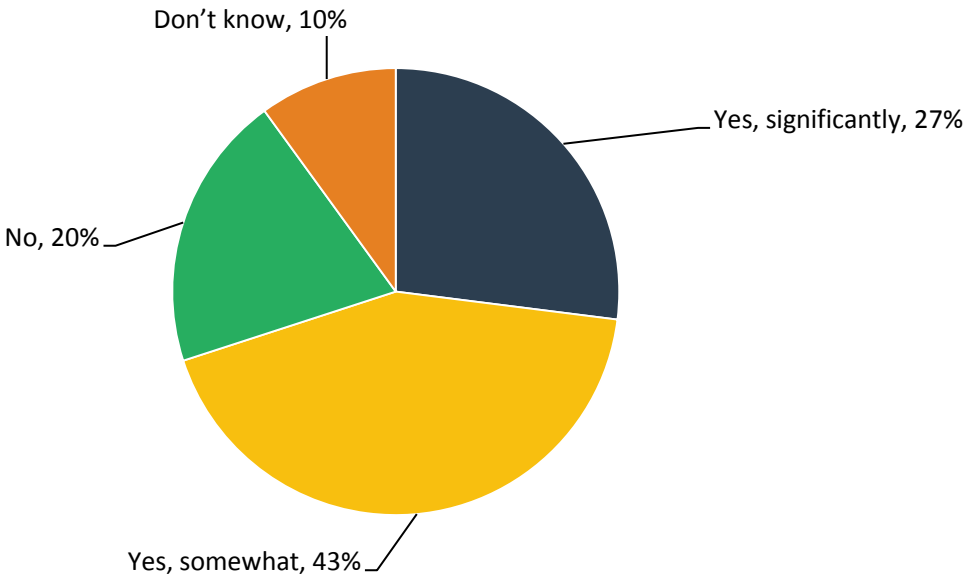
Source: Enterprise Strategy Group and ISSA, 2017

The Cybersecurity Skills Shortage

As in 2016, ESG and ISSA wanted to understand how the global cybersecurity skills shortage is impacting organizations. The short answer is that the impact is widespread, as 27% of cybersecurity professionals say that the cybersecurity skills shortage has had a significant impact on their organizations, while 43% claim that their organizations have been impacted somewhat by the global cybersecurity skills shortage (see Figure 28). These responses were similar to those of 2016 (29% said "significantly," 40% said "somewhat").

Figure 28. Level of Impact of 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=343)



Source: Enterprise Strategy Group and ISSA, 2017

As far as the specific consequences driven by the cybersecurity skills shortage, survey respondents point to an increased workload on existing staff, the need to hire and train junior employees rather than experienced professionals, and a focus on high-priority issues at the expense of planning, strategy, and training (see Figure 29). The top two results are similar to those of 2016 while the next two differ (see Table 4).

Figure 29. How Cybersecurity Skills Shortage Has Impacted Organizations

You indicated that the organizations you've worked for over the past few years were impacted by the global cybersecurity skills shortage. What type of impact did the global cybersecurity skills shortage have on these organizations? (Percent of respondents, N=238, multiple responses accepted)

Source: Enterprise Strategy Group and ISSA, 2017

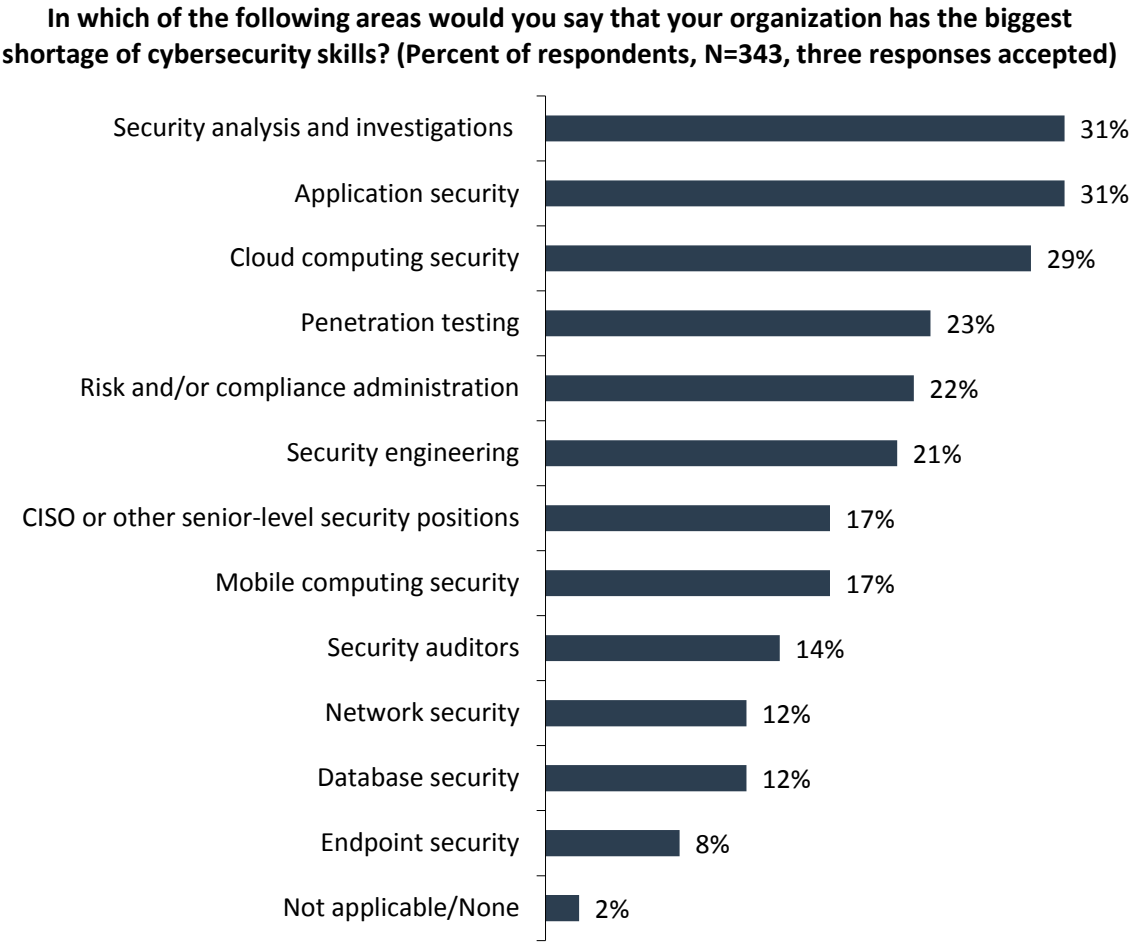
Table 4. How Cybersecurity Skills Shortage Has Impacted Organizations, by Year

Top Four Issues Associated with the Cybersecurity Skills Shortage 2017	Top Four Issues Associated with the Cybersecurity Skills Shortage 2016
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
Cybersecurity staff time is spent disproportionally on high priority events	Inability to utilize/learn some security technologies to their full potential
Cybersecurity team has limited time to work with business units	Higher attrition and turnover in cybersecurity staff

Source: Enterprise Strategy Group and ISSA, 2017

ESG/ISSA wanted to uncover areas where cybersecurity skills shortages were most acute. The research reveals that three areas stand out: Security analysis and investigations, application security, and cloud computing security (see Figure 30). These were also the top three areas identified in 2016.

Figure 30. Area(s) with Biggest Shortage of Cybersecurity Skills

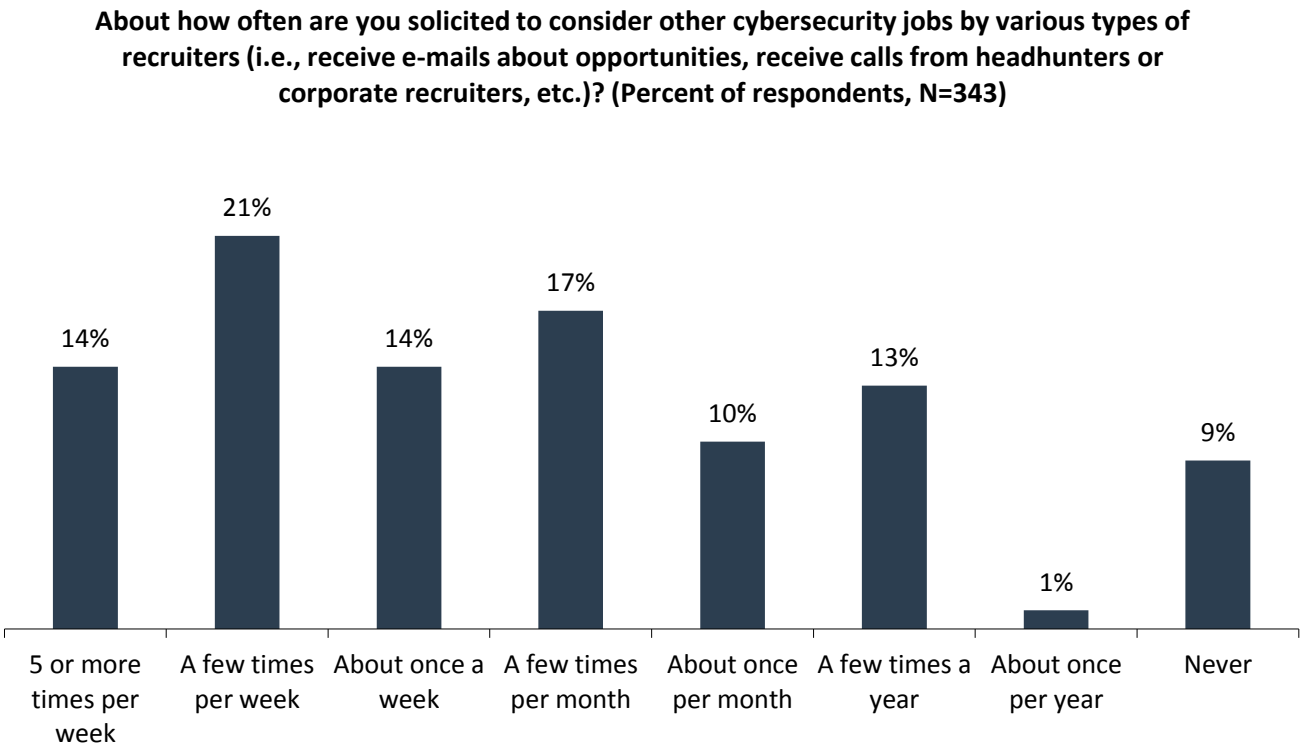


Source: Enterprise Strategy Group and ISSA, 2017

Note that 38% of survey respondents say that the cybersecurity skills shortage has led to high rates of employee burnout and employee attrition. This situation is exacerbated by the fact that there are more cybersecurity jobs than there are people to fill them.

This has led to a chaotic cybersecurity job market highlighted by salary inflation and aggressive recruiting tactics. Nearly half (49%) of survey respondents are actively solicited to consider other cybersecurity jobs at least once per week (see Figure 31). This rate is in line with last year's, results where 46% of cybersecurity professionals were recruited at least once per week.

Figure 31. Frequency of Solicitation by Job Recruiters

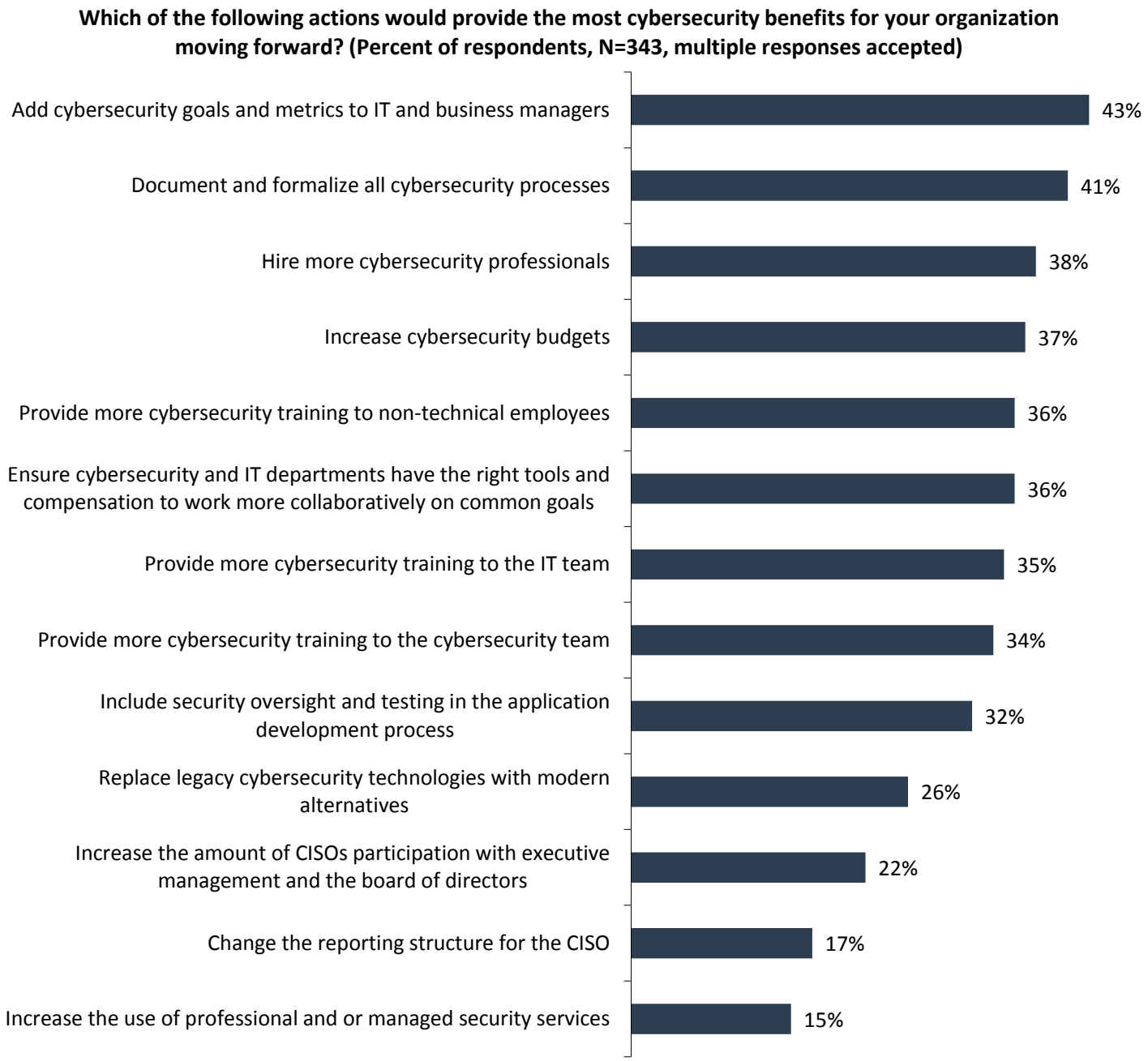


Source: Enterprise Strategy Group and ISSA, 2017

Cybersecurity Improvement

Finally, cybersecurity professionals were asked to identify the most beneficial cybersecurity actions their organizations could take in the future. As seen in Figure 32, the most commonly identified actions include adding cybersecurity goals and metrics to IT and business managers (43%), documenting and formalizing all cybersecurity processes (41%), and hiring more cybersecurity professionals (38%). In addition to highlighting the need to get the business and IT more involved and accountable for cybersecurity performance, respondents believe that security inefficiencies must be addressed through more formal and documented processes. And while hiring more employees could help the ongoing cybersecurity skills shortage, solutions like technology automation, SaaS offerings, and managed security services could serve as alternatives.

Figure 32. Actions That Would Provide the Most Cybersecurity Benefits to Organization



Source: Enterprise Strategy Group and ISSA, 2017

Conclusion

The ESG/ISSA report reveals several pervasive issues:

1. Many cybersecurity professionals are not managing their careers well.
2. The majority of cybersecurity professionals aren't receiving 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. Cybersecurity professionals are in high demand leading to a cycle of perpetual recruitment, high levels of attrition, and salary inflation.
4. The cybersecurity skills shortage is impacting the majority of organizations and placing an undue burden on existing infosec staff.
5. Too many organizations still treat security as a necessary evil rather than as part of business processes and culture.

Implications for Cybersecurity Professionals

Just as they did in 2016, cybersecurity professionals should use the research presented in this report as guidance 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:

- **Invest more time in career development.** The report reveals that most cybersecurity professionals don't have a well-defined career path and 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. This is especially true for junior cybersecurity professionals who have the opportunity to take their careers into emerging technical areas (i.e., cloud security, IoT security, etc.) or focus on business aspects of cybersecurity (i.e., risk management, CISO positions, etc.). Cybersecurity professionals should take the time to explore career possibilities, research appealing options, and map out a career progression to achieve their goals over time.
- **Look to training and peers rather than security certifications to improve cybersecurity KSAs.** Cybersecurity professionals should join professional organizations/user groups, attend industry events, and take specific hands-on training courses to maximize networking opportunities that can help them improve the skills they need for day-to-day excellence and long-term career development.
- **Develop business skills throughout your careers.** The research presented in this report reveals that many cybersecurity professionals tend to have limited understanding of the business aspects of cybersecurity. To increase career development, ambitious cybersecurity professionals should focus on business processes and objectives and then align them with risk management, cybersecurity controls, and continuous monitoring.
- **Take advantage of the sellers' market when appropriate.** Given the global skills shortage, underappreciated, bored, and overwhelmed cybersecurity professionals should take their skills elsewhere. Look for 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.** The ESG/ISSA data suggest that the majority of organizations will feel the impact of the cybersecurity skills shortage in one way or another. Therefore, cybersecurity professionals must assume that they will be short on people and skills. Smart infosec pros will plan for this reality with compensating

controls such as an increasing dependence on managed/professional services, process automation, and more use of advanced analytics technologies.

Research Implications for Employers

All organizations face competition to attract and retain cybersecurity talent. To recruit and retain the best cybersecurity talent, organizations should:

- **Recruit cybersecurity professionals from IT and beyond.** Most cybersecurity professionals start their cybersecurity careers in IT. With no end in sight for the global cybersecurity skill shortage, CISOs should create aggressive programs for recruiting IT talent interested in cybersecurity opportunities. Based upon the report data, it may be worthwhile to target candidates who've worked with multiple technologies, those with IT operations and networking technology experience, and those with a background of collaborating with business managers on IT initiatives. It may be helpful that cloud computing is placing many IT infrastructure jobs at risk. These IT administrators would make ideal candidates for cybersecurity. Smart CISOs will also look beyond IT alone and recruit individuals with business backgrounds as well. These individuals could help bridge the business/cybersecurity gap that exists in many organizations today.

- **Invest more in cybersecurity training.** Advancing the KSAs of the existing cybersecurity team and new recruits demands a commitment toward continuing education and training. Investing in leading cybersecurity training can improve the effectiveness of the current cybersecurity staff and lower overall risk to the business.

- **Provide career development advice and services.** CISOs should adopt programs and support services to help cybersecurity team members develop their careers. This should include mentoring programs as well as encouraging the cybersecurity team to participate in professional organizations. This effort will help improve the cybersecurity team's job satisfaction and longevity.

- **Assess job satisfaction within the cybersecurity department**. CISOs should survey the cybersecurity staff to assess job satisfaction levels and areas for improvement. If the organization has a strong commitment to cybersecurity, CISOs should be able to fine-tune problem areas like improving training and career development.

- **Anticipate cyber-attacks and data breaches.** Most organizations admit to at least one security incident over the past few years, though the numbers are likely a lot higher. In truth, organizations should expect to experience security compromises on an ongoing basis. This means that organizations need formal processes for incident response. Furthermore, these plans should extend beyond the IT domain to include business executives, legal counsel, HR managers, etc. For those looking for a template in this area, the NIST-800-61 Computer Incident Handling Guide can help.

- **Take the cybersecurity skills shortage into account as part of every initiative and decision.** The ESG/ISSA report reinforces previous data detailing the global cybersecurity skills shortage. It is now clear that CISOs should assume a cybersecurity personnel and skills deficit in each decision they make. For example, CISOs should:

    - Emphasize ease of use for all security technology purchases.
    - Initiate and push projects for security automation and orchestration that use technology to alleviate tedious manual processes.
    - Investigate, test, and deploy technologies offering advanced analytics technologies.
    - Find use cases for managed security services.

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 August 7, 2017 and September 13, 2017.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 343 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.

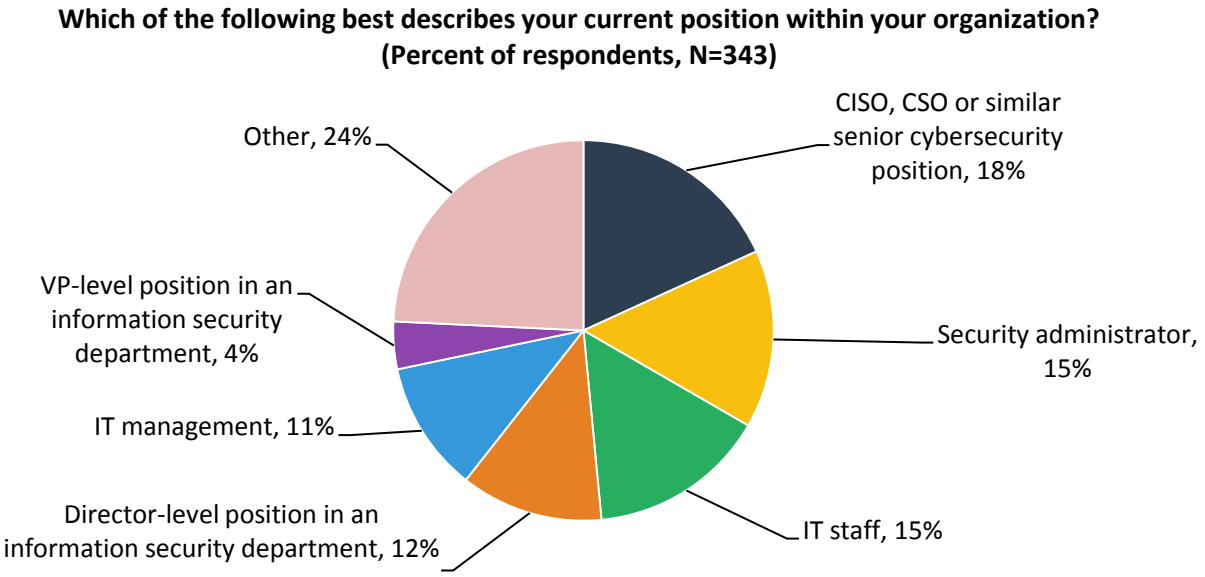
Respondent Demographics

The data presented in this report is based on a survey of 343 qualified respondents and cybersecurity professionals. Figures Figure 33Figure 36 detail the demographics of the respondent base at an individual and organizational level.

Respondents by Current Position

Respondents' current role is shown in Figure 33.

Figure 33. Respondents by Current Position

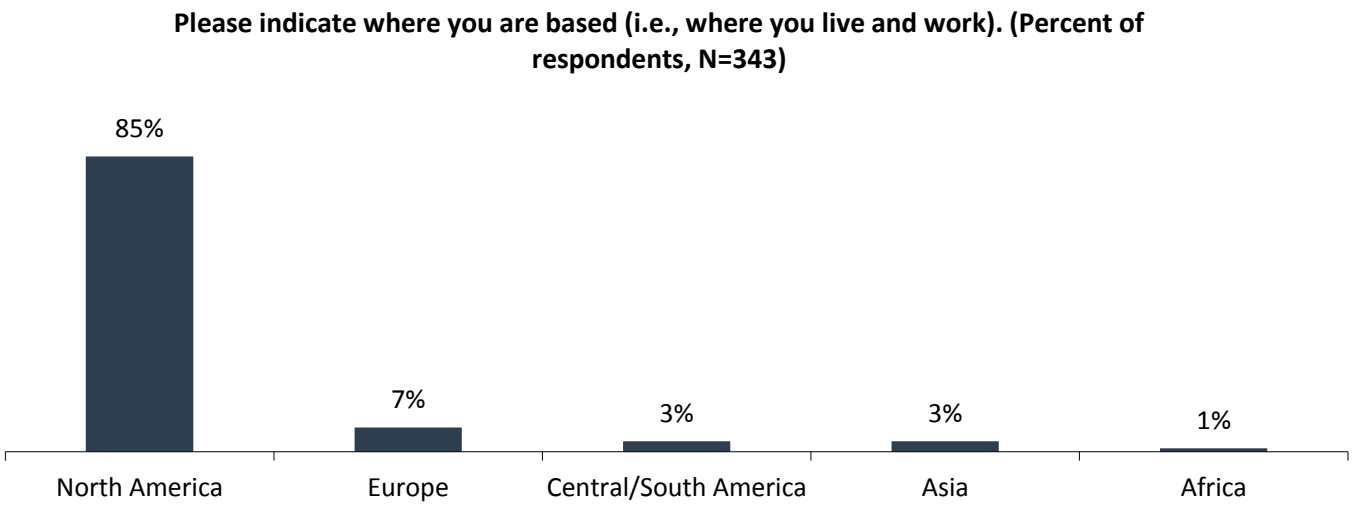


Source: Enterprise Strategy Group and ISSA, 2017

Respondents by Region

The regional breakdown of respondents is shown in Figure 34.

Figure 34. Respondents by Region

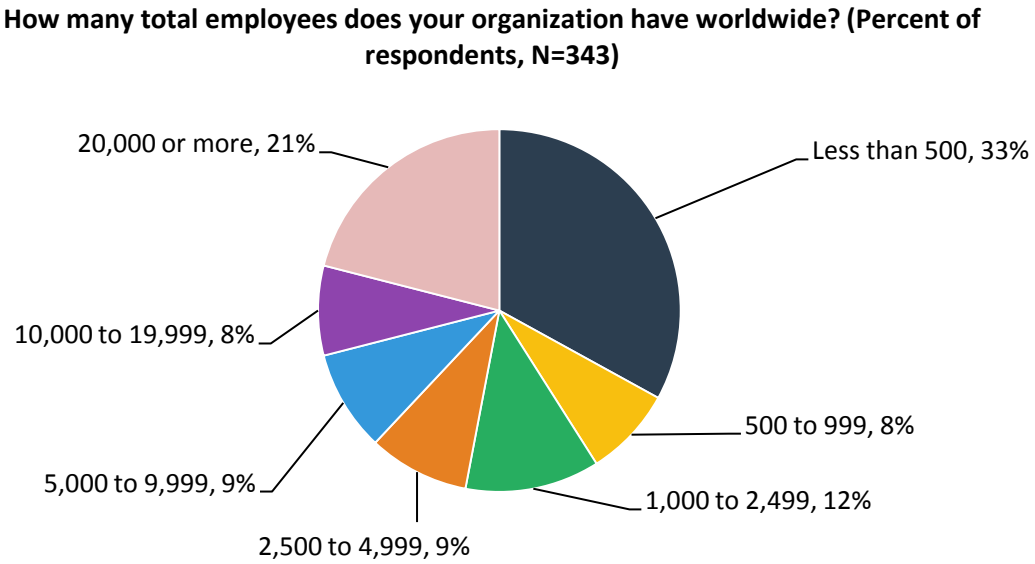


Source: Enterprise Strategy Group and ISSA, 2017

Respondents by Number of Employees

The number of employees in respondents' organizations is shown in Figure 35.

Figure 35. Respondents by Number of Employees

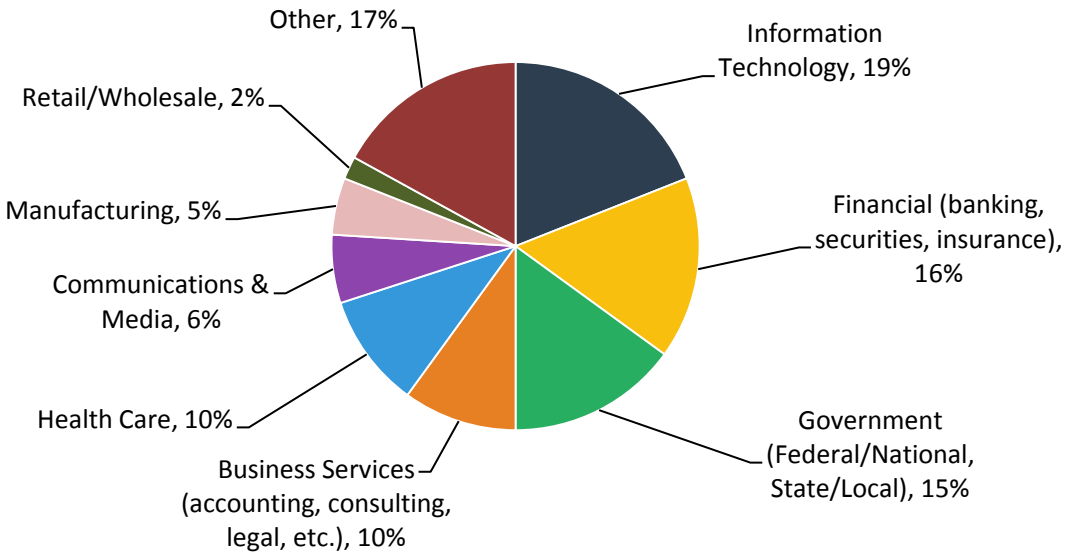


Source: Enterprise Strategy Group and ISSA, 2017

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 36.

Figure 36. Respondents by Industry



Source: Enterprise Strategy Group and ISSA, 2017

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

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