

RESEARCH REPORT

The Life and Times of Cybersecurity Professionals

Volume VII

By Jon Oltsik, Analyst Emeritus, and Bill Lundell, Senior Director of Syndicated Research
Enterprise Strategy Group

SEPTEMBER 2024



Contents

Executive Summary	3
Report Conclusions	3
Introduction.....	4
Research Objectives	4
Research Findings	5
Cybersecurity Professionals Face Growing Challenges in Their Field	5
Job Satisfaction in Cybersecurity Is More Than Just a Paycheck.....	8
Boosting Cybersecurity Programs Calls for More Training and a Cultural Shift.....	12
The Cybersecurity Skills Gap Remains, With Companies Lagging in Effective Responses	17
CISO Success Hinges on Top Notch Leadership and Communications Skills	21
Conclusion	25
Research Methodology	26
Respondent Demographics	27

Executive Summary

Report Conclusions

TechTarget's Enterprise Strategy Group conducted an in-depth survey of 369 IT and cybersecurity professionals who are currently part of the Information Systems Security Association (ISSA) member list. Respondents represented organizations of all sizes across the globe.

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

- **Cybersecurity professionals face growing challenges in their field.** A majority of cybersecurity professionals believe that working as a cybersecurity professional has become more difficult over the past two years, with nearly three-quarters citing both the increasing complexity and workloads associated with cybersecurity as a reason. Compounded by other factors like working with disinterested business managers, finding out about IT initiatives or projects after they are well underway, and constantly responding to emergencies, it's no wonder that more than half of those surveyed claim their job is stressful at least half the time.
- **Job satisfaction in cybersecurity is more than just a paycheck.** More than four in ten survey respondents reported that they are *very satisfied* with their current jobs. The leadership team's commitment to strong cybersecurity was the most common factor in determining job satisfaction, followed by such considerations as organizational support and financial incentives for career advancement, strong leadership from the CISO and other security managers, and the ability to work with highly skilled and talented cybersecurity staff. Despite relatively high job satisfaction levels, more than one-third of cybersecurity professionals have considered leaving the profession all together, while more than two-thirds have considered leaving their current job. The reasons for leaving the cybersecurity profession are not surprising, including the high stress associated with a cybersecurity career, a lack of a cybersecurity commitment from the leadership team, difficulties managing a work/life balance, and a lack of clear career advancement opportunities.
- **Boosting cybersecurity programs calls for more training and a cultural shift.** When asked to rate their organization's cybersecurity culture, more than one-third of respondents said their organization's cybersecurity culture is advanced, 41% indicated that their organization's cybersecurity culture is average, and 24% claim their organization's cybersecurity culture is fair or poor. In a progressive organization, cybersecurity is everyone's job, so it follows that nearly one-third of cybersecurity professionals estimate that their IT staff performs more than half of all cybersecurity tasks on a day-to-day basis. Improving cybersecurity programs requires, among other things, additional training and a culture shift. Cybersecurity professionals believe the creation or improvement of a cybersecurity culture can be accomplished by making managers more accountable for cybersecurity performance and generally aligning business initiatives and processes with the appropriate security policies, controls, and oversight.
- **The cybersecurity skills gap remains, with companies lagging in effective responses.** Nearly two-thirds of cybersecurity professionals claim that their organization has been impacted by the cybersecurity skills shortage. Of those organizations affected, more than half say the skills shortage has increased workloads on existing staff, while four in ten claim that the skills shortage has led to an inability to fully learn or utilize some security technologies to their full potential. In addition to increasing compensation, cybersecurity professionals believe their organization could address the skills shortage by better educating HR and recruiters on their cybersecurity needs and associated recruiting strategies.
- **CISO success hinges on top-notch leadership and communications skills.** While nearly two-thirds of respondents report that their CISO regularly interacts with the board of directors, just more than half said this level of interaction was adequate. Nearly three-quarters of respondents claim that their CISO is very effective or effective, though there is a strong correlation between effectiveness and level of interaction with executives and board members. Additionally, mastering communication and leadership skills remains paramount for CISOs to thrive in their roles and drive meaningful cybersecurity outcomes for their organizations.

Introduction

Research Objectives

The seventh annual *Life and Times of Cybersecurity Professionals* study continues to pinpoint many of the same issues as past editions, underscoring persistent challenges such as rising cyberthreats, IT complexity, ubiquitous vulnerabilities, heavy workloads, and difficulties embedding cybersecurity into organizational processes and cultures. Beyond illustrating cybersecurity problems, this year's edition highlights specific areas where cybersecurity professionals suggest ways their organizations can alleviate the burdens on cybersecurity practitioners while simultaneously bolstering defenses and reducing risks.

Above all, the report's most significant revelation is a crisis in cybersecurity leadership as organizations don't provide adequate support for their cybersecurity programs or the professionals tasked with executing them. This is evident in areas like inadequate training of non-cybersecurity staff, the lack of integration between cybersecurity and other business functions, and ineffective human resources efforts to recruit specialized cybersecurity talent. Overall, the survey findings reveal immense pressures on CISOs and emphasize the urgent need for them to have a stronger voice at the highest levels of their organizations to advocate for necessary changes on each of these fronts.

This serves as the seventh such research project, dating back to 2016. All references to previous Enterprise Strategy Group and ISSA research in this report can be found in [*The Life and Times of Cybersecurity Professionals Volume VI*](#).

This study sought to answer the following questions:

- Why has working as a cybersecurity professional become more difficult today than it was two years ago?
- How satisfied are cybersecurity professionals at their current jobs? What are the biggest factors for determining their level of job satisfaction?
- How likely are cybersecurity professionals to leave their current job in 2024 for any reason, including retirement, career change, and leaving for another cybersecurity job?
- How do cybersecurity professionals characterize the stress level typically associated with their careers? What are the most stressful aspects of jobs or careers as a cybersecurity professional?
- What actions do cybersecurity professionals believe would be the most helpful for the advancement of their careers?
- How would cybersecurity professionals characterize the cybersecurity culture at their organization?
- How has the global cybersecurity skills shortage impacted cybersecurity professionals' organizations? How do respondents think that has changed over the last two years? What actions do cybersecurity professionals believe could be taken to address the impact of the cybersecurity skills shortage?
- How would cybersecurity professionals characterize the working relationships between their organization's cybersecurity and IT departments and between cybersecurity and lines-of-business groups?
- Which actions do cybersecurity professionals believe their organization could take to improve cybersecurity programs?
- Do cybersecurity professionals believe their CISO regularly meets with executive management and the board of directors? Do they think the level of their CISO's participation with executive management and the board of directors is adequate?

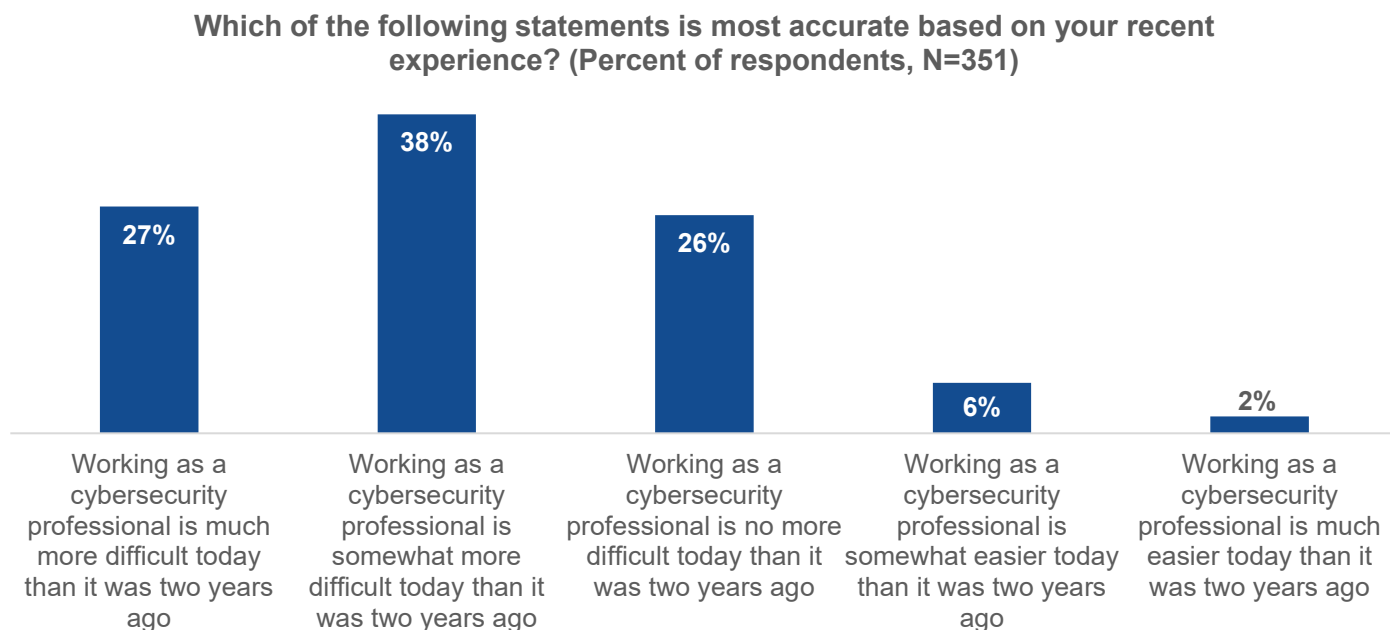
Survey participants represented a wide range of industries including manufacturing, technology, financial services, and retail/wholesale. For more details, please see the Research Methodology and Respondent Demographics sections of this report.

Research Findings

Cybersecurity Professionals Face Growing Challenges in Their Field

Cybersecurity careers seem to grow more difficult each year. Indeed, according to Figure 1, nearly two-thirds (65%) of respondents claim that working as a cybersecurity professional is more difficult than it was two years ago, similar to 2023 where 63% offered a similar response.

Figure 1. Cybersecurity Careers Are Not Getting Any Easier

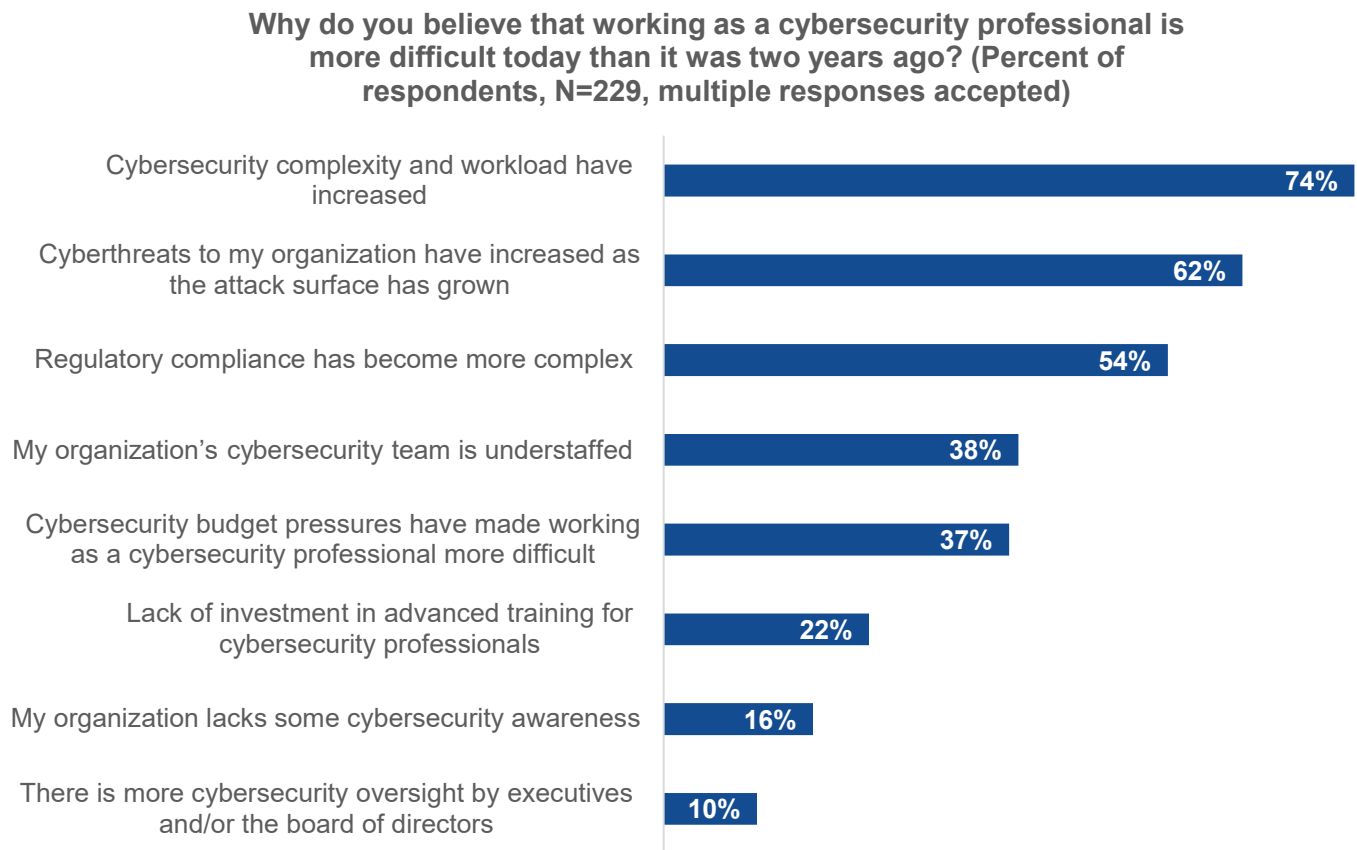


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

What are the biggest drivers behind this trend? Cybersecurity professionals face growing career difficulties due to various factors, including complex workloads, targeted threats, a growing attack surface, and regulatory compliance complexity overhead (see Figure 2). Rapid technology evolution and adoption also introduce new vulnerabilities and attack vectors at an unprecedented pace, requiring continuous learning and adaptation from cybersecurity teams. Staff and skill shortages often burden these teams as well.

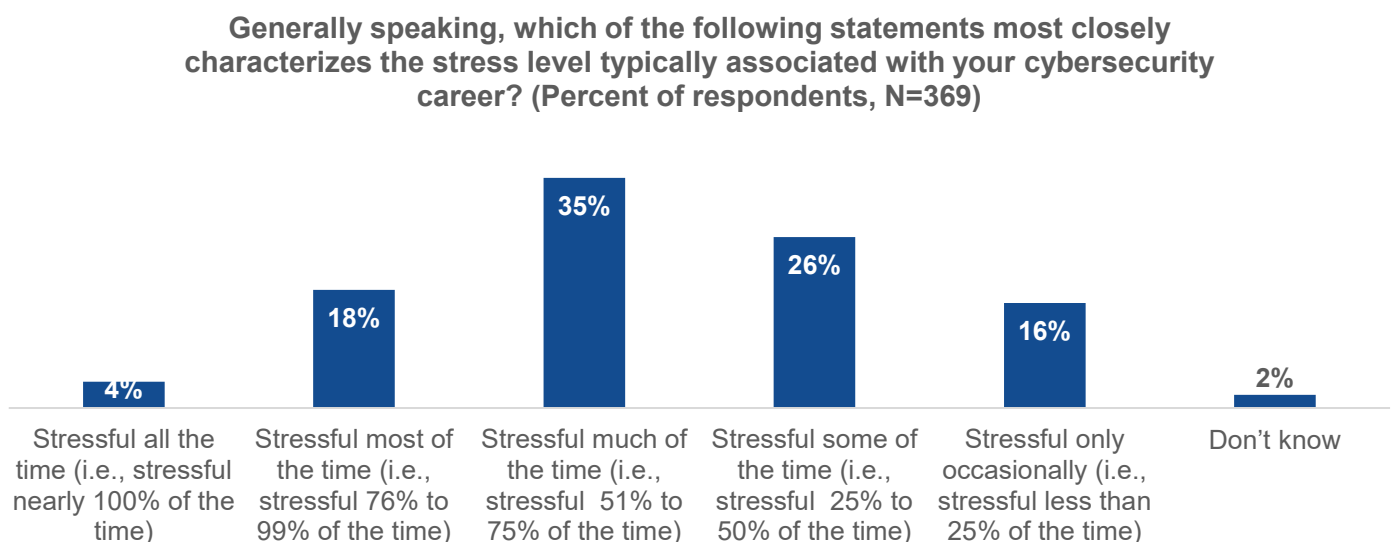
All of these challenges and issues cybersecurity professionals must contend with on a regular basis are often very stressful. Indeed, when asked, more than half (57%) of those surveyed claim their job is stressful at least half the time, slightly higher than 2023 (see Figure 3).

Figure 2. Reasons Being a Cybersecurity Professional Is More Difficult Today



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

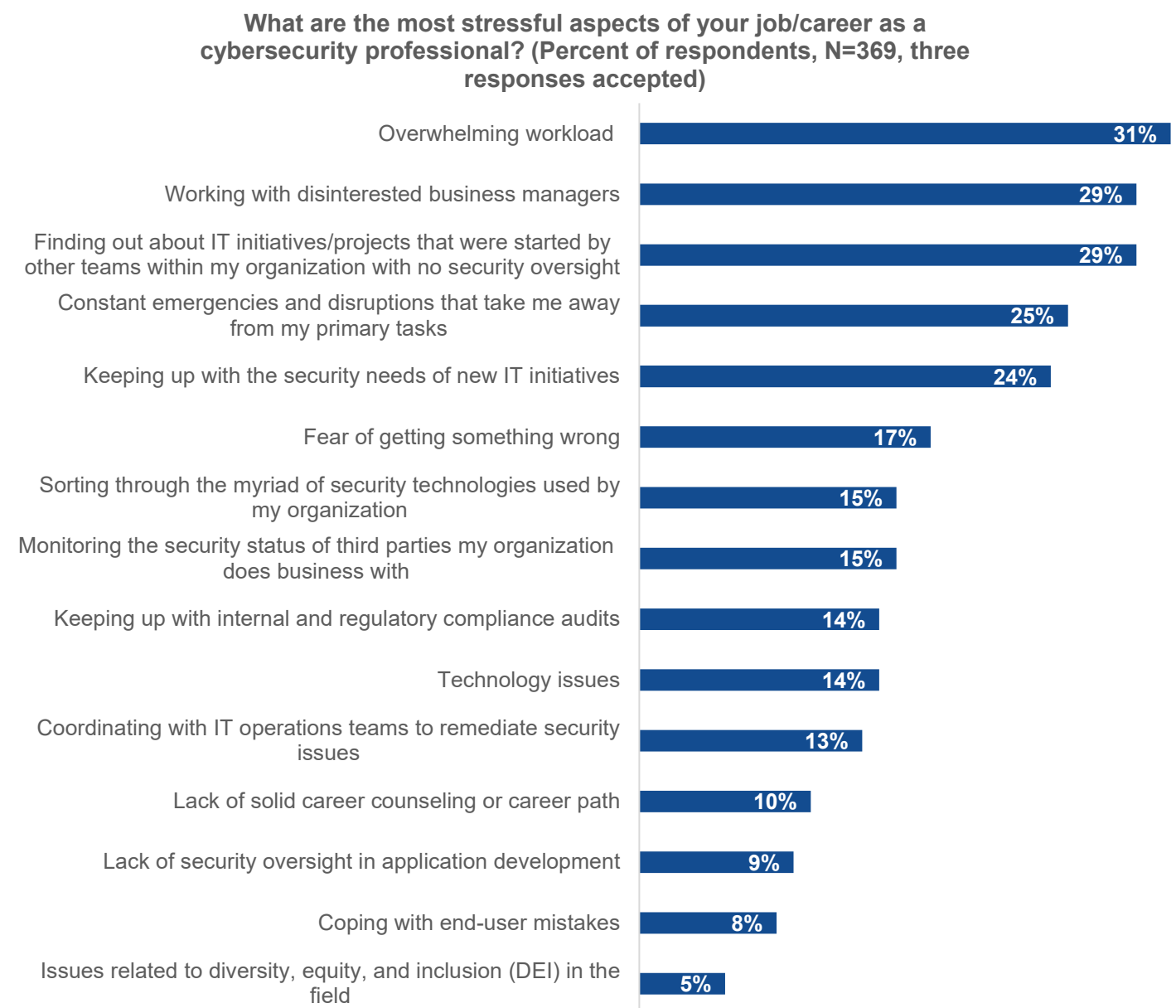
Figure 3. Stress Level Typically Associated with Cybersecurity Careers



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Cybersecurity professionals attribute job stress to factors like an overwhelming workload, working with disinterested business managers, finding out about IT initiatives or projects after they are well underway, and constantly responding to emergencies (see Figure 4). Nearly one-quarter of respondents cite keeping up with the security needs of new IT initiatives, illustrating the need for security oversight of digital transformation and AI-based projects and initiatives.

Figure 4. Stressful Aspects of the Cybersecurity Profession

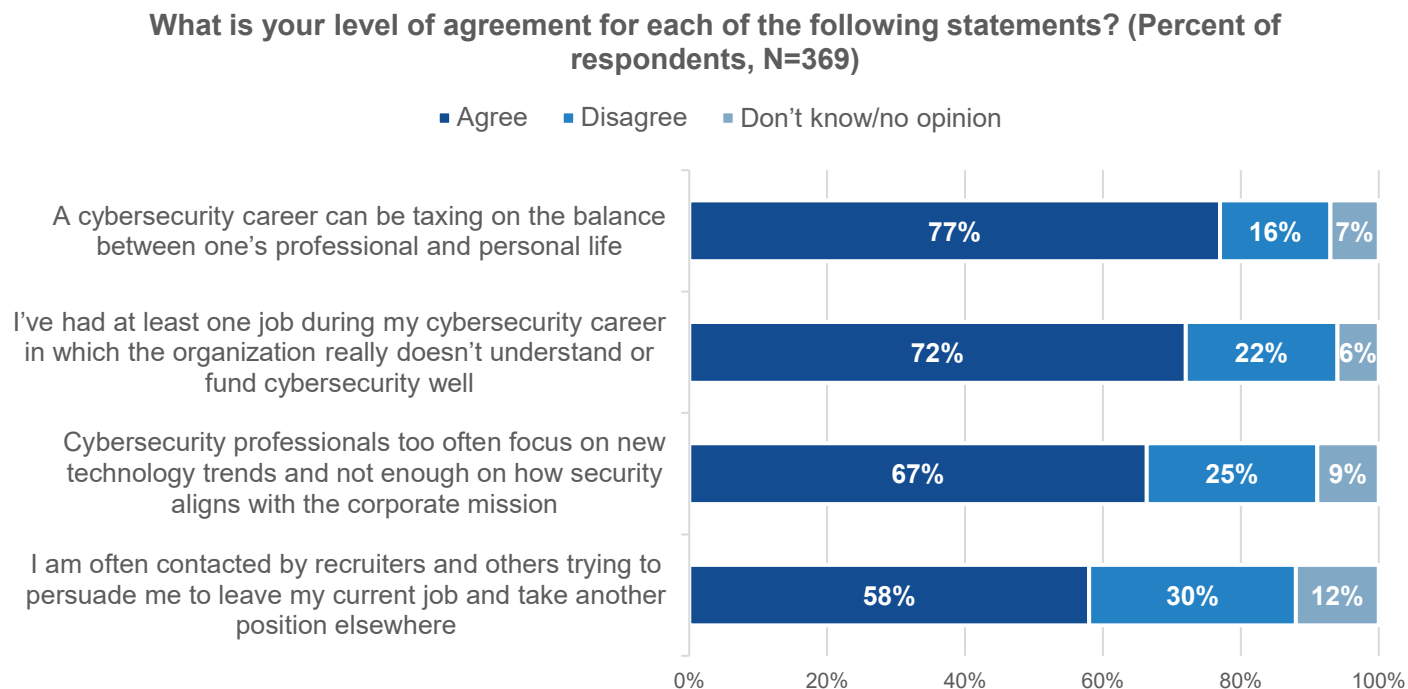


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

While cybersecurity careers grow more difficult and stressful, survey respondents face several other occupational hazards. Specifically, Figure 5 reveals that more than three-quarters (77%) of respondent organizations believe a cybersecurity career can be a taxing balancing act between one's personal and professional life, and 72% had at least one job where their organizations didn't understand or fund cybersecurity well. In many cases (67%), security

professionals admit that they often focus too much of their attention on security technology trends and not enough on the overall corporate mission.

Figure 5. Cybersecurity Professionals' Opinions on the Cyber Landscape



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Job Satisfaction in Cybersecurity Is More Than Just a Paycheck

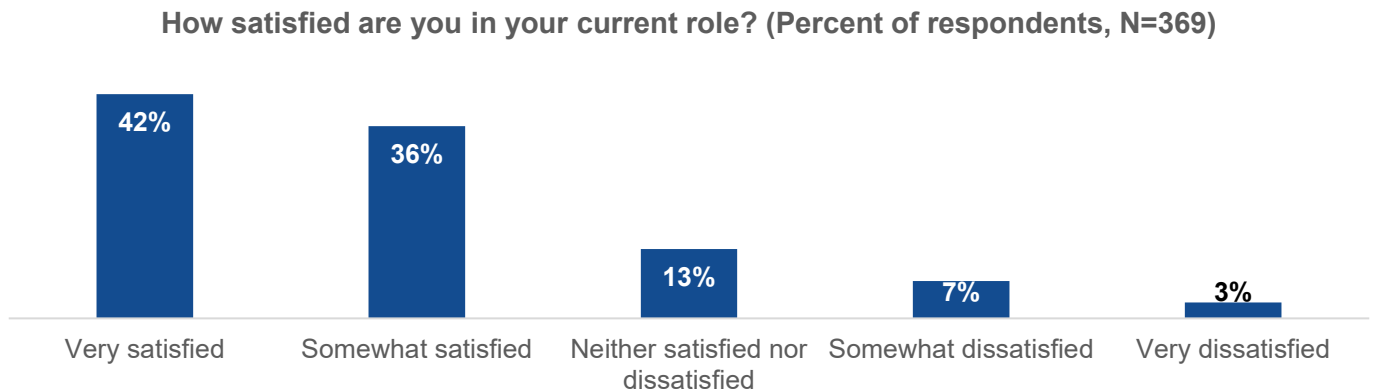
Despite the myriad career obstacles revealed in this research, most survey respondents remain relatively positive in terms of job satisfaction. In this year's study, Figure 6 reveals that 42% of survey respondents reported that they are very satisfied with their current jobs, almost identical to last year's results (44%). There's even a slight improvement in the dissatisfied population: In 2023, 13% of respondents were somewhat or very dissatisfied, compared with 10% this year. One can only surmise that cybersecurity professionals are willing to battle through occupational obstacles in their commitment to the global cybersecurity mission.

Of course, job satisfaction is subjective, varying from individual to individual, but the data clearly indicates that job satisfaction goes beyond financial compensation alone. In 2024, the leadership team's commitment to strong cybersecurity was the most common factor in determining job satisfaction (see Figure 7). Overall, there was a noticeable change from 2023, when competitive or industry-leading financial compensation, rather than leadership's cybersecurity commitment, was the top factor cited for determining job satisfaction.

Clearly, compensation remains important, but cybersecurity professionals also value organizational support and financial incentives for career advancement (38% in 2024, 36% in 2023), strong leadership from the CISO and other security managers (28% in 2024, 24% in 2023), and the ability to work with highly skilled and talented cybersecurity staff (28% in 2024, 38% in 2023).

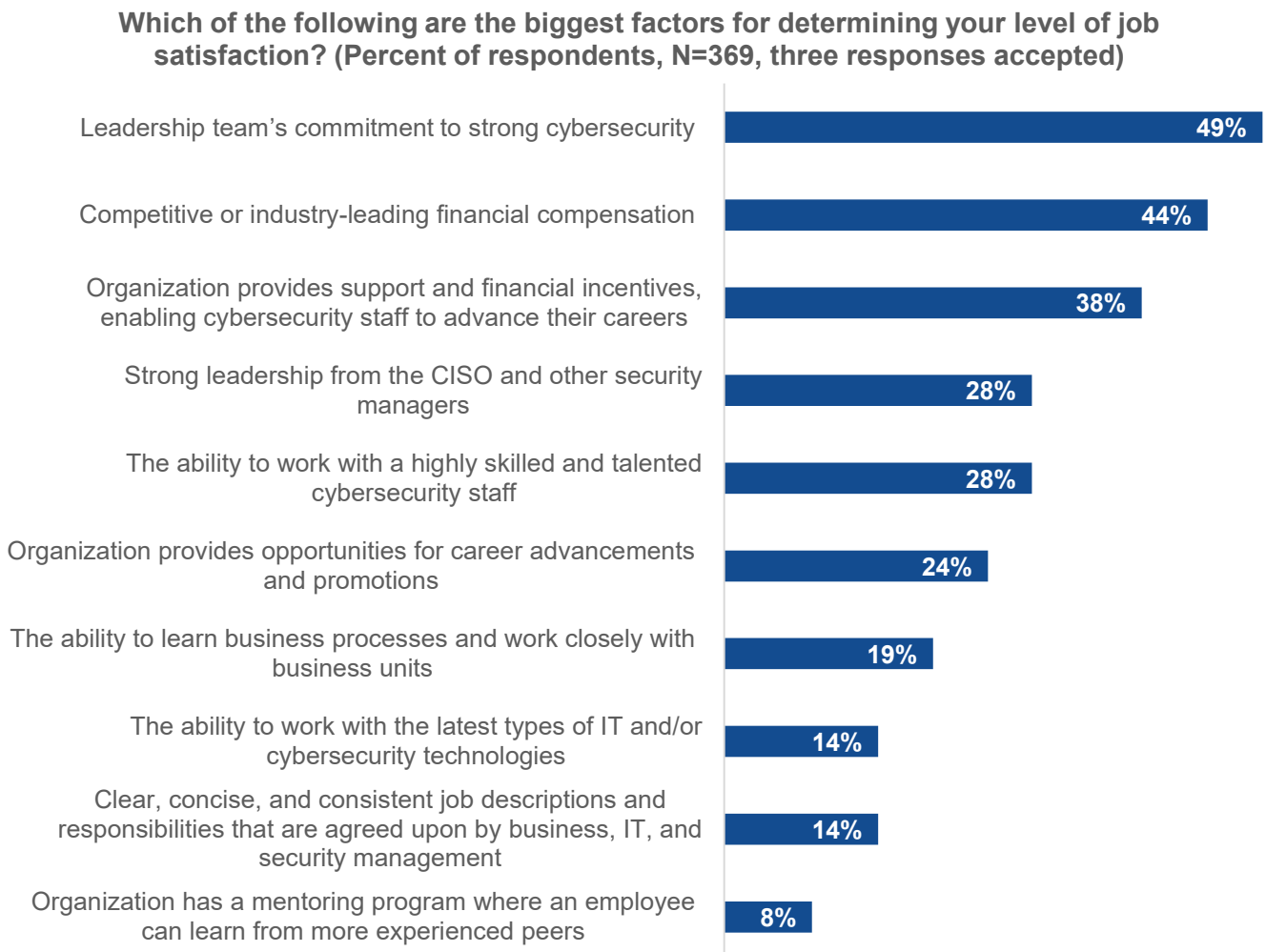
In summary, cybersecurity professionals tend to be satisfied in their jobs if they work for an organization with a commitment to cybersecurity, appropriate cybersecurity oversight, professional development support, and adequate compensation. This can be a recipe for cybersecurity professional and organizational success.

Figure 6. Cybersecurity Professionals Are Mostly Satisfied to Some Extent



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

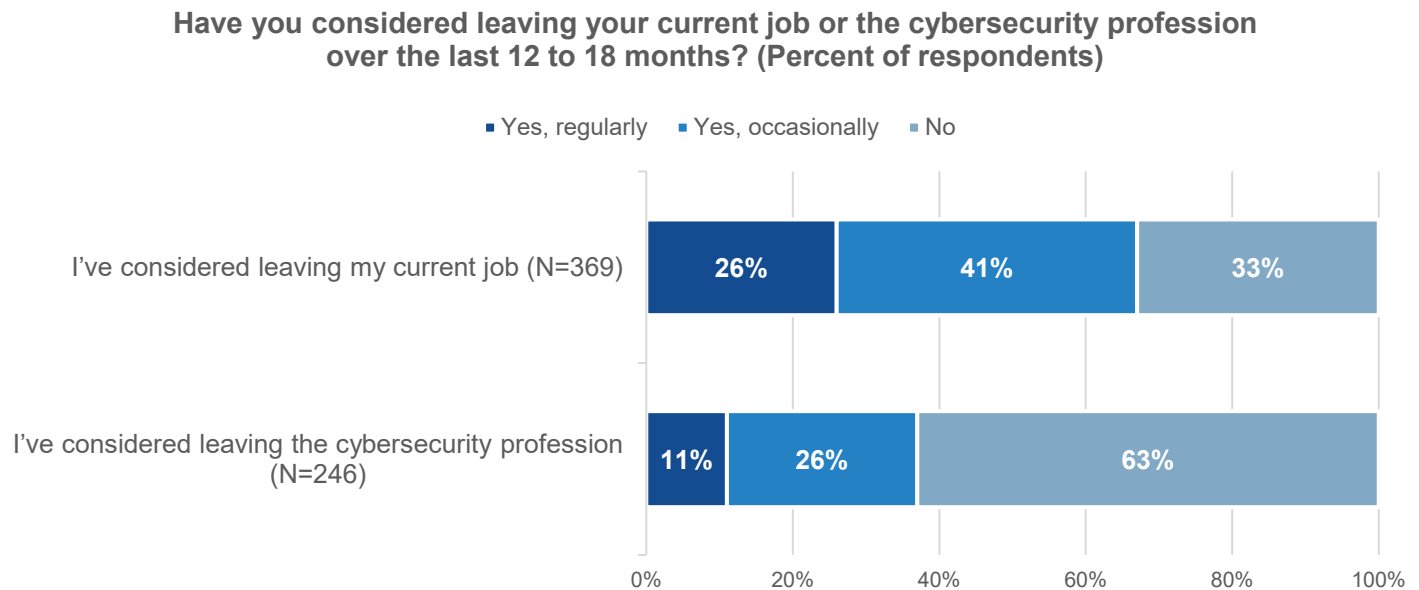
Figure 7. Factors Driving Cybersecurity Job Satisfaction



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

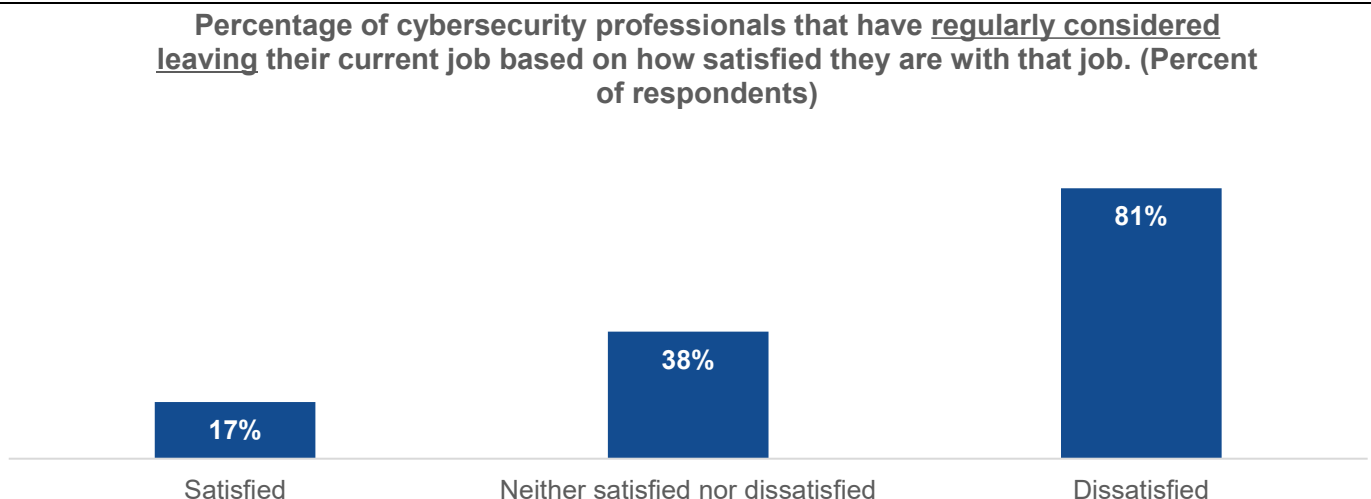
Job stress, dissatisfaction, and compensation inequity are simply too much for many current cybersecurity professionals. Alarming, Figure 8 reveals that more than one-third (37%) have considered leaving the profession all together, compared with 30% in 2023, while more than two-thirds (67%) of survey respondents have considered leaving their current job. As it turns out, job satisfaction is a key reason why cybersecurity professionals consider leaving their jobs. Specifically, 81% of those dissatisfied with their current job responded that they've considered leaving on a regular basis, compared with 38% who are neither satisfied nor dissatisfied, and only 17% of those satisfied (see Figure 9).

Figure 8. Potential for Leaving Current Cybersecurity Job or Even the Profession Entirely...



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 9. Leaving Current Cybersecurity Job Correlates Strongly with Job Satisfaction

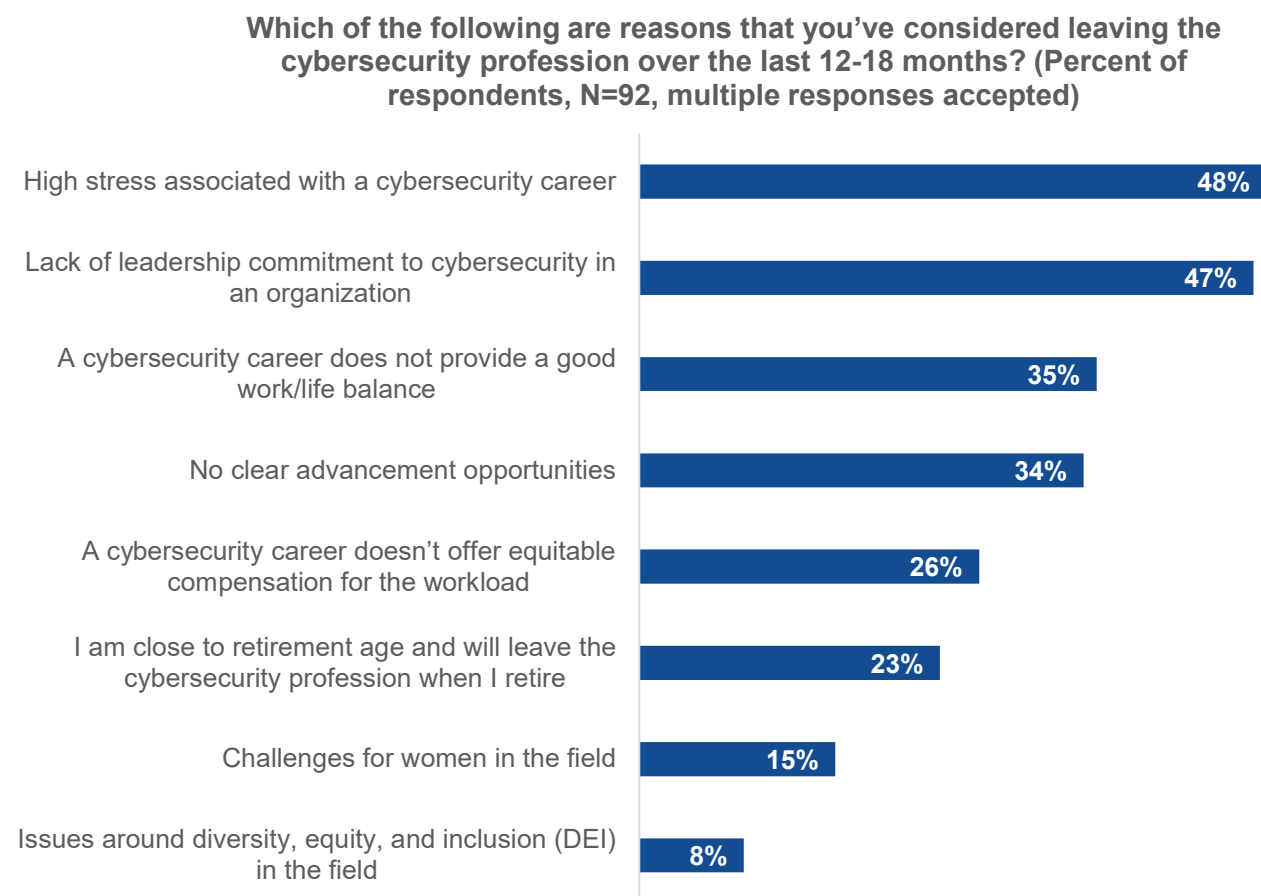


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The reasons for leaving the cybersecurity profession are not surprising, including the high stress associated with a cybersecurity career, a lack of a cybersecurity commitment from the leadership team, difficulties managing a work/life balance, and a lack of clear career advancement opportunities (see Figure 10).

As in previous years, this research data represents a red flag for organizations. CISOs should actively monitor the cybersecurity staff for signs of disillusion, dissatisfaction, and outright burnout, acting as an advocate for them with executive management, finance, and HR. The adage “Pay now or pay later” applies here; additional support services and compensation increases are far cheaper than the cost of a data breach.

Figure 10. Reasons Cybersecurity Professionals Have Considered Leaving the Profession



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Cybersecurity professional career development and success depends upon a commitment to continuous education. Survey respondents recognize this, suggesting several strategies for career advancement (see Figure 11).

The “network effect” is evident within the survey results. Cybersecurity professionals depend upon networking directly with others, attending events, and joining cybersecurity professional organizations as methods for staying current on the threat landscape, learning from peers, and bolstering their skill sets. Specialized security skills like ethical hacking, cloud security, and security auditing may require pursuing security certifications, while rotating jobs provides broad experience and can help cybersecurity professionals determine where they want their careers to end up. This job rotation strategy is particularly effective for those working at large enterprise organizations.

Figure 11. Most Helpful Career Advancement Techniques

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Boosting Cybersecurity Programs Calls for More Training and a Cultural Shift

When asked to rate their organization's cybersecurity culture, respondents provided ratings that are quite similar to last year's. Specifically, Figure 12 reveals that more than one-third (35%) of respondents said their organization's cybersecurity culture is advanced (compared with 31% in 2023), 41% indicated that their organization's cybersecurity culture is average (compared with 43% last year), and 24% claim their organization's cybersecurity culture is fair or poor (compared with 27% in 2023).

While the data appears to be trending in the right direction, Enterprise Strategy Group and ISSA view the results with caution. As the saying goes, "The cybersecurity chain is only as strong as its weakest link." An "average" cybersecurity culture, where cybersecurity is considered a shared responsibility by some employees and is included in some business initiatives, suggests that other employees and business initiatives ignore or minimize cybersecurity. This leaves ample room for misconfigured systems, vulnerable software, and uninformed employees, creating avoidable cyber-risks throughout the enterprise.

Figure 12. Rating Organizations' Cybersecurity Culture

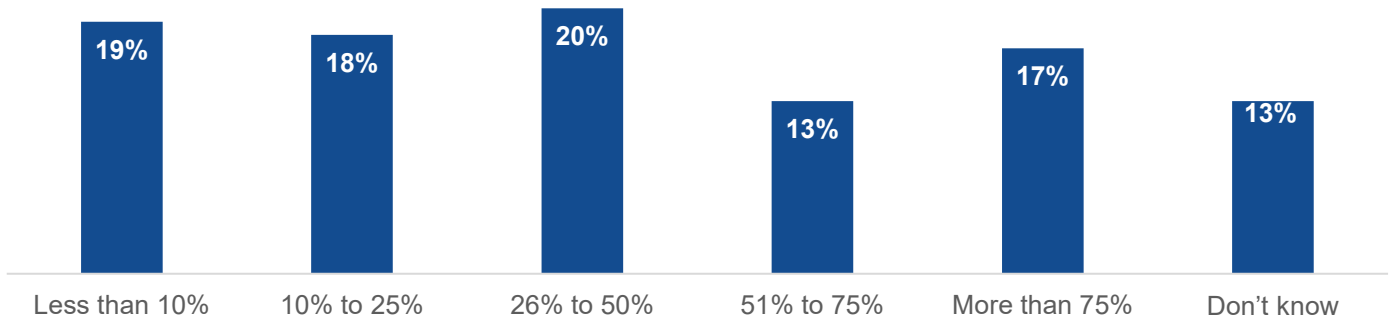
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

In a progressive organization, cybersecurity is everyone's job. For example, security professionals tend to monitor cyber-risks, identify technical vulnerabilities, and prioritize critical remediation actions. Upon executing these tasks, security teams often rely on IT operations, DevOps, and software developers to actually make technology changes (i.e., change configuration settings, patch systems, correct software errors, etc.) for risk mitigation. This symbiotic relationship is illustrated in Figure 13, which reveals that 30% of cybersecurity professionals estimate that IT staff performs more than half of all cybersecurity tasks on a day-to-day basis.

Unfortunately, the relationship between security and IT teams can be strained due to a combination of factors such as differing goals, tools, and management. Survey respondents suggest several ways to improve these relationships, including building information security oversight into IT projects, implementing cross-department process automation, improving communication, and embedding cybersecurity staff into functional technology groups (see Figure 14). These recommendations are intended to implant security within IT people, processes, and technologies.

Figure 13. IT Staff Is Bearing a Cybersecurity Workload Burden...

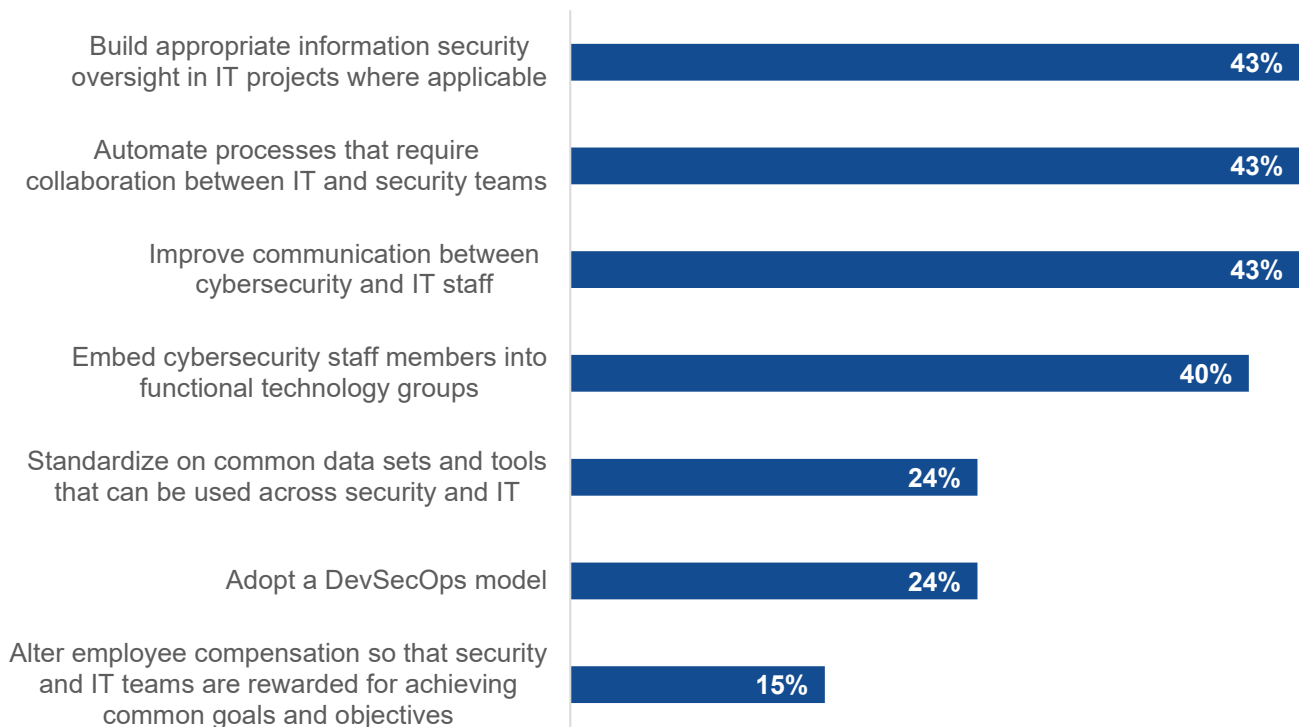
In your opinion, how much of your organization's day-to-day security tasks are done by people with IT (rather than security) titles? (Percent of respondents, N=369)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 14. ...Confirming the Need for Collaborative Relationships Between IT and Security Teams

Regardless of the current status, which of the following actions could be most impactful for improving the working relationship between the security and IT teams at your organization? (Percent of respondents, N=331, three responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Cybersecurity professionals also offered multiple ideas for enhancing the relationship between security and business managers, including improving cyber-risk identification, focusing cybersecurity resources on business-critical assets, establishing business-focused cybersecurity positions, and increasing CISO participation with executives and the board (see Figure 15).

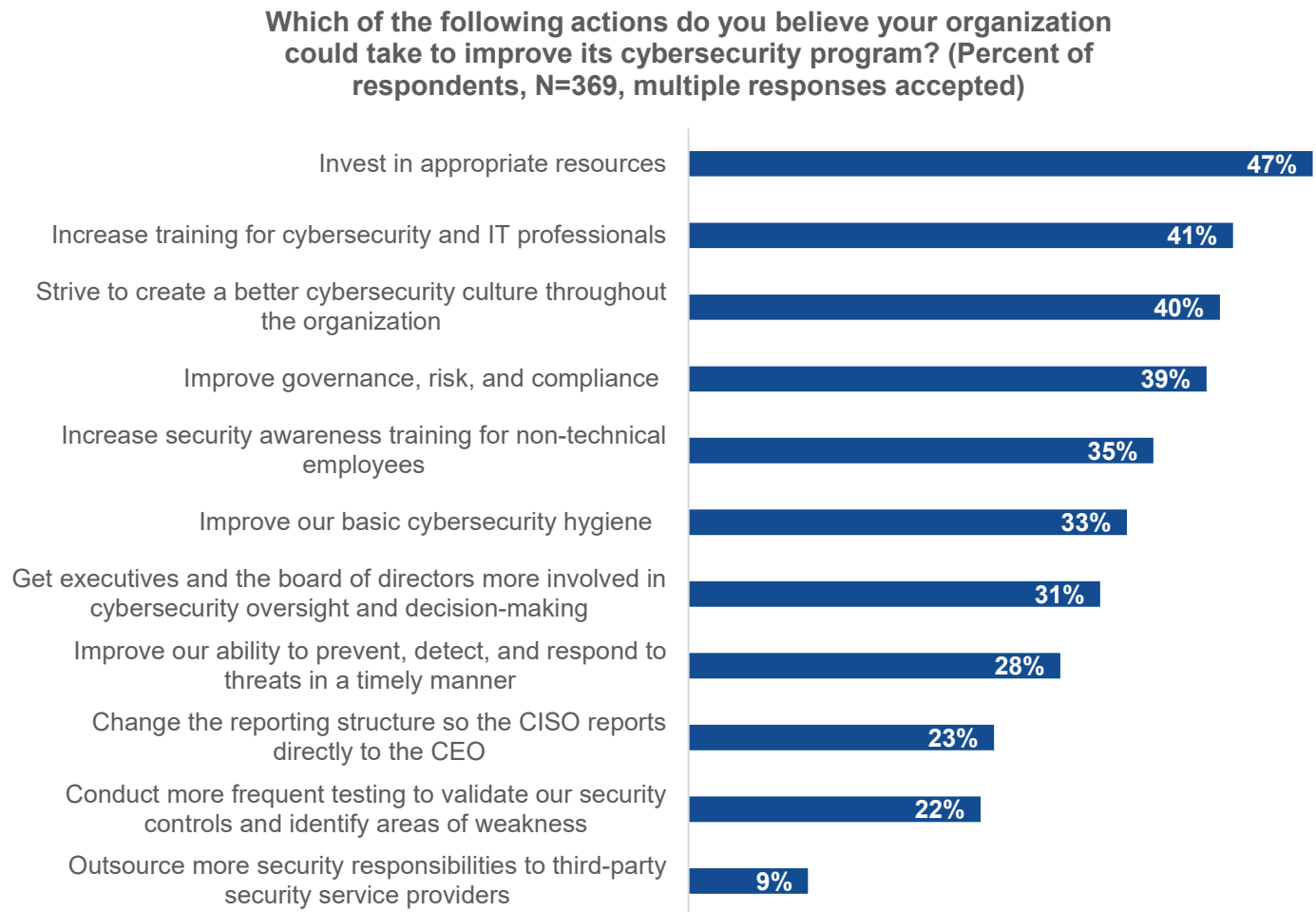
These recommendations are worth taking to executives and corporate boards for review. Of course, business managers should weigh in with their own input. For example, which cyber-risk metrics are most important for corporate oversight? Which assets do executives and boards consider business-critical? By coming to a mutual agreement, business management and security teams can better identify and monitor cyber-risk and use this cooperative effort to guide cybersecurity decisions.

Figure 15. Improving Relationships Between Security and Business Managers



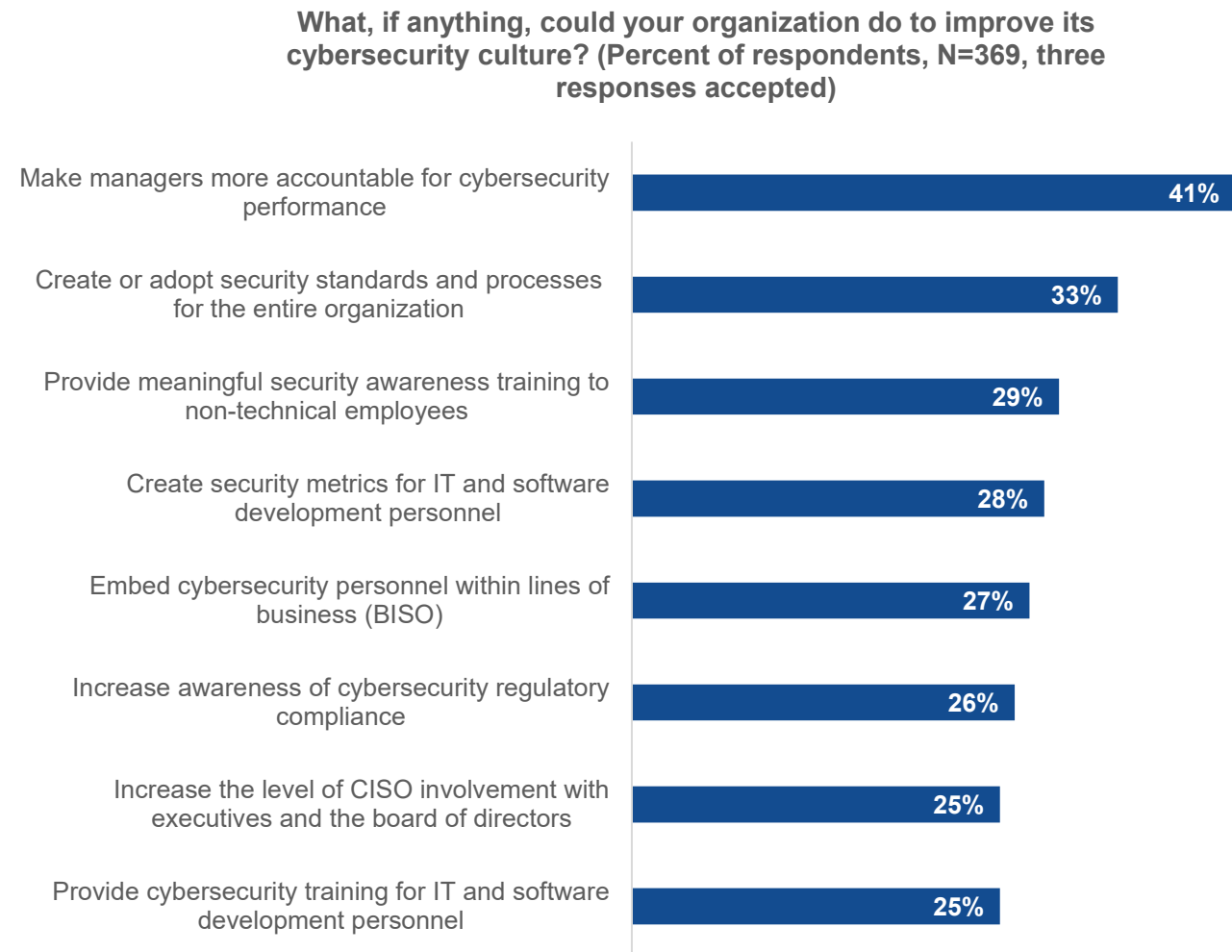
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

According to Figure 16, improving cybersecurity programs requires more resources, additional training, and a culture shift. The need for comprehensive training was also called out throughout the research as it can help professionals stay ahead of evolving risks, while fostering a cybersecurity-focused culture and improving overall resilience. By prioritizing these aspects, organizations can better prepare their teams to meet the increasing demands of the field.

Figure 16. Actions Cybersecurity Professionals Believe Could Improve Cybersecurity Programs

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

As in the past, survey respondents were asked what their organizations could do to improve cybersecurity culture. According to Figure 17, more than four in ten (41%) cybersecurity professionals said making managers more accountable for cybersecurity performance, an increase from 36% in 2023. Other suggestions included creating or adopting security standards and processes for the organization and providing meaningful security awareness training. Cooperation between security and IT teams was also emphasized as 28% mentioned creating standard security metrics for IT and software development personnel. Also, 27% endorsed embedding cybersecurity personnel within lines of business. The goal? Align business initiatives and processes with the appropriate security policies, controls, and oversight.

Figure 17. Actions Cybersecurity Professionals Believe Could Improve Cybersecurity Programs

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The Cybersecurity Skills Gap Remains, With Companies Lagging in Effective Responses

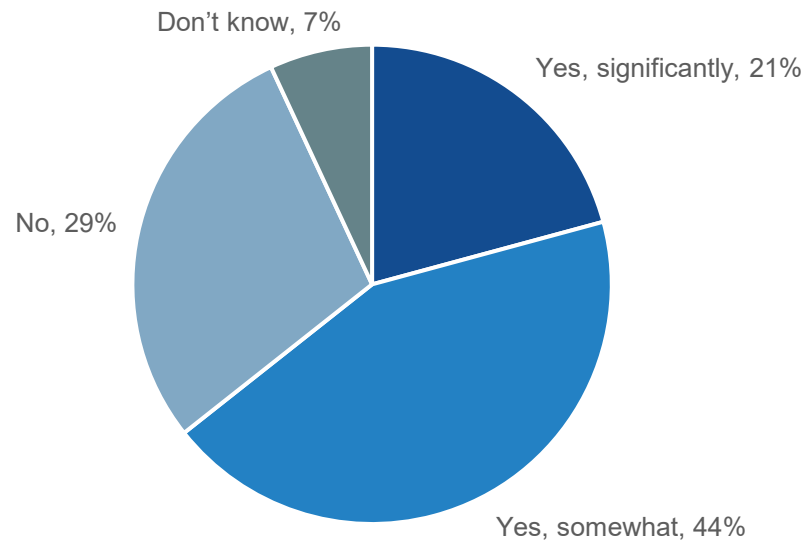
The cybersecurity skills shortage remains a perpetual problem. In 2024, Figure 18 reveals that nearly two-thirds (65%) of respondents claim that their organization has been impacted by the cybersecurity skills shortage, a slight decrease from last year (71% in 2023), but within consistent range over the past few years (i.e., low of 57% and high of 71%).

According to Figure 19, more than half (52%) of respondents say the skills shortage is about the same as it was two years ago (compared with 41% in 2023) and 10% believe things have improved over the past two years (compared to 5% in 2023). The data is slightly more positive than 2023 as 37% believe things have gotten worse over the past two years, compared with 54% in 2023.

The overall conclusions in 2024 are consistent with historical trends: The majority of organizations are impacted by the cybersecurity skills shortage and the situation isn't really improving. CISOs must adopt strategies for coping with this ubiquitous issue with training, process automation, technology consolidation, improved analytics, and increased use of managed security services.

Figure 18. The Global Cybersecurity Skills Shortage Has Impacted Many Organizations...

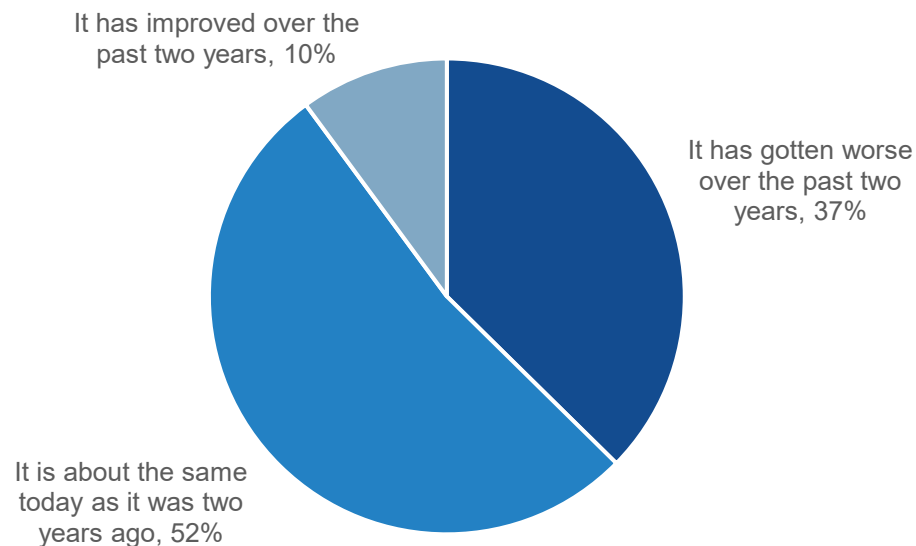
There has been a lot written about the global cybersecurity skills shortage. Has this trend impacted the organization for which you currently work? (Percent of respondents, N=369)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 19. ...And Has Gotten Worse for Many Over the Last Two Years

How do you think the cybersecurity skills shortage and its impact on your organization has changed over the past two years? (Percent of respondents, N=239)

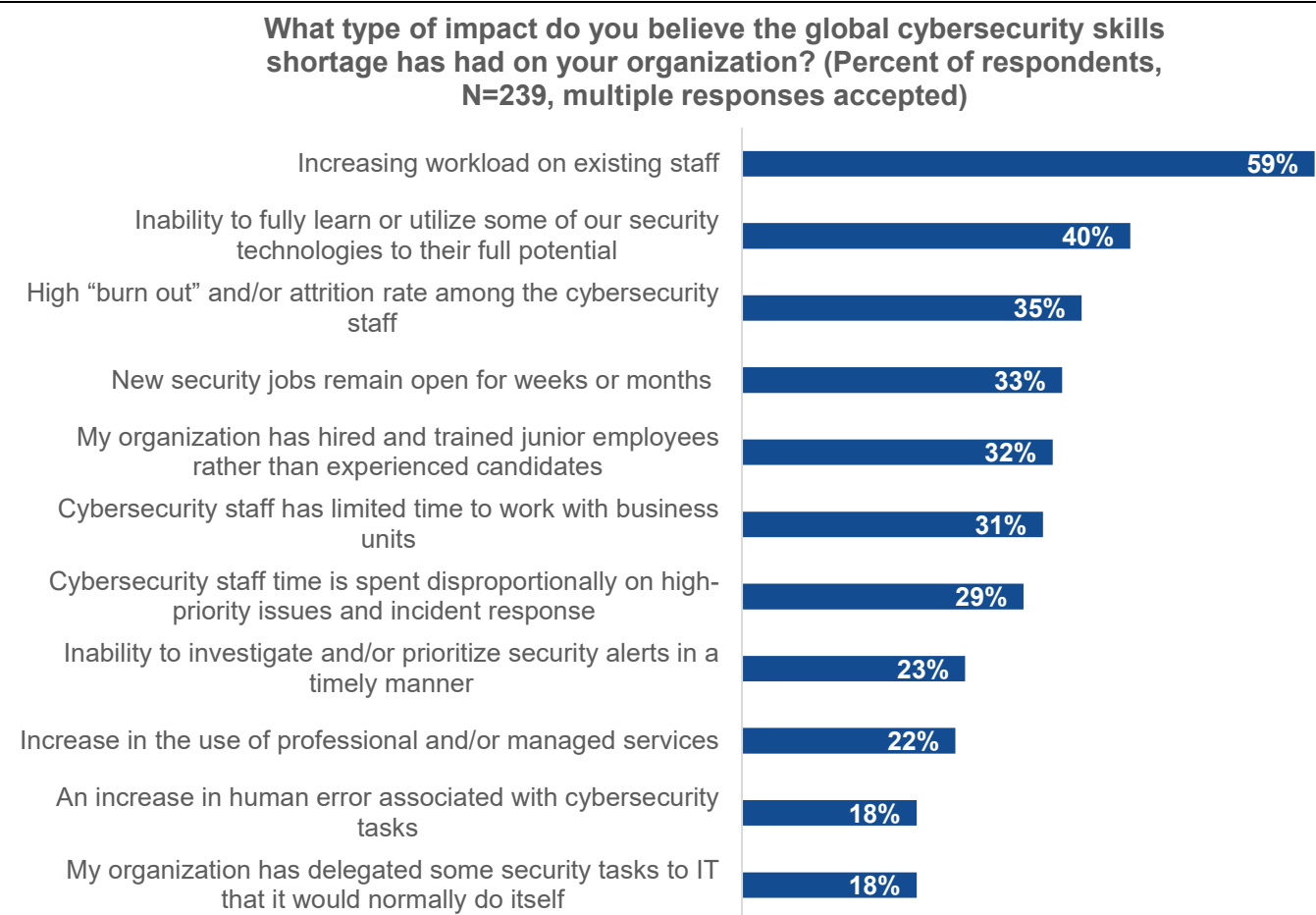


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Persistent skill shortages have numerous implications that ultimately increase risks to the business. Of those organizations impacted, 59% say the skills shortage has increased workloads on existing staff compared with 61% in 2023 (see Figure 20). Additionally, 40% claim that the skills shortage has led to an inability to fully learn or utilize some security technologies to their full potential (39% in 2023). Security technology vendors should be alarmed by this data point and invest in the appropriate resources for customer success. As in 2023, other issues include high rates of employee burn out, jobs remaining open for lengthy periods, and the need to hire and train junior rather than experienced cybersecurity professionals.

Business executives should review this data with a risk management perspective. Increasing cybersecurity workloads result in suboptimal risk identification and human error. The inability to properly use security technologies means reduced ROI and security controls gaps. High employee burnout leads to attrition, high training costs, and staff disillusion. In the long run, managing through the cybersecurity skills shortage must be considered a business, not just a technology, priority.

Figure 20. The Impact of the Cybersecurity Skills Shortage

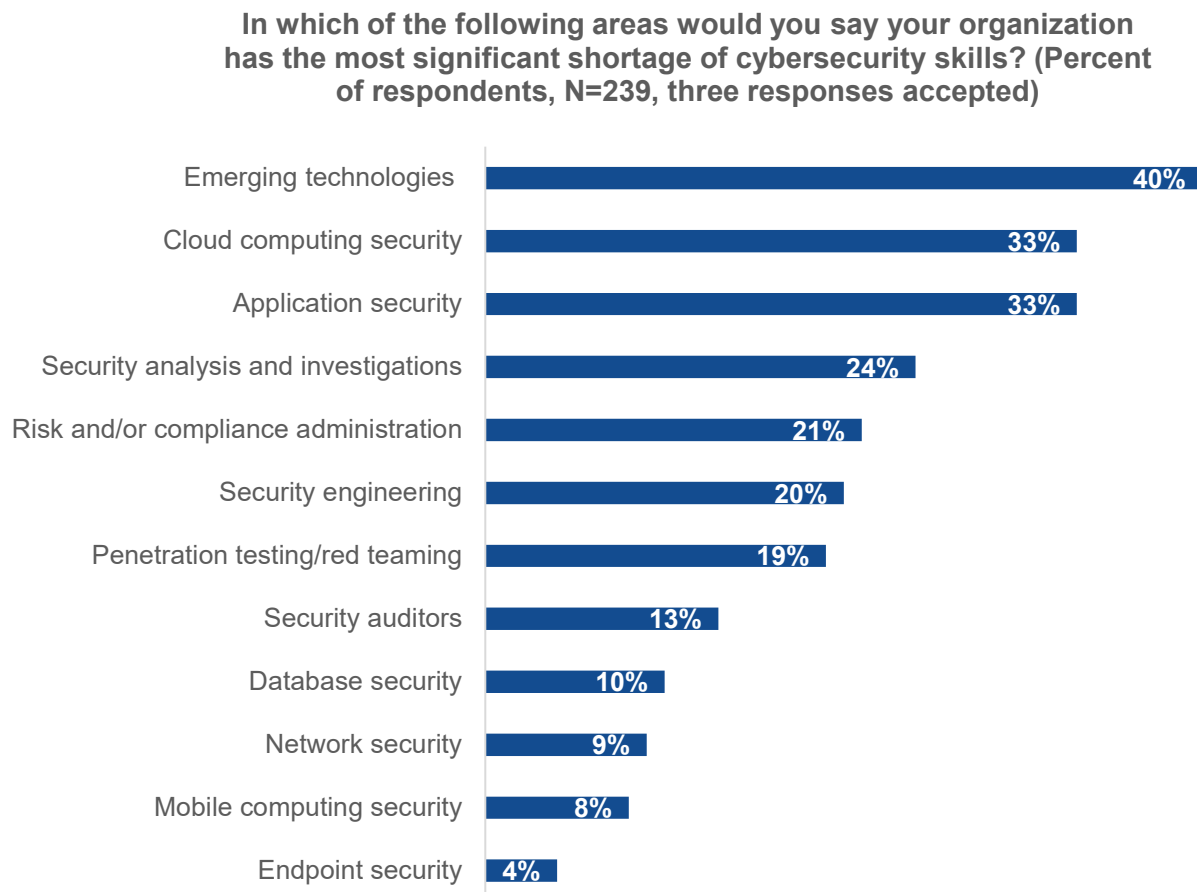


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Over the many years of the Enterprise Strategy Group and ISSA research project, cloud security, application security, and security analysis and investigations have been cited as areas of acute skills shortages, and this year is no different (see Figure 21).

In 2024, survey respondents were presented with a new option, emerging technologies, which was defined in the survey as generative AI cybersecurity solutions. Not surprisingly, this topped the list, with 40% of respondents claiming their organization has an acute skill shortage in this area.

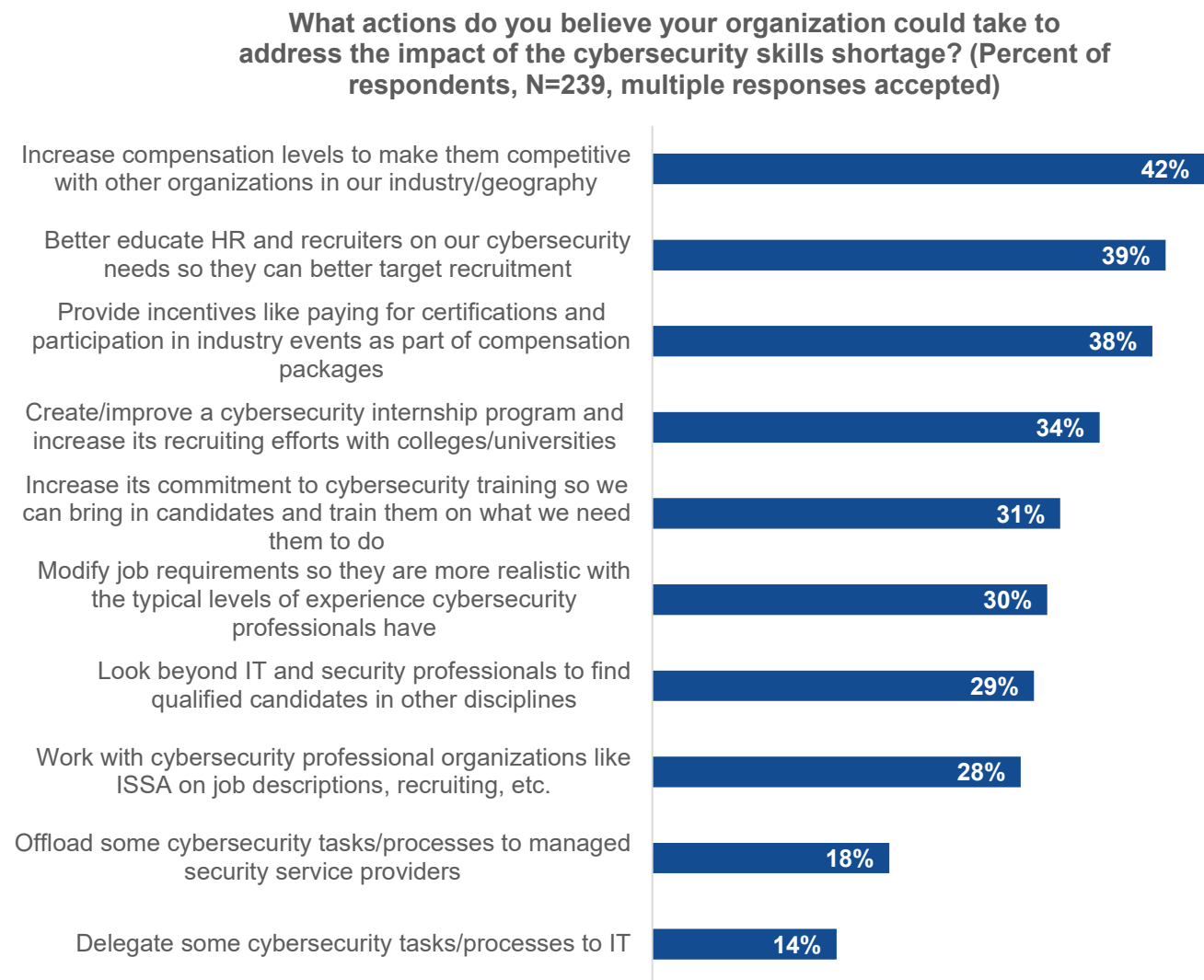
Figure 21. Most Significant Skills Shortage Areas Include Emerging Technologies and Cloud



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The security skills shortage remains omnipresent with no end in sight. Therefore, survey respondents were asked what their organizations could do to better address this ongoing challenge. Increasing compensation packages is an understandable response but others are a bit less obvious. For example, survey respondents believe human resource professionals truly lack an understanding of the skills needed for a cybersecurity position and compensate for this by requiring multiple (and sometimes irrelevant) certifications and unreasonable years of experience for even the most basic security roles. To counteract this, 39% of cybersecurity professionals believe their organization could address the skills shortage by better educating HR and recruiters on their cybersecurity needs and associated recruiting strategies (see Figure 22).

Clearly, organizations must explore diverse strategies for addressing the enduring cybersecurity skills shortage, from investing in education and training programs to fostering collaboration and knowledge-sharing within the industry. Only through concerted efforts can the cybersecurity skills gap be effectively narrowed. Again, this should be a business and technical priority as improvements in this area can result in improved risk management and a more stable—and happy—workforce.

Figure 22. Addressing the Impact of the Cybersecurity Skills Shortage

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

CISO Success Hinges on Top Notch Leadership and Communications Skills

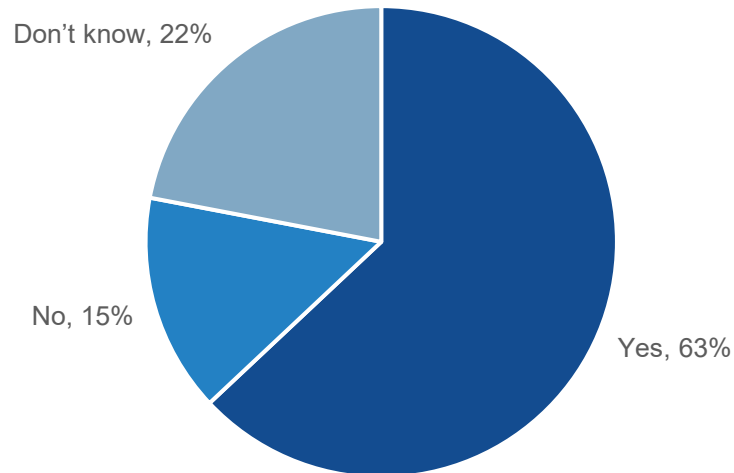
According to Figure 23, nearly two-thirds (63%) of respondents report that their CISO regularly interacts with the board of directors, slightly lower than last year's result.

When asked if the CISO's level of interaction was adequate, just more than half (51%) of respondents said it was (see Figure 24). What's troubling is that nearly one-quarter (24%) of cybersecurity professionals don't believe the level of interaction is sufficient (27% in 2023).

This data may also indicate that many corporate boards are content with "good enough" security and don't really want to get involved beyond supporting basic protections. This behavior is insufficient, especially given new SEC and EU cybersecurity regulations (i.e., the NIS 2 Directive). Corporate boards, executives, and CISOs should be working harmoniously to improve cyber-risk management, bolster cybersecurity awareness training, and protect business-critical assets.

Figure 23. Most CISOs Are Regularly Interacting with Executives and Board of Directors...

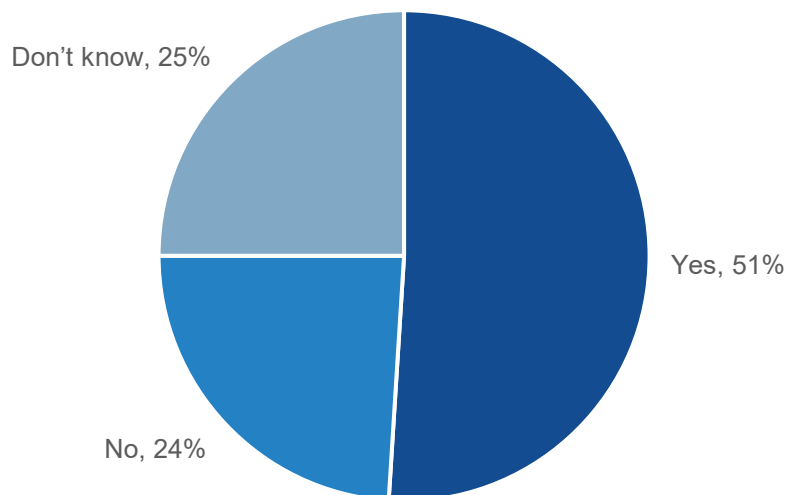
Does your organization's CISO regularly meet with executive management and the board of directors (or similar oversight group)? (Percent of respondents, N=298)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 24. ...And This Level of Interaction Is Mostly Considered Adequate

Do you think your organization's CISO's level of interaction with executive management and the board of directors is adequate? (Percent of respondents, N=298)

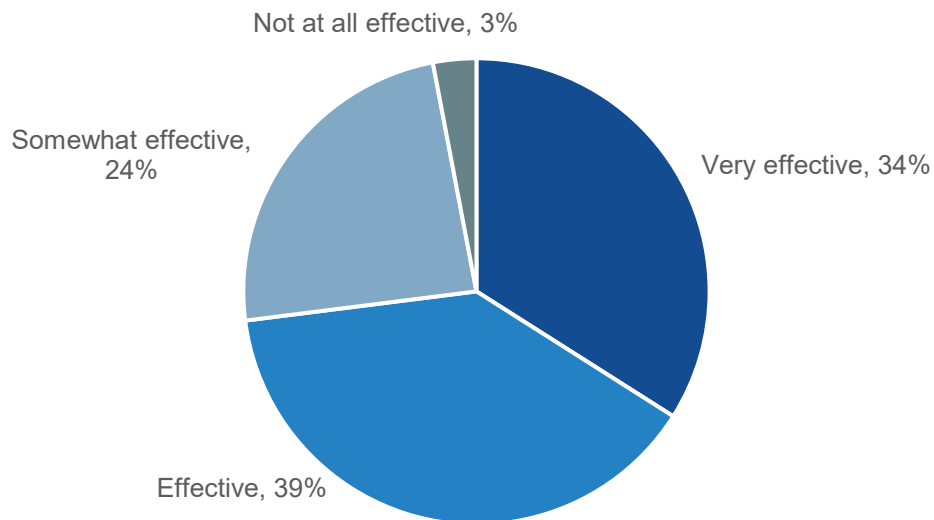


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Nearly three-quarters of respondents claim that their CISO is very effective (34%) or effective (39%), which is similar to 2023 (see Figure 25). There is room for improvement, as 27% believe their CISO is somewhat effective or not effective at all, a slight improvement over 2023. There is also a strong correlation between effectiveness and level of interaction with executives and board members. Specifically, Figure 26 reveals that 80% of cybersecurity professionals who believe their CISO is very effective indicate that CISO regularly meets with the C-suite and board of directors, compared to only 47% of those with somewhat effective CISOs and 0% with ineffective CISOs.

Figure 25. Perceived Effectiveness of CISOs Is Generally High...

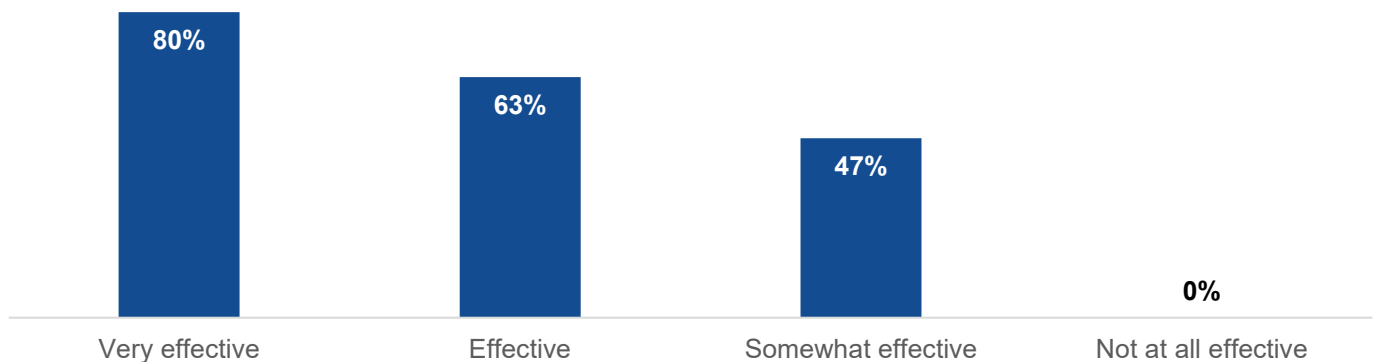
In your opinion, how effective is your CISO? (Percent of respondents, N=298)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 26. ...But Much Higher When CISOs Regularly Meet With the C-suite and Board

Percentage of organizations with CISOs that regularly meet with executive management and the board of directors by perceived effectiveness of CISO. (Percent of respondents, N=298)

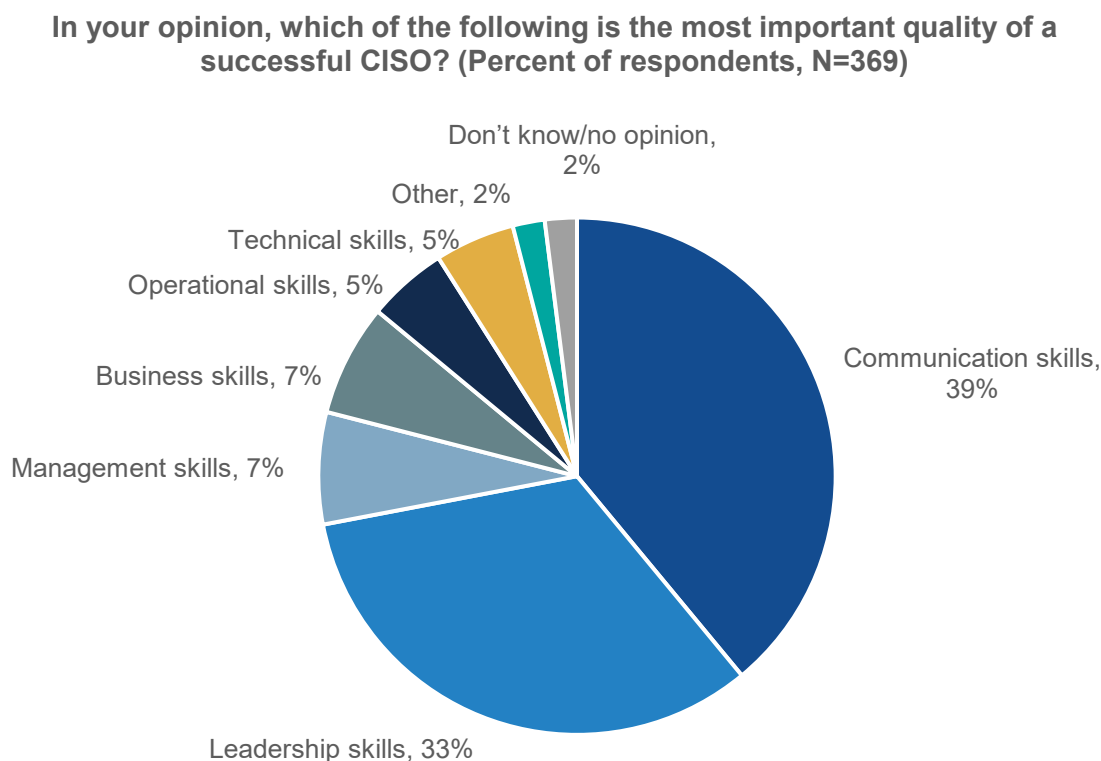


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Survey respondents believe the success of a CISO depends on exemplary communication and leadership skills. Interestingly, communication and leadership topped the list in 2023 but in reverse order. Regardless, these two qualities remain top priorities for CISO success (see Figure 27).

These skills are particularly crucial given that more than one-quarter of all CISOs often report directly to the CEO or the board of directors, increasing the importance of their role in steering the organization's cybersecurity posture and aligning it with broader business objectives. Mastering communication and leadership skills remains paramount for CISOs to thrive in their roles and drive meaningful cybersecurity outcomes for their organizations.

Figure 27. Most Important Quality for Successful CISOs



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Conclusion

The seventh annual *The Life and Times of Cybersecurity Professionals* study continues to reveal the many aspects of a cybersecurity career. On one hand, many cybersecurity professionals are satisfied with their career choice and dedicated to the mission. On the other hand, they face constant challenges including overwhelming workloads, the relentless pace of new IT initiatives, and disinterested business managers who view cybersecurity as no more than a necessary evil. While the report did uncover finite progress in some areas, it remains mostly consistent with previous years, demonstrating that organizations continue to underinvest in the staffing and training needed to protect themselves from cyber-risk.

Similar to 2023, two-thirds (65%) of cybersecurity professionals believe that the profession has become more difficult over the past two years, while 57% believe that their job is stressful more than half of the time. Given this situation, it is not surprising that 26% of respondents have considered leaving their current job over the last 12 to 18 months, while 37% considered leaving the cybersecurity profession entirely.

Survey respondents believe that a strong culture acts as a cybersecurity foundation. In fact, nearly half (49%) of respondents claim that leadership's commitment to cybersecurity is the most important factor in determining job satisfaction. Some organizations are performing well here, as 35% of respondents rate their organization's cybersecurity culture as advanced. Still, it's alarming that 24% say that their organization's cybersecurity culture is fair or poor. This is a recipe for a disgruntled cybersecurity team, relentless attrition, and poor results.

The report also demonstrates that the cybersecurity skills shortage continues as an issue. This year, 59% of organizations are impacted by the skills shortage, while 37% of respondents believe it has gotten worse over the past two years. As in the past, skill shortage ramifications include an overwhelming workload on existing staff, an inability to optimize security technologies, high staff burnout, and open security jobs that can't be filled. To address these issues more effectively, survey respondents suggest adjusting compensation, better educating HR and recruiters on staffing needs, providing training and career advancement incentives, and creating a cybersecurity internship program. Regardless of any internal changes, CISOs must factor the cybersecurity skills shortage into their decisions about cybersecurity strategy and day-to-day programs.

Cybersecurity professionals look to their CISOs to champion their cause with executives and in the boardroom. While this is happening, 24% of respondents believe CISOs aren't participating enough with corporate leaders. The dangerous threat landscape and new regulations will likely amplify CISO voices in the near future. Meanwhile, cybersecurity professionals stress that CISOs need strong communication and leadership skills most, reflecting the business nature of the job.

In summary, *The Life and Times of Cybersecurity Professionals, Volume VII* exposes numerous continuous trends. A cybersecurity career can be both exhilarating and taxing simultaneously. Individuals in this field must be mission-driven while understanding the personal and professional challenges involved. Executives must understand that cybersecurity should be treated as an organizational rather than technical pursuit. Therefore, culture and leadership are essential. The cybersecurity skills shortage is a reality that hasn't dissipated and won't in the future. Addressing the skills shortage will require progressive use of training, process automation, increasingly intelligent technologies, and supplemental use of security services. CISOs must be tightly coupled with business processes and strategies to improve risk mitigation, implement the right security controls, and anticipate new types of threats.

These changes can help mitigate risk while improving cybersecurity program efficacy and efficiency. They will also benefit the cybersecurity professional community by providing the right training, tools, and support for them to be successful. Cybersecurity truly takes a village.

Research Methodology

To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations across the globe between February 21, 2024, and March 18, 2024. To qualify for this survey, respondents were required to be information security or IT professionals from ISSA's member list. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 369 IT and cybersecurity professionals.

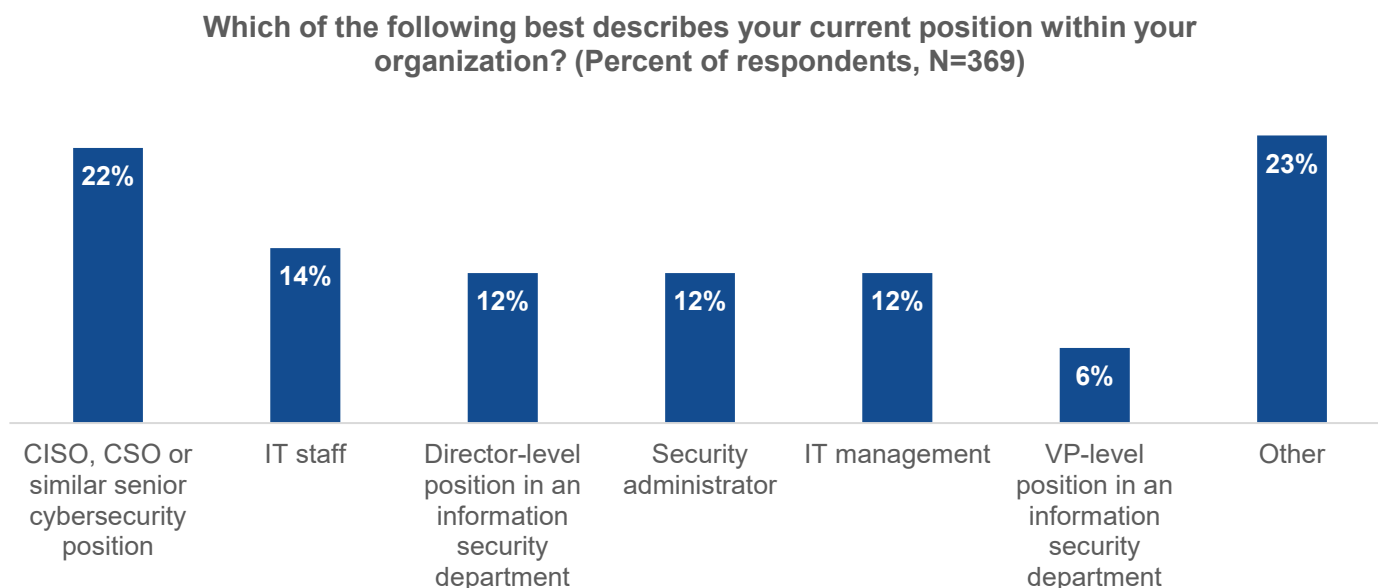
Please see the Respondent Demographics section of this report for more information on these respondents.

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

Respondent Demographics

Respondent data presented in this report is based on a survey of 369 qualified respondents. Figure 28 through Figure 33 detail the demographics of the respondent base at an individual and organizational level.

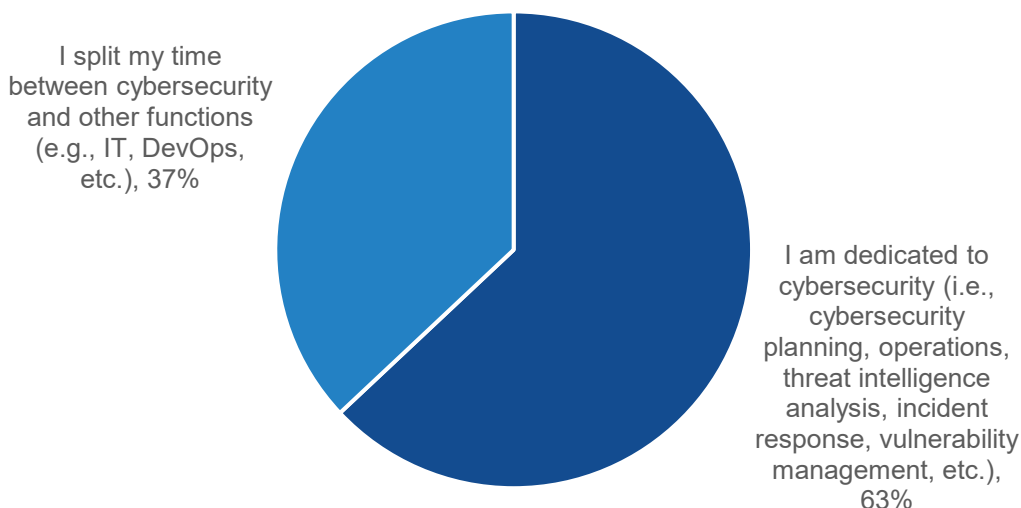
Figure 28. Respondents by Current Position



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

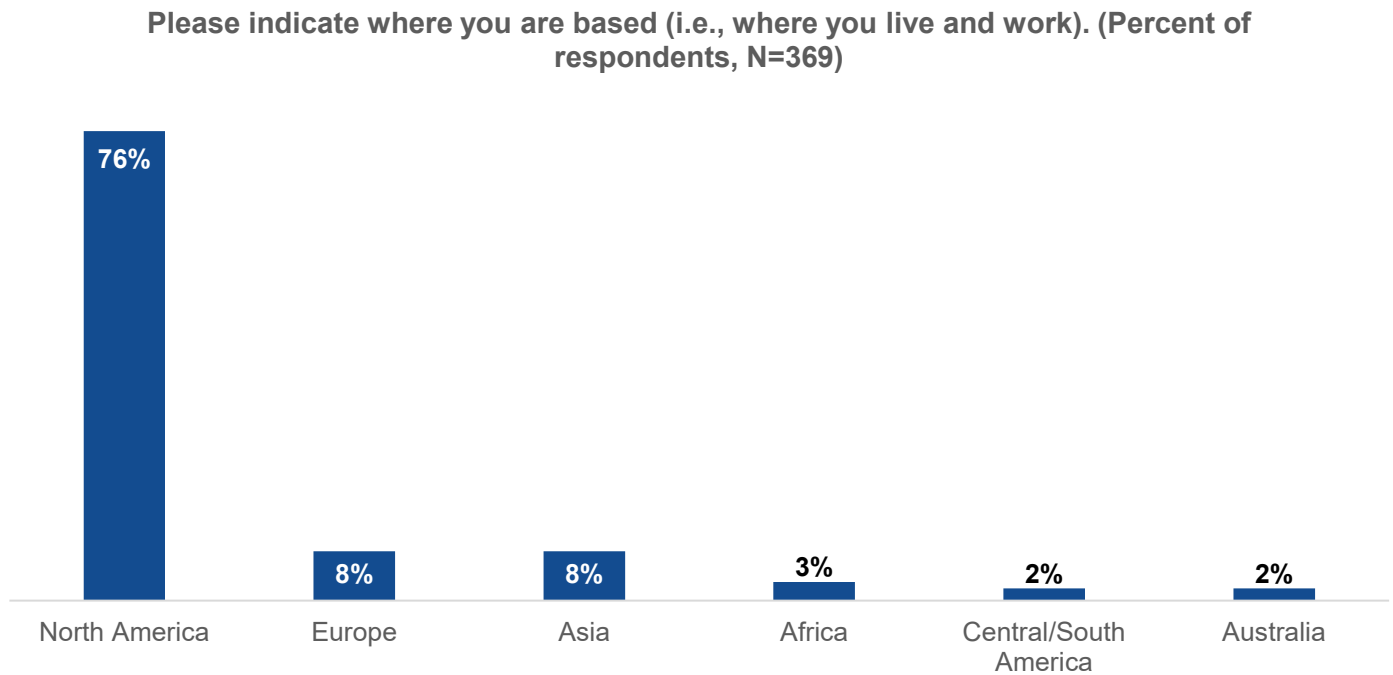
Figure 29. Respondents by Job Responsibilities

Which of the following best describes your overall job responsibilities? (Percent of respondents, N=369)



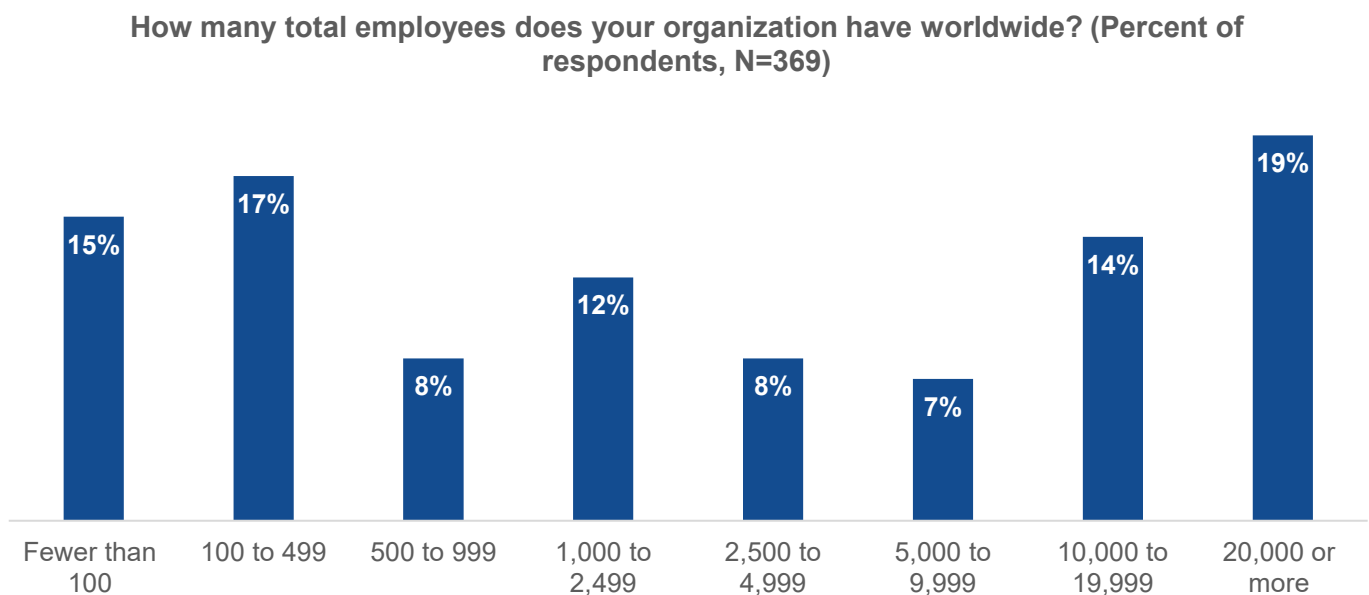
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 30. Respondent Organizations by Region



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

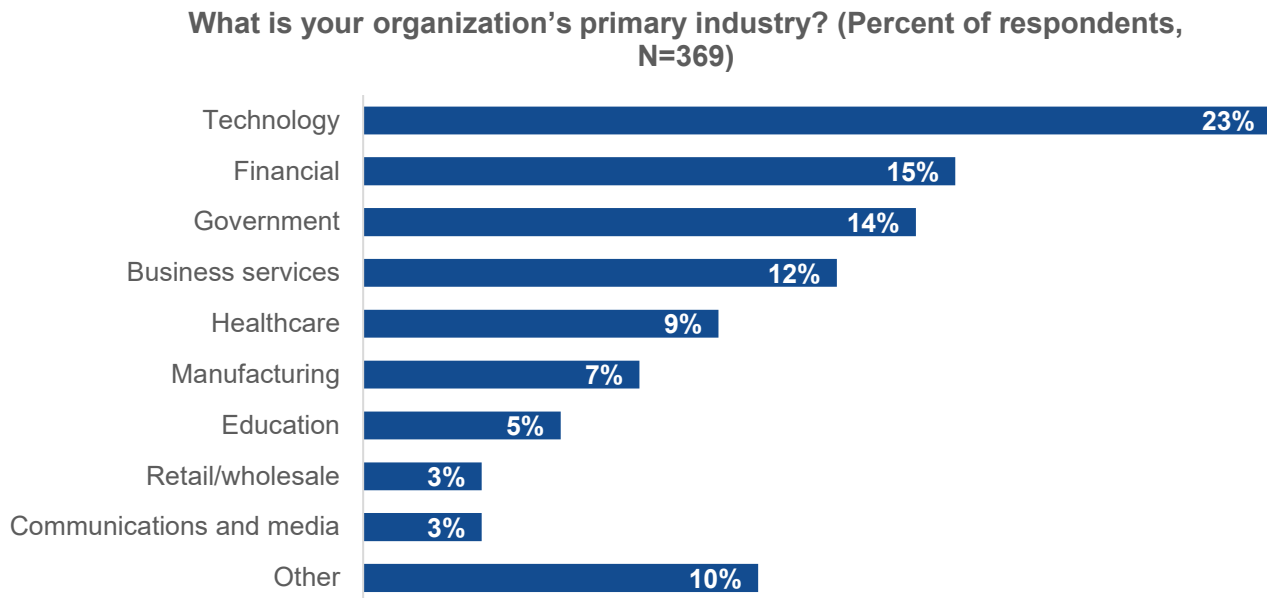
Figure 31. Respondent Organizations by Number of Employees



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

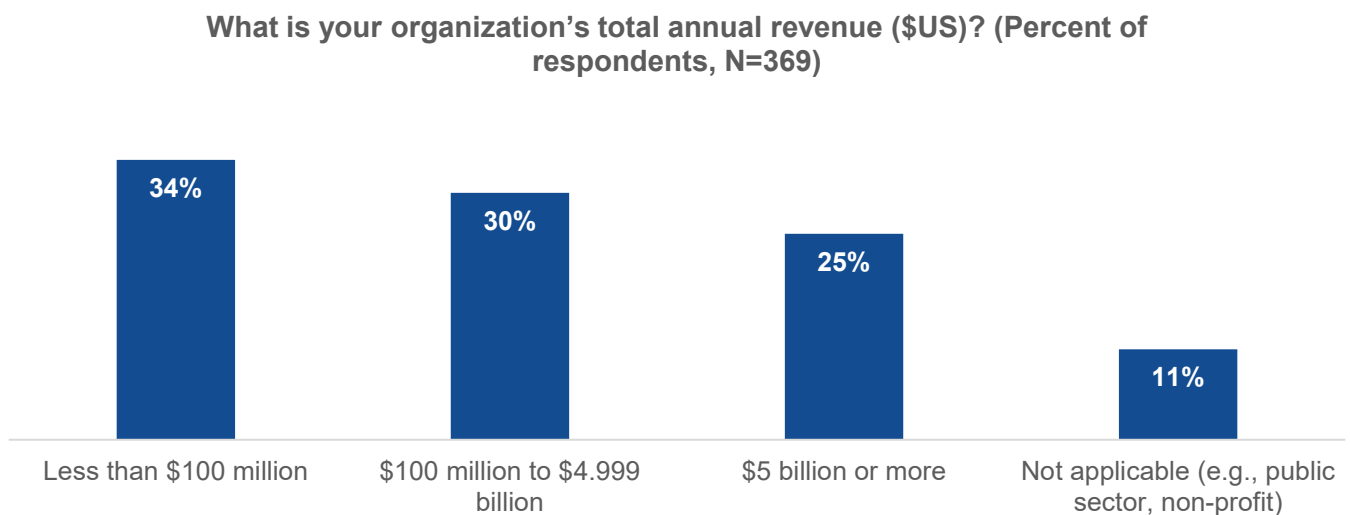
Respondents were asked to identify their organization's primary industry. In total, Enterprise Strategy Group received completed, qualified responses from individuals in 21 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 32.

Figure 32. Respondent Organizations by Industry



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 33. Respondent Organizations by Annual Revenue



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.


Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 contact@esg-global.com

 www.esg-global.com