Enterprise Strategy Group™ by TechTarget

RESEARCH REPORT

The Life and Times of Cybersecurity Professionals Volume VI

By Jon Oltsik, Distinguished Analyst & Fellow and Bill Lundell, Director of Syndicated Research

Enterprise Strategy Group

October 2023

Contents

Executive Summary

Report Conclusions

TechTarget's Enterprise Strategy Group conducted an in-depth survey of 301 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:

- **Working as a cybersecurity professional is getting increasingly difficult.** A majority of cybersecurity professionals believe that working as a cybersecurity professional has become more difficult over the past two years, with more than eight in ten respondents citing both the increasing complexity and workloads associated with cybersecurity. Despite cybersecurity professional challenges, more than four in ten survey respondents report that they are very satisfied with their current jobs. Beyond individual financial incentives, cybersecurity pros equate job satisfaction with business management's commitment to cybersecurity, working with other experienced professionals, and incentives like the opportunity for continuous advanced training.
- **Cybersecurity programs could be improved by embracing a cybersecurity culture.** Less than one-third of cybersecurity professionals claim their organization has an advanced cybersecurity culture, where cybersecurity is considered a shared responsibility and part of the organization's business initiatives. Additionally, many have worked for at least one organization that knowingly ignored security best practices and/or regulatory compliance requirements in the past. However, many seem unwilling to compromise their professional ethics in situations where their organization knowingly ignores security best practices and/or regulatory compliance requirements and would in fact be willing to act as whistleblowers. Cybersecurity professionals point to actions like including cybersecurity considerations in business planning, providing more/better security awareness training, and emphasizing security best practices rather than regulatory compliance as ways of building or improving cybersecurity culture.
- **The cybersecurity skills shortage is not improving, and organizations are not responding with the right countermeasures.** This iteration of research clearly indicates that the cybersecurity skills shortage continues unabated, with nearly three-quarters of organizations claiming to have been impacted by it. Furthermore, nearly one-third of cybersecurity professionals believe the impact of the cybersecurity skills shortage is actually *understated*, meaning they believe it is a more substantial problem than reported. Those organizations impacted by the cybersecurity skills shortage report ramifications like an increasing workload on existing staff, lengthy job openings, and burnout rates leading to staff attrition.
- **CISO success depends upon leadership and communications skills.** More than three-quarters of all survey respondents work at an organization with a CISO or virtual CISO. Among these organizations, almost half indicate their CISOs report to the CIO or other senior IT manager, while nearly one-quarter report directly to the CEO. When asked to identify the qualities that make CISOs successful, nearly three-quarters pointed toward leadership or communications skills. In most cases, CISOs actively interact directly with their board of directors or similar oversight body.
- **Organizations are working toward future cybersecurity improvement.** More than three-quarters consider the partnership between security and IT groups to be good or very good, but there are exceptions, as 24% rate this relationship as fair or poor. Survey respondents did offer some suggestions for improvement, such as ensuring security staff involvement in IT projects from their onset, increasing cross-training between IT and security, automating end-to-end processes, and embedding cybersecurity staff members into functional IT groups. Cybersecurity professionals also have suggestions for improving the relationship between security and business managers, including better identification of cyber-risks as they apply to the business, increasing executive (and board-level) cybersecurity training, focusing cybersecurity on business-critical assets, and establishing BISOs (or perhaps CISOs) within business units.

Introduction

Research Objectives

As cyber-attacks continue unabated, the global population depends upon cybersecurity professionals to protect them from a global army of state-sponsored actors, cyber-criminals, hacktivists, and script kiddies alike. Unfortunately, cybersecurity teams are often understaffed, lacking advanced skills, and working in an environment of constant pressure. To gain further insight into these trends, TechTarget's Enterprise Strategy Group and the Information Systems Security Association (ISSA) surveyed 301 IT and cybersecurity professionals at organizations all over the world.

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 2023 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/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?
- At any time in their career, have cybersecurity professionals experienced a situation in which the organization they worked for was knowingly ignoring security best practices and/or regulatory compliance requirements? If put in that situation, would these cybersecurity professionals be willing to act as whistleblowers?
- How has the global cybersecurity skills shortage impacted cybersecurity professionals' organizations? How do they 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 difficult is it for organizations to recruit and hire cybersecurity professionals?
- Do organizations have a chief information security officer (CISO), or similar position, in place today? To whom does the CISO report? What do cybersecurity professionals believe is the most important quality of a successful CISO?
- Do cybersecurity professionals think their organization's CISO's level of participation with executive management and the board of directors is adequate?
- 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?

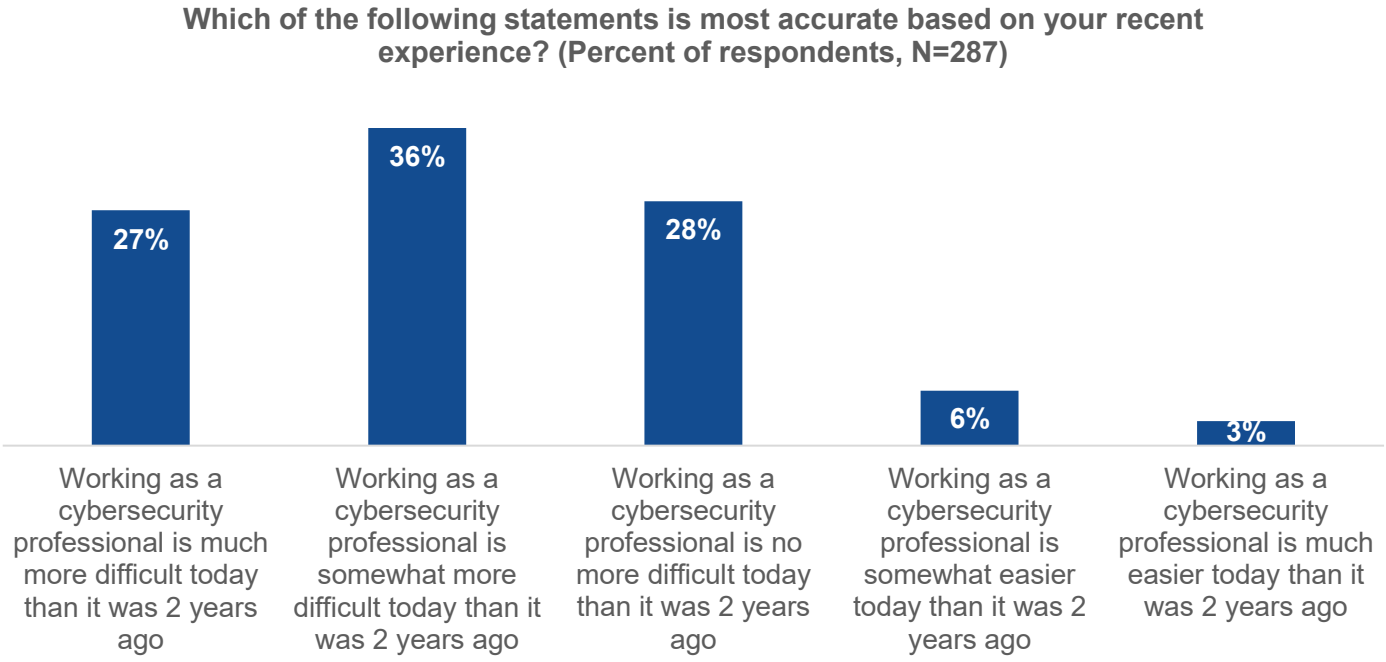
Survey participants represented a wide range of industries including manufacturing, technology, financial services, and retail/wholesale. For more details, please see the Research Methodology and Respondent Demographics sections of this report.

Research Findings

Working as a Cybersecurity Professional Is Getting Increasingly Difficult

A majority (63%) of cybersecurity professionals believe that working as a cybersecurity professional has become more difficult over the past two years (see Figure 1).

Figure 1. Most Believe Working as a Cybersecurity Professional Has become More Difficult

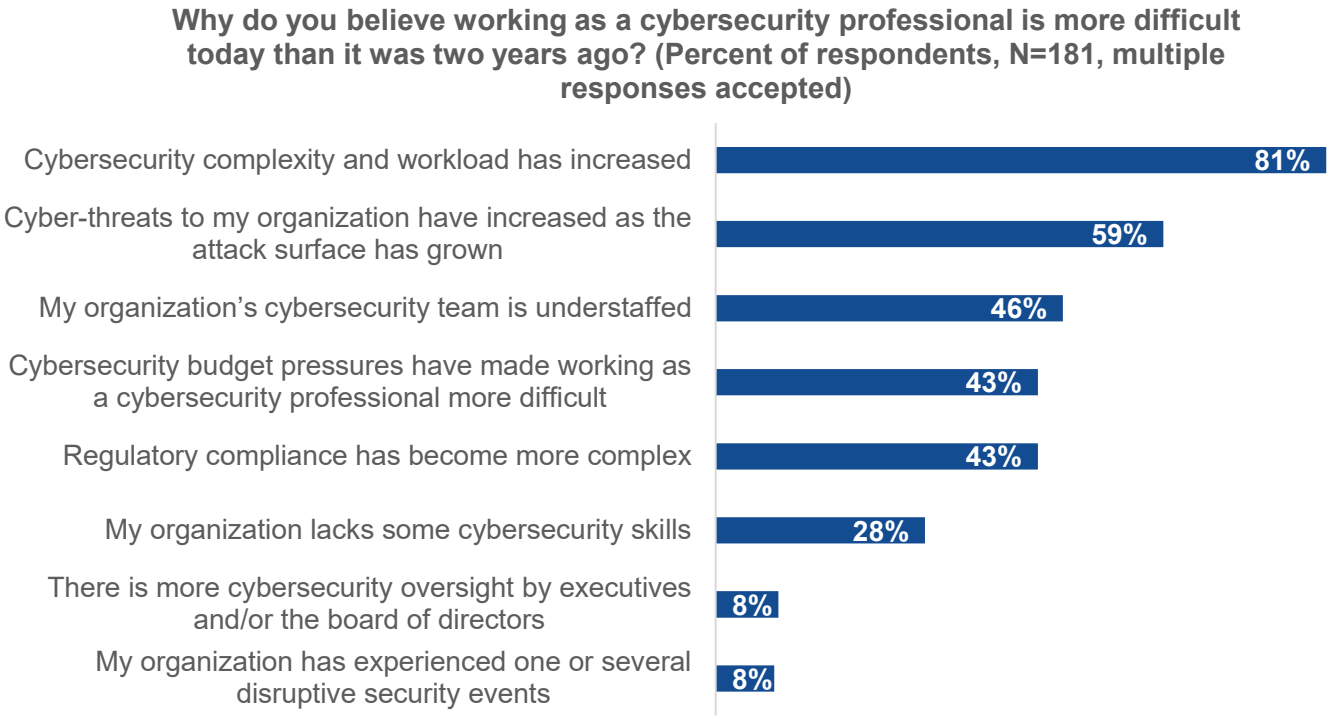


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

When asked why this was the case, more than eight in ten respondents cited both the increasing complexity and workloads associated with cybersecurity (see Figure 2). Among the other common reasons why being a cybersecurity professional is more difficult today include a growing attack surface, an understaffed security team, and continuous budget pressures. Cybersecurity pros are being asked to do more while many lack adequate resources to do so. This is a recipe for failure.

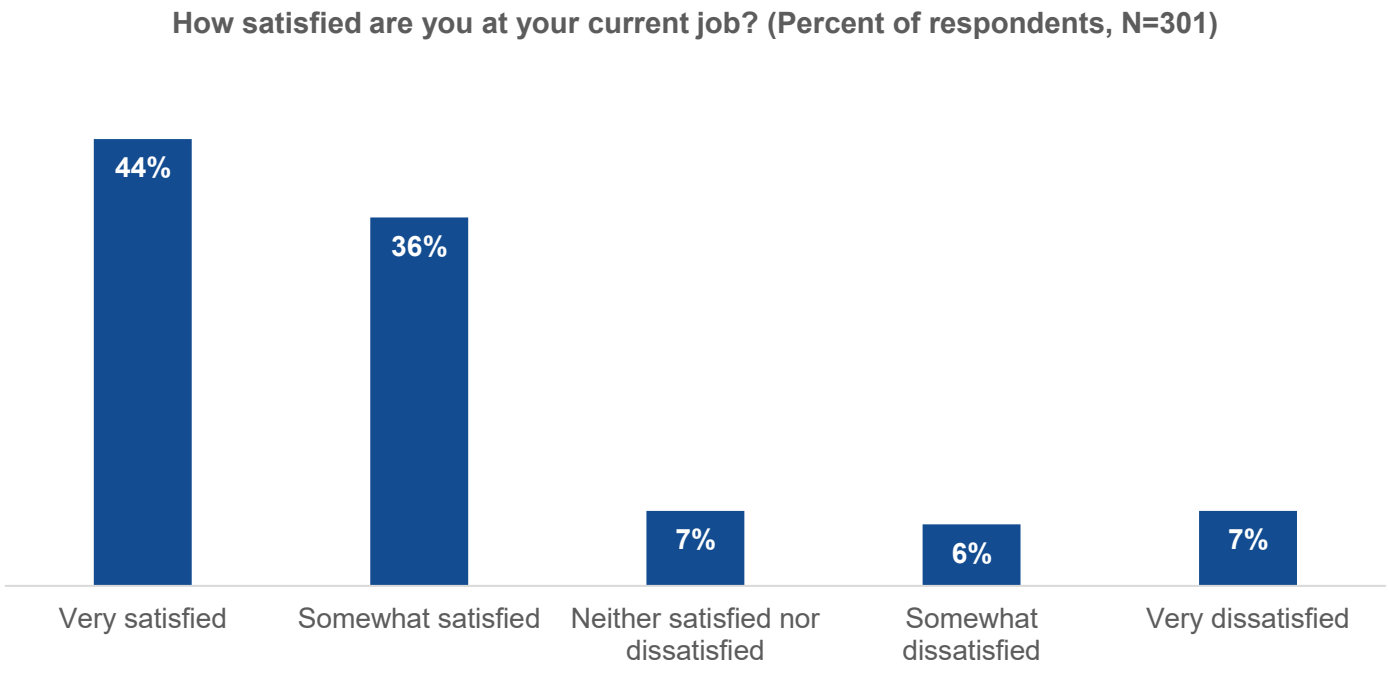
Despite cybersecurity professional challenges, 44% of survey respondents report that they are very satisfied with their current jobs (see Figure 3). This is a testament to cybersecurity professionals' dedication to the mission. However, it is worth noting that 13% of cybersecurity professionals are somewhat or very *dissatisfied* with their current position. Dissatisfied employees predictably lead to employee attrition, exacerbating the challenges described previously.

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



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

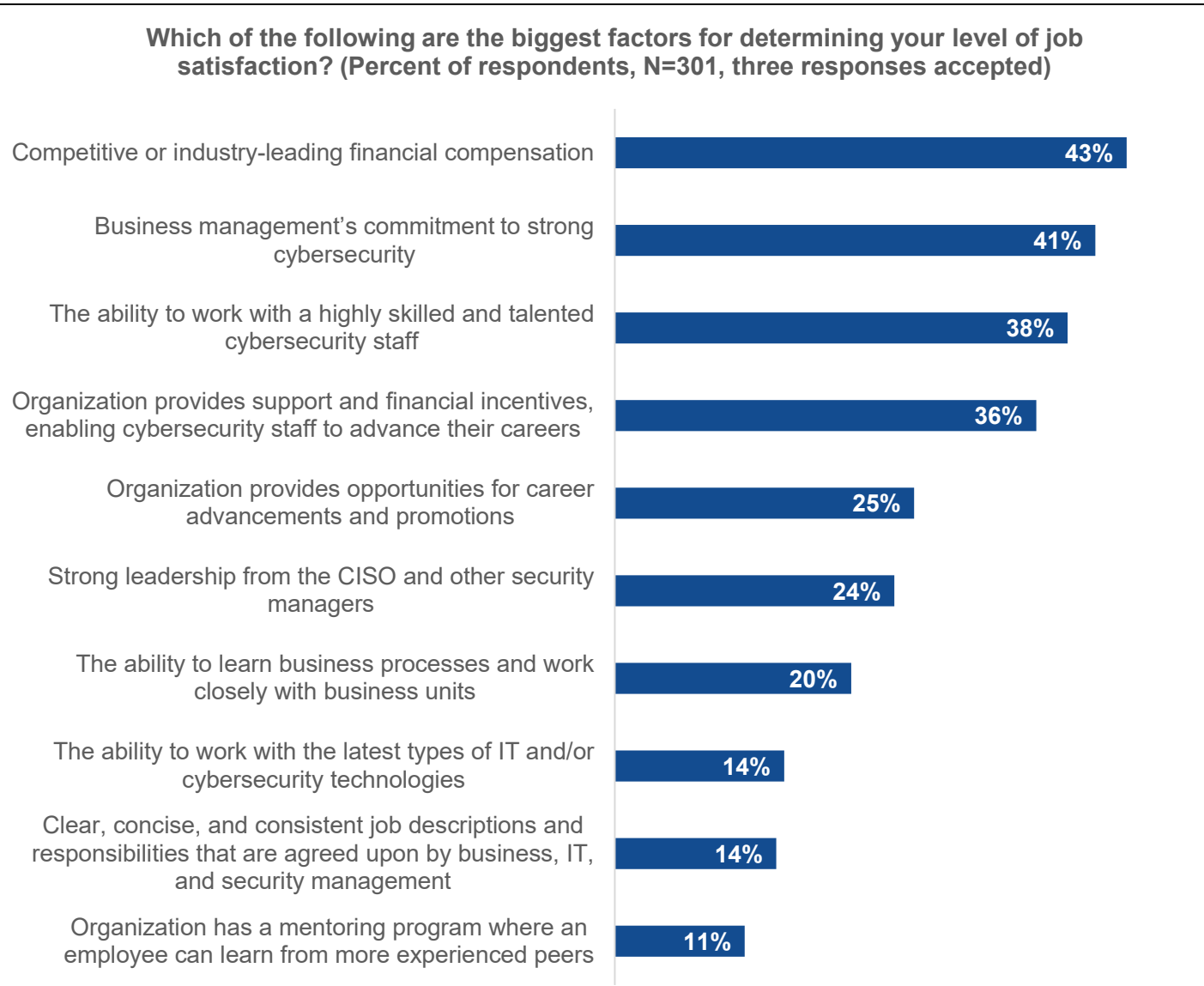
Figure 3. Satisfaction Level for Current Job Among Cybersecurity Professionals



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

What factors drive job satisfaction? Recognizing their value, cybersecurity professionals want to be paid a competitive salary with commensurate benefits (see Figure 4). Beyond individual financial incentives, cybersecurity pros equate job satisfaction to business management's commitment to cybersecurity, the ability to work with other experienced professionals, and incentives like the opportunity for continuous advanced training. It's safe to assume that dissatisfied cybersecurity professionals work at organizations lacking one or several of these attributes.

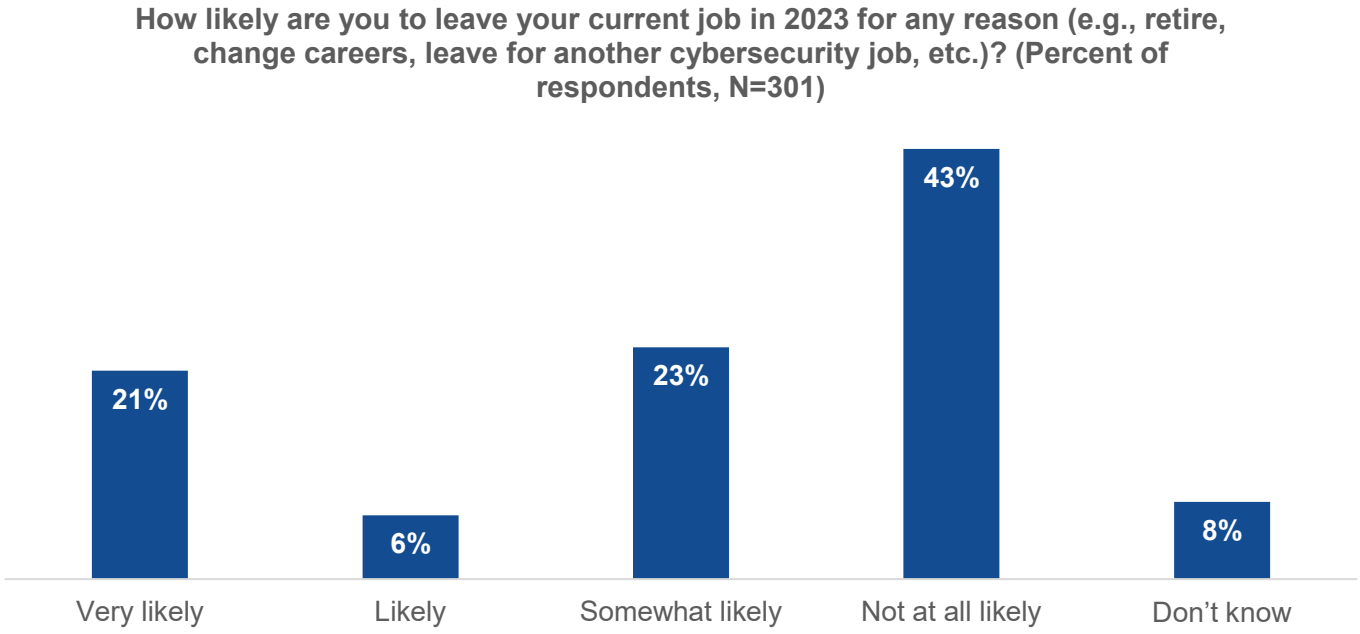
Figure 4. Biggest Factors that Determine Job Satisfaction Level



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

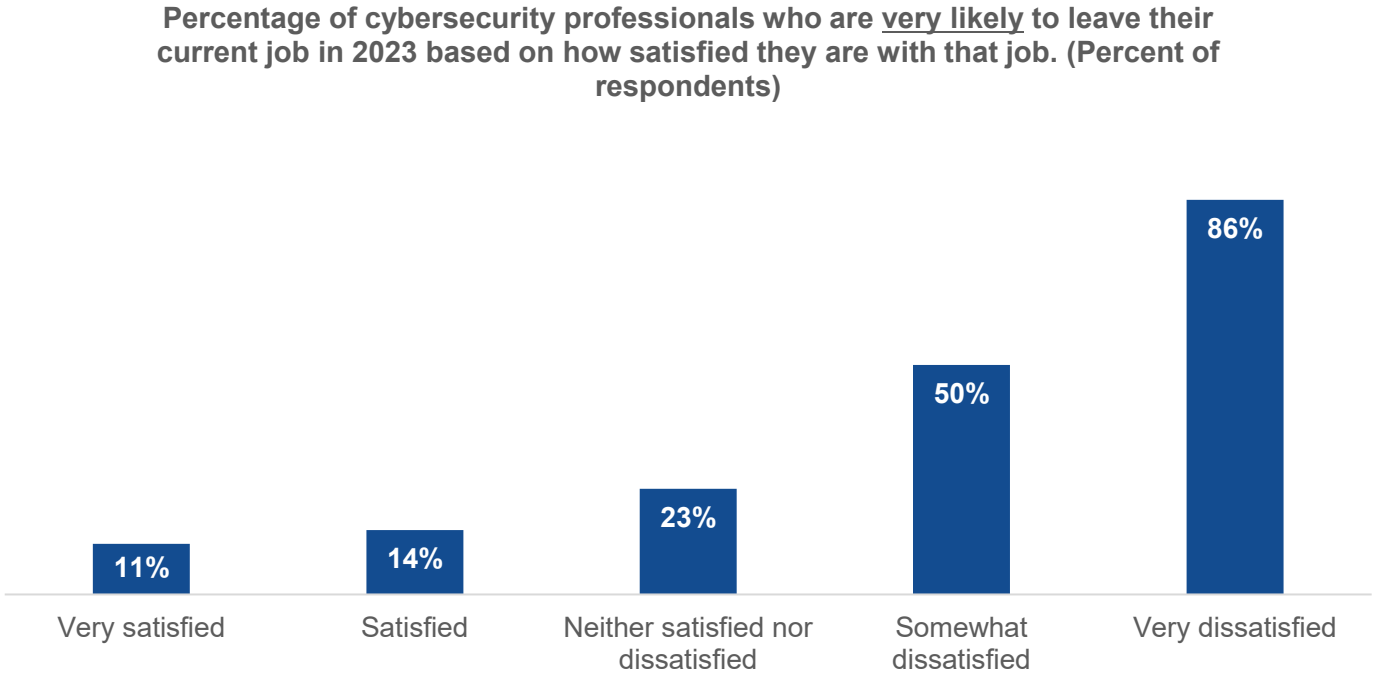
Growing job difficulties and dissatisfaction lead unavoidably to employee attrition as cybersecurity pros seek better opportunities. Indeed, half of survey participants are somewhat likely (23%), likely (6%), or very likely (21%) to leave their current jobs this year (see Figure 5). Not surprisingly, there is a strong correlation between job churn and job satisfaction as 86% of cybersecurity professionals that are *very dissatisfied* with their current jobs are also *very likely* to leave those jobs this year (see Figure 6). CISOs should coordinate with HR managers to assess and address staff satisfaction issues before key security personnel seek an exit. Organizations lacking a strong cybersecurity culture or adequate employee compensation can expect a state of constant staff churn.

Figure 5. Likelihood of Leaving Current Cybersecurity Job in 2023…



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

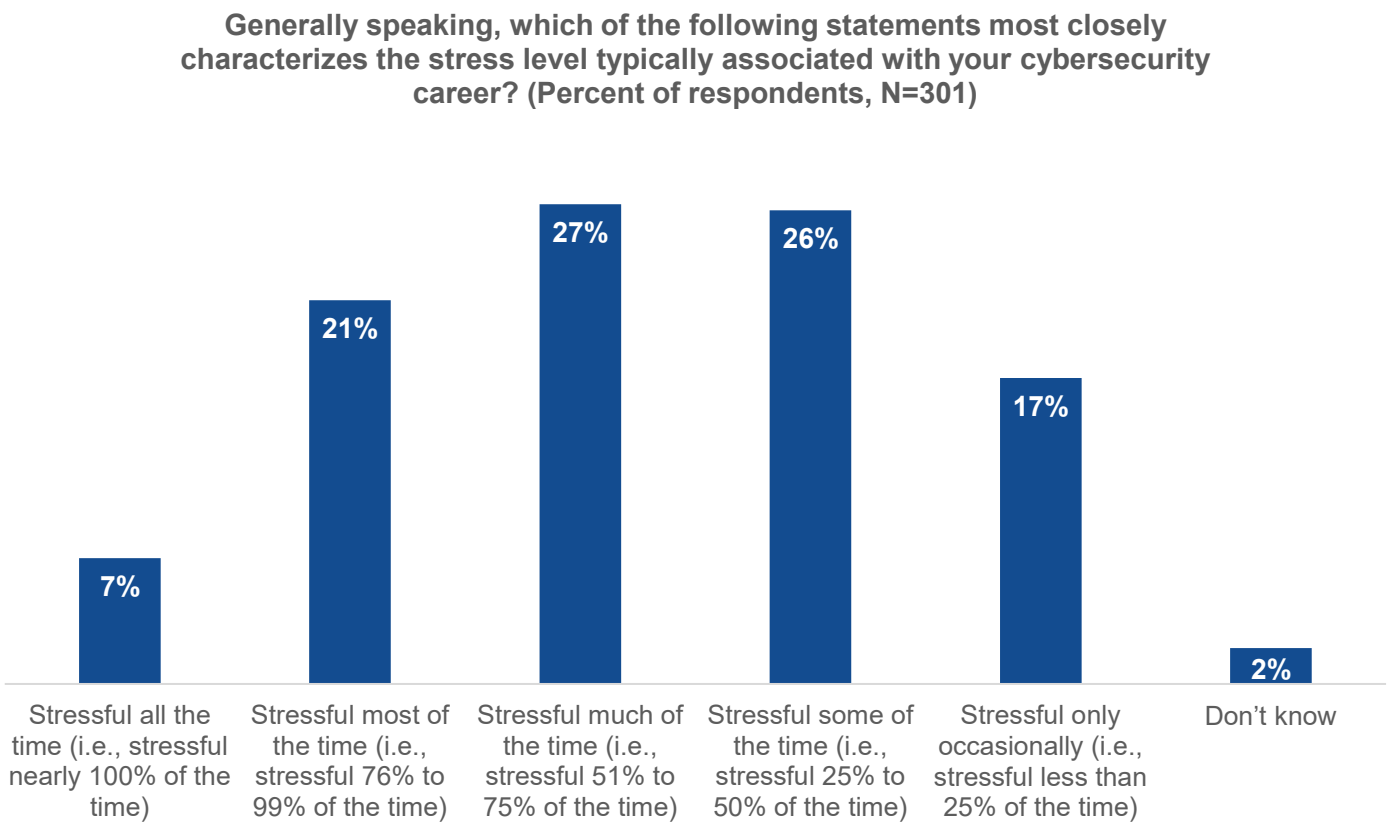
Figure 6. …Is Significantly Higher Among Those Dissatisfied with Their Current Job



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

Of course, job stress is also a critical component of job satisfaction. The data here isn't good, with 55% of cybersecurity professionals claiming they experience on-the-job stress at least half the time (see Figure 7).

Figure 7. Most Cybersecurity Professionals Report Their Jobs Are Often Stressful



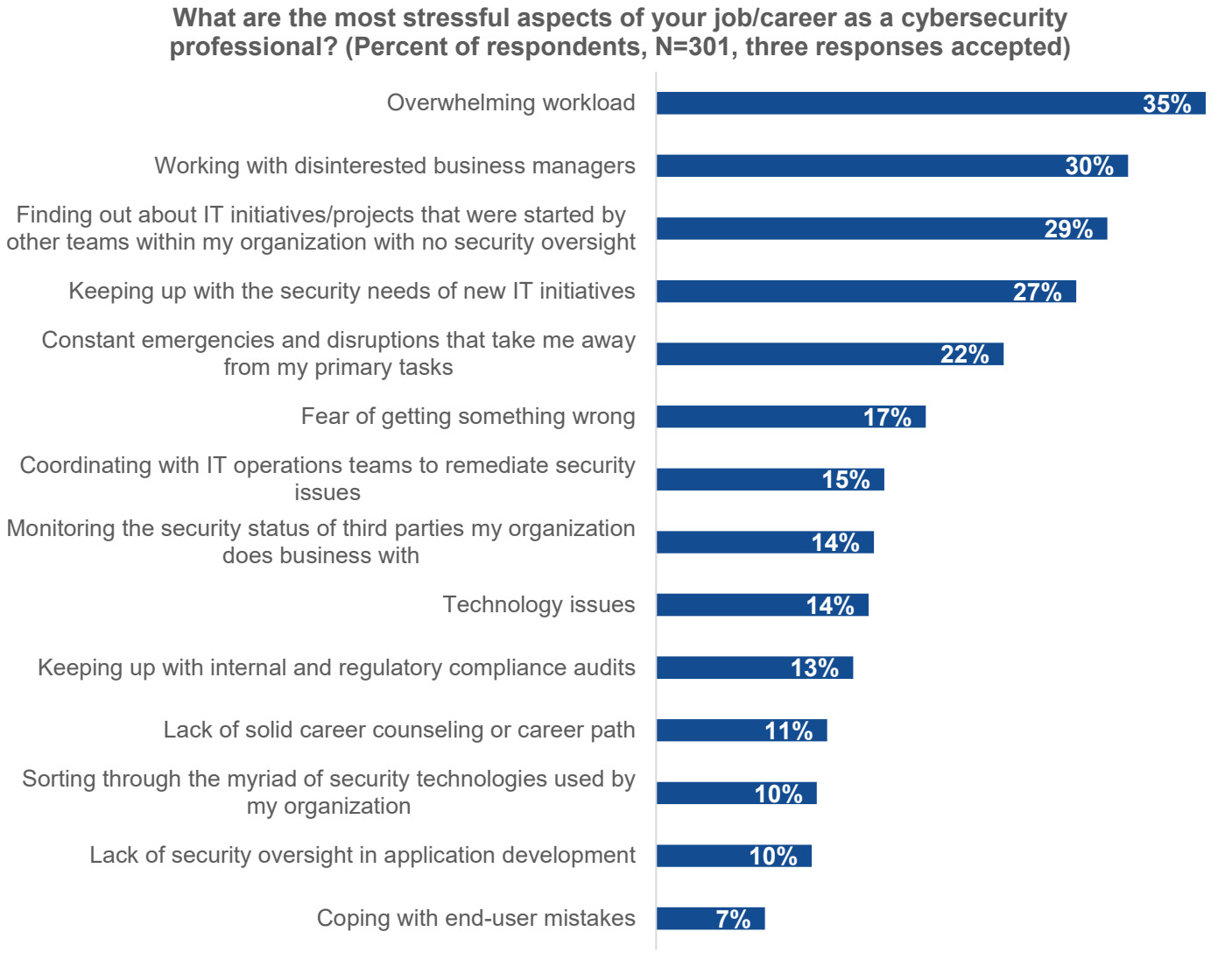
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The causes of job stress present a consistent pattern throughout the research: an overwhelming workload and working with disinterested business managers (see Figure 8). According to Table 1, the overwhelming workload is particularly stressful for cybersecurity professionals working at enterprise organizations (i.e., 1,000 or more employees), with 41% of enterprise cybersecurity pros saying the overwhelming workload is the most stressful aspect of their job versus 26% of those working at smaller organizations (i.e., fewer than 1,000 employees).

Beyond these worries, cybersecurity professionals find it stressful when they aren't included in IT initiative planning or keeping up with the security needs of IT initiatives in general. Security pros also work in an environment of constant emergencies and disruption, which is a stressful situation. It is worth noting that the three most commonly cited stressful aspects of a cybersecurity profession remained consistent in the 2021 and 2023 iterations of this study.[1]

[1] Source: Enterprise Strategy Group Research Report, *The Life and Times of Cybersecurity Professionals 2021 Volume V*, July 2021. All references to past iterations of this study come from this research report.

Figure 8. Most Stressful Aspects of Cybersecurity Jobs/Careers



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

Table 1. Overwhelming Workloads Are a Much More Common Stressor for Enterprise Organizations

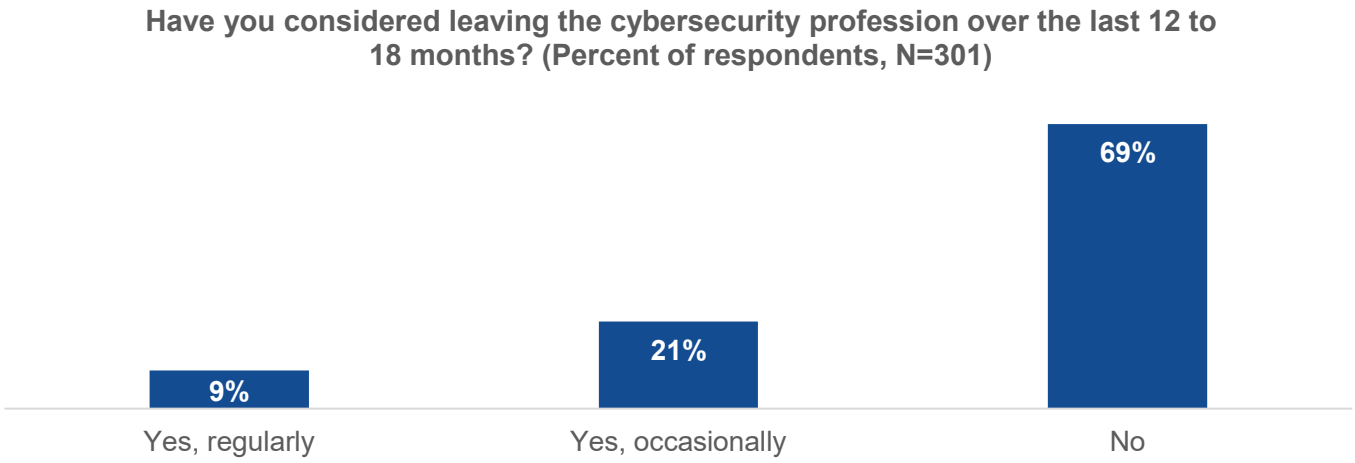
	Enterprise organizations (1,000 or more employees)	Small/midmarket organizations (fewer than 1,000 employees)
Overwhelming workload	41%	26%

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

The good news is that most cybersecurity professionals are dedicated to the profession for the foreseeable future. The bad news? Nearly one-third of those surveyed have considered leaving the profession on an occasional (21%) or regular (9%) basis over the last 12-18 months (see Figure 9). The most common reasons driving these thoughts

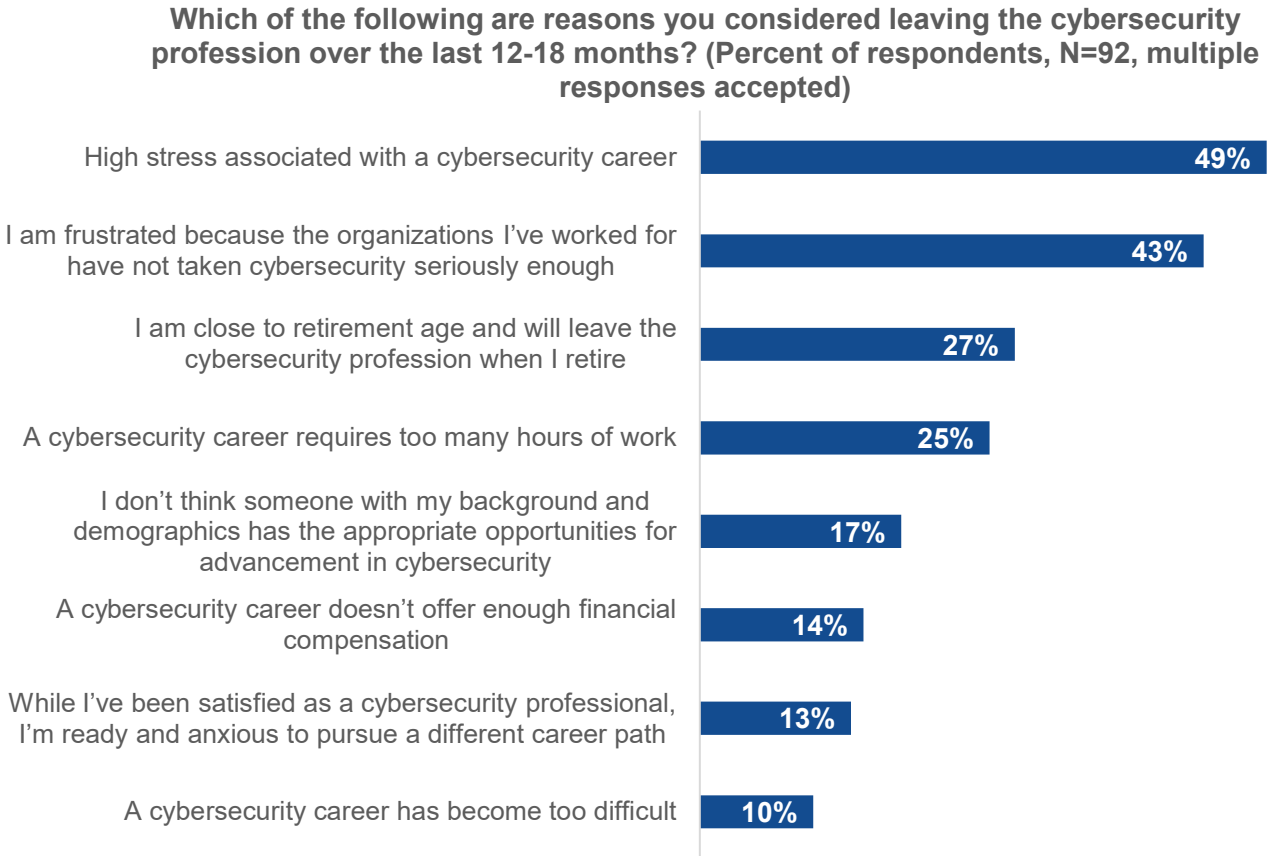
include the stress factors that are associated with a cybersecurity career, a lack of cybersecurity commitment by their employers, or an impending plan to retire (see Figure 10).

Figure 9. Nearly One-third of Cybersecurity Pros Considered Leaving the Profession Recently



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

Figure 10. Reasons for Considering Leaving the Cybersecurity Profession



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

As cybersecurity professionals assess job opportunities, they must figure out the best avenues for career advancement. The data points to a balance of "who you know" and "what you know" as key to success here. Indeed, according to Figure 11, survey respondents believe networking with other cybersecurity professionals, participating in training sessions, attending industry events, and joining a cybersecurity professional organization are part of a career development strategy. It is also advantageous to gain experience across many different roles and attain appropriate security certifications.

Figure 11. Actions That Would Be Most Helpful for Cybersecurity Career Advancement

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

Despite the cybersecurity skills shortage, many entry-level cybersecurity candidates lament that it can be difficult to break into the profession. What should they do to address the hiring bottleneck? Cybersecurity pros recommend that they seek apprenticeships, internships, or mentors; get a basic cybersecurity certification (i.e., ComptTIA Security+, ISACA Cybersecurity Fundamentals, GIAC Information Security Fundamentals (GISF), etc.); and network with a local chapter of a professional organization like ISSA (see Figure 12). While these best practices should help, it still may be difficult for inexperienced (but ambitious) individuals to attain their first job. Enterprise Strategy Group and ISSA recommend persistence here as a first cybersecurity job can lead to fruitful career opportunities.

Figure 12. *Primary* Piece of Advice for Prospective Cybersecurity Professionals

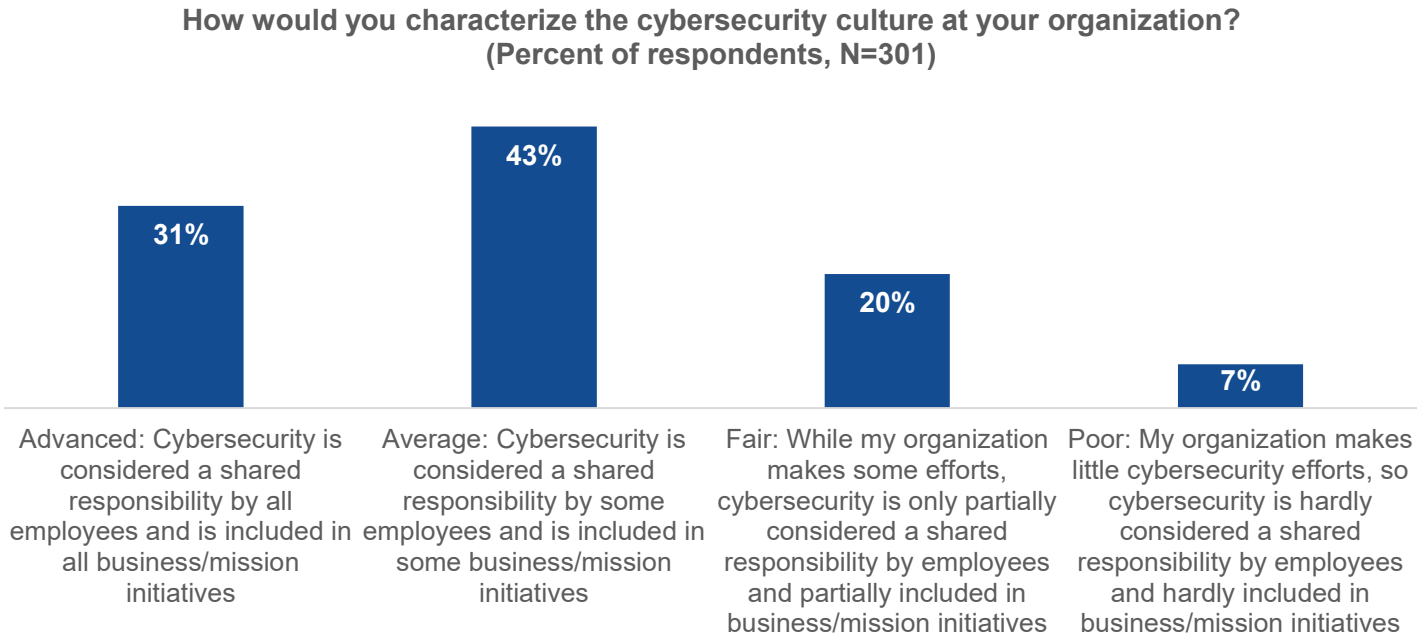
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Cybersecurity Programs Could Be Improved by Embracing a Cybersecurity Culture

Not many cybersecurity professionals are bullish overall about the state of cybersecurity culture at their organizations. Indeed, less than one-third (31%) claim their organization has an advanced cybersecurity culture, where cybersecurity is considered a shared responsibility and part of the organization's business initiatives (see Figure 13). Conversely, 43% rate their organization's cybersecurity culture as average, with more than one-quarter (27%) giving their organization a rating of fair or poor.

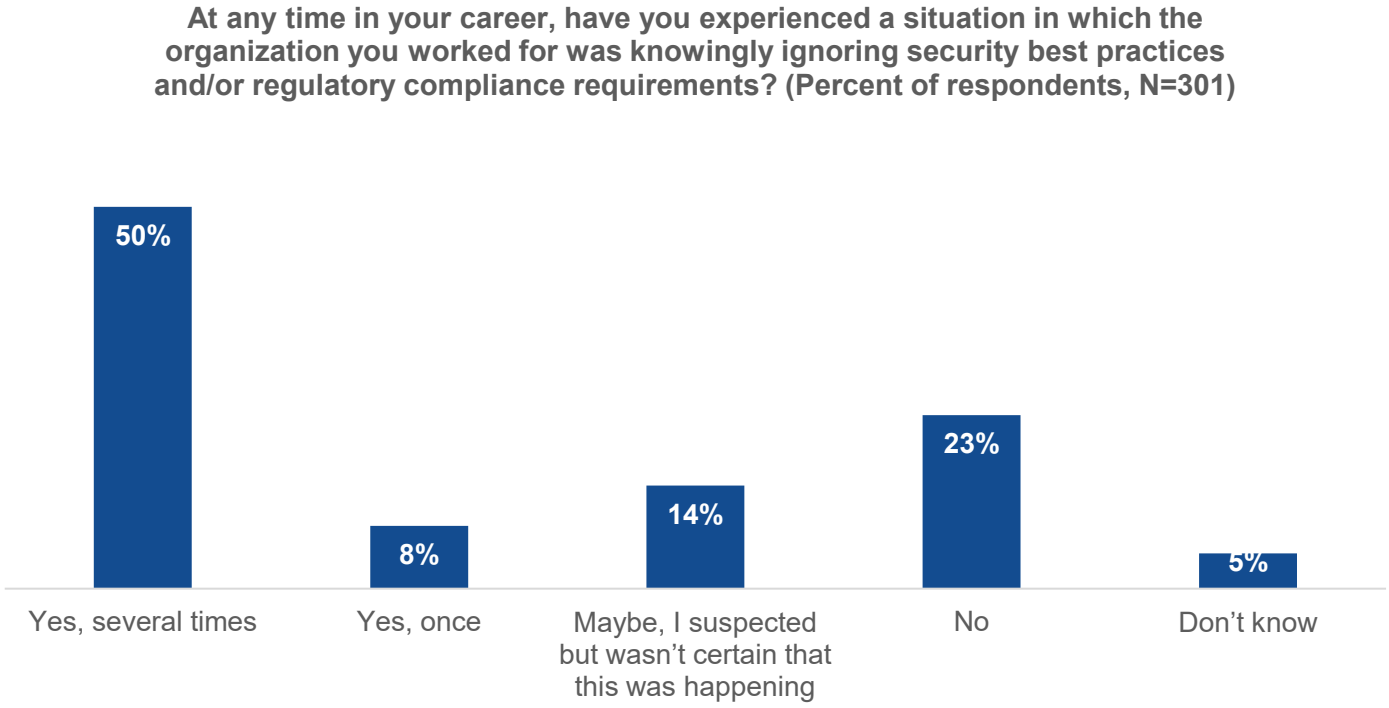
While most cybersecurity professionals report an advanced or average cybersecurity culture at their current employer, many have worked for at least one organization that knowingly ignored security best practices and/or regulatory compliance requirements in the past. Specifically, more than half of respondents say they have been in one (8%) or several (50%) situations in which an organization they worked for was knowingly ignoring security best practices and/or regulatory compliance requirements (see Figure 14).

Figure 13. Characterization of the Cybersecurity Culture at Organizations



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

Figure 14. Career History with Organizations Apathetic to Cybersecurity

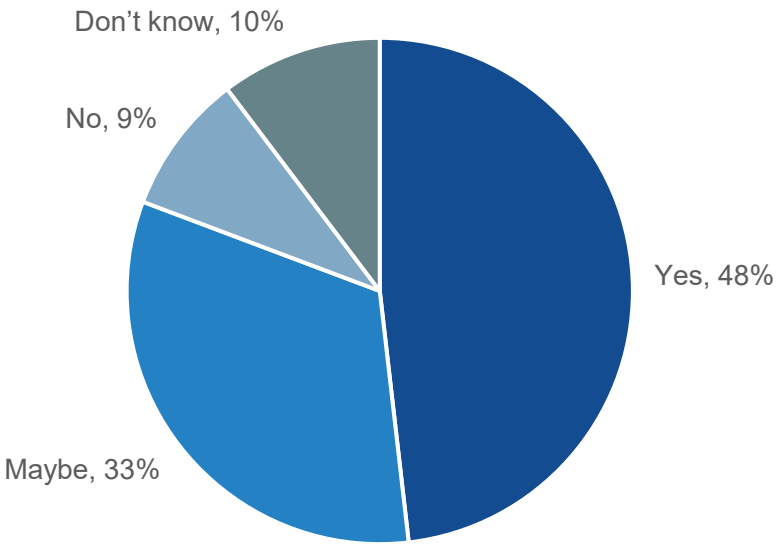


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Cybersecurity professionals may be asked to compromise their professional ethics in situations where their organization knowingly ignores security best practices and/or regulatory compliance requirements. According to Figure 15, many seem unwilling to do so and would act as a whistleblower if this state of affairs occurred. The willingness to be a whistleblower was true of most cybersecurity professionals regardless of their positions, years of experience, or the size of their organizations.

Figure 15. Cybersecurity Pros Willingness to Act as Whistleblowers

If you were put in a situation in which the organization you worked for knowingly ignored security best practices and/or regulatory compliance requirements, despite warnings from the security team, would you be willing to act as a whistleblower? (Percent of respondents, N=301)

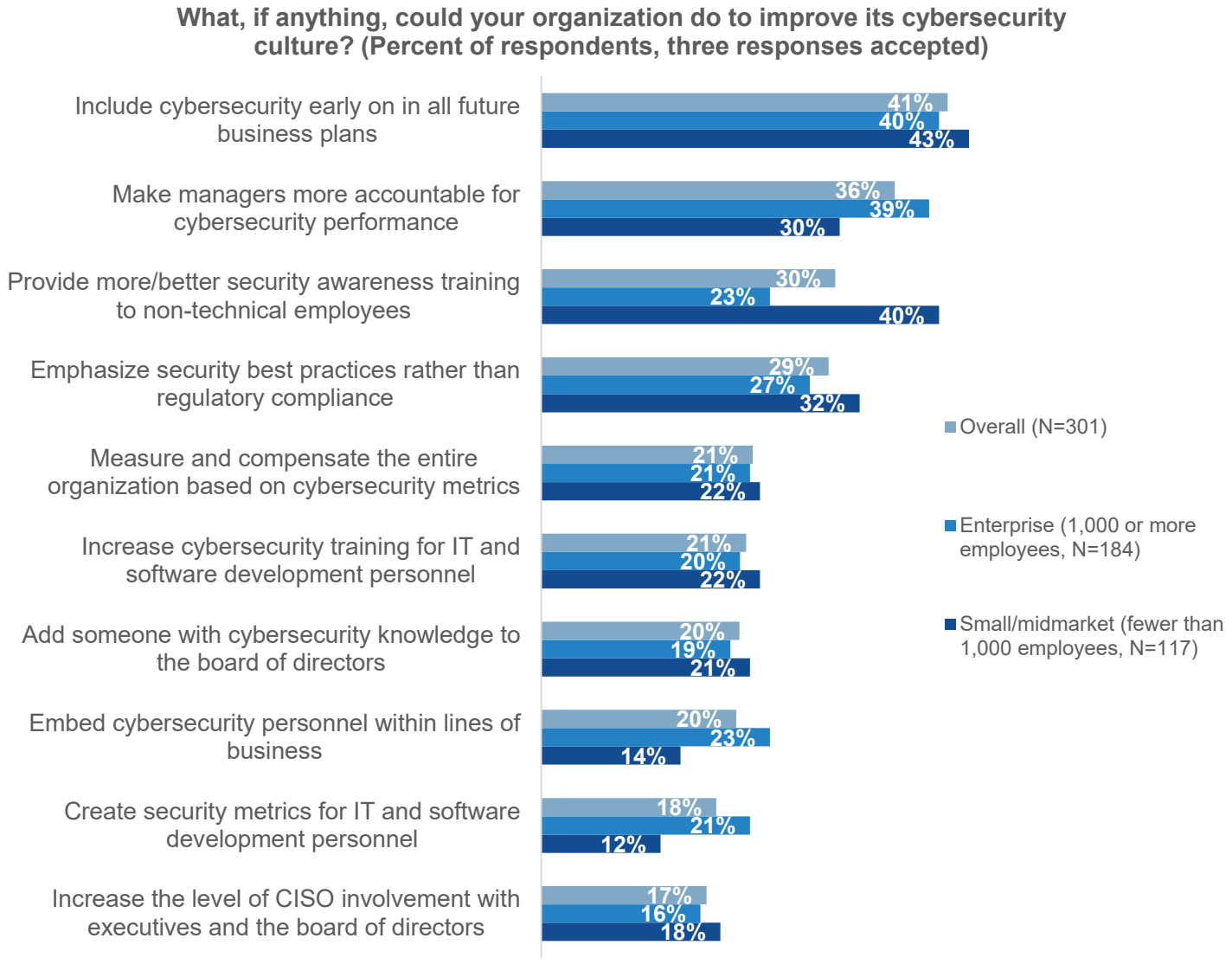


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

How can organizations improve their cybersecurity culture? Cybersecurity professionals point to actions like including cybersecurity considerations in business planning, providing more/better security awareness training, and emphasizing security best practices rather than regulatory compliance (see Figure 16). Note that 36% suggest making managers more accountable for cybersecurity performance. Certainly, business managers should support cybersecurity programs and champion cybersecurity culture, but making them accountable may be a bridge too far unless they knowingly ignore corporate governance or established security policies.

Responses to this question varied by organizational size. Smaller organizations (i.e., those with fewer than 1,000 employees) emphasized providing more and/or better security awareness training (40% versus 23% for organizations with more than 1,000 employees). For their part, enterprise organizations were more likely to suggest creating security metrics for IT and software development personnel (21% versus 13%) and embedding cybersecurity personnel within lines of business (23% versus 13%).

Figure 16. Steps Organizations Could Take to Improve Cybersecurity Culture

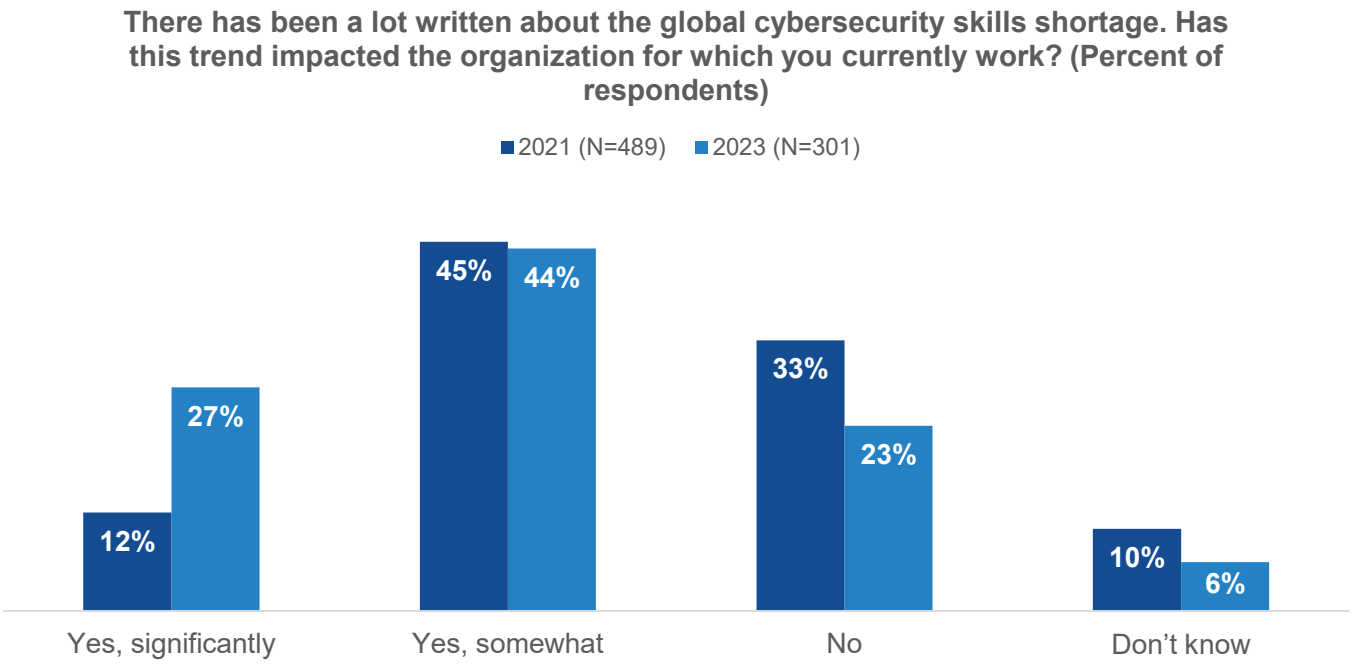


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The Cybersecurity Skills Shortage Is Not Improving, and Organizations Are Not Responding With the Right Countermeasures

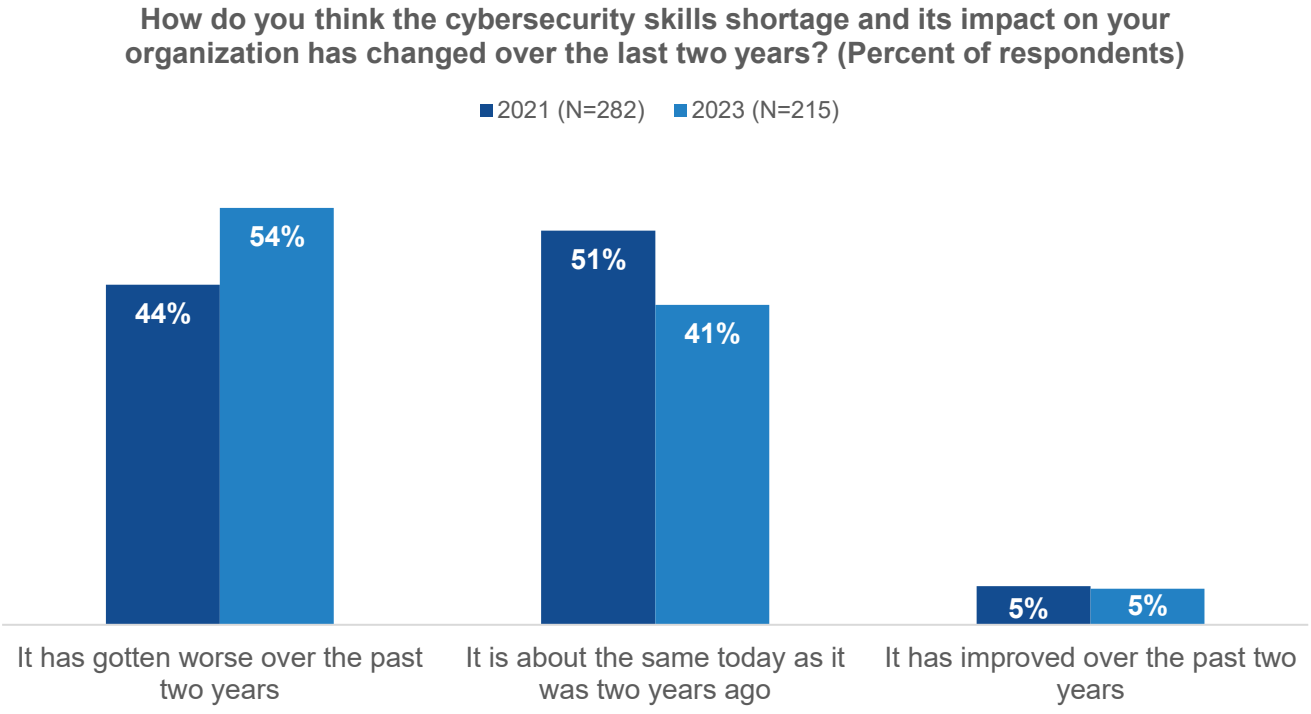
After six editions of *The Life and Times of Cybersecurity Professionals*, this iteration of the research clearly indicates that the cybersecurity skills shortage continues unabated. In 2023, 71% of organizations claim to be impacted by cybersecurity skills shortage, which is an increase of 14% from 2021 (see Figure 17). Alarmingly, those citing significant impacts also increased from 12% in 2021 to 27% in 2023. There is also an interesting correlation whereby organizations with the largest cybersecurity teams are those experiencing significant impact from the cybersecurity skills shortage. These firms may have specialized needs that can't be addressed or simply need even larger security teams than they currently have. It is also distressing that more than half (54%) believe the skills shortage has gotten worse over the past two years, a 10% increase over 2021 (see Figure 18).

Figure 17. The Global Cybersecurity Skills Shortage Is Still Impacting Organizations…



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

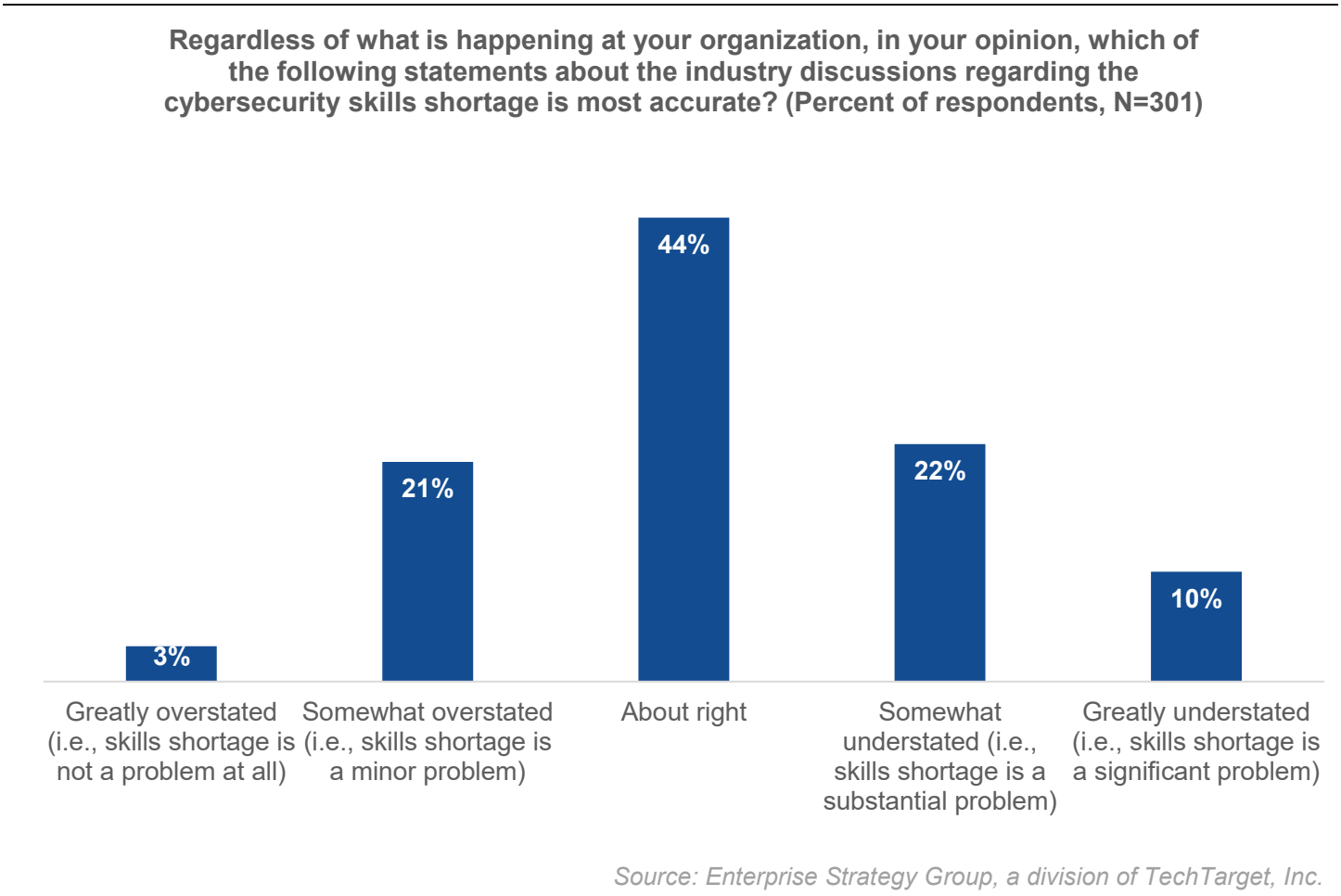
Figure 18. …And It Continues to Get Worse



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

Furthermore, Figure 19 reveals that nearly one-third (32%) of cybersecurity professionals believe the impact of the cybersecurity skills shortage is actually understated (i.e., the cybersecurity skill shortage is a *more substantial* problem than reported). CISOs must recognize that there is no end in sight to the security skills shortage and consider its implications in every decision they make. In lieu of security staff or advanced skills, organizations must include process automation, advanced analytics, generative AI, and managed services as part of their cybersecurity strategy.

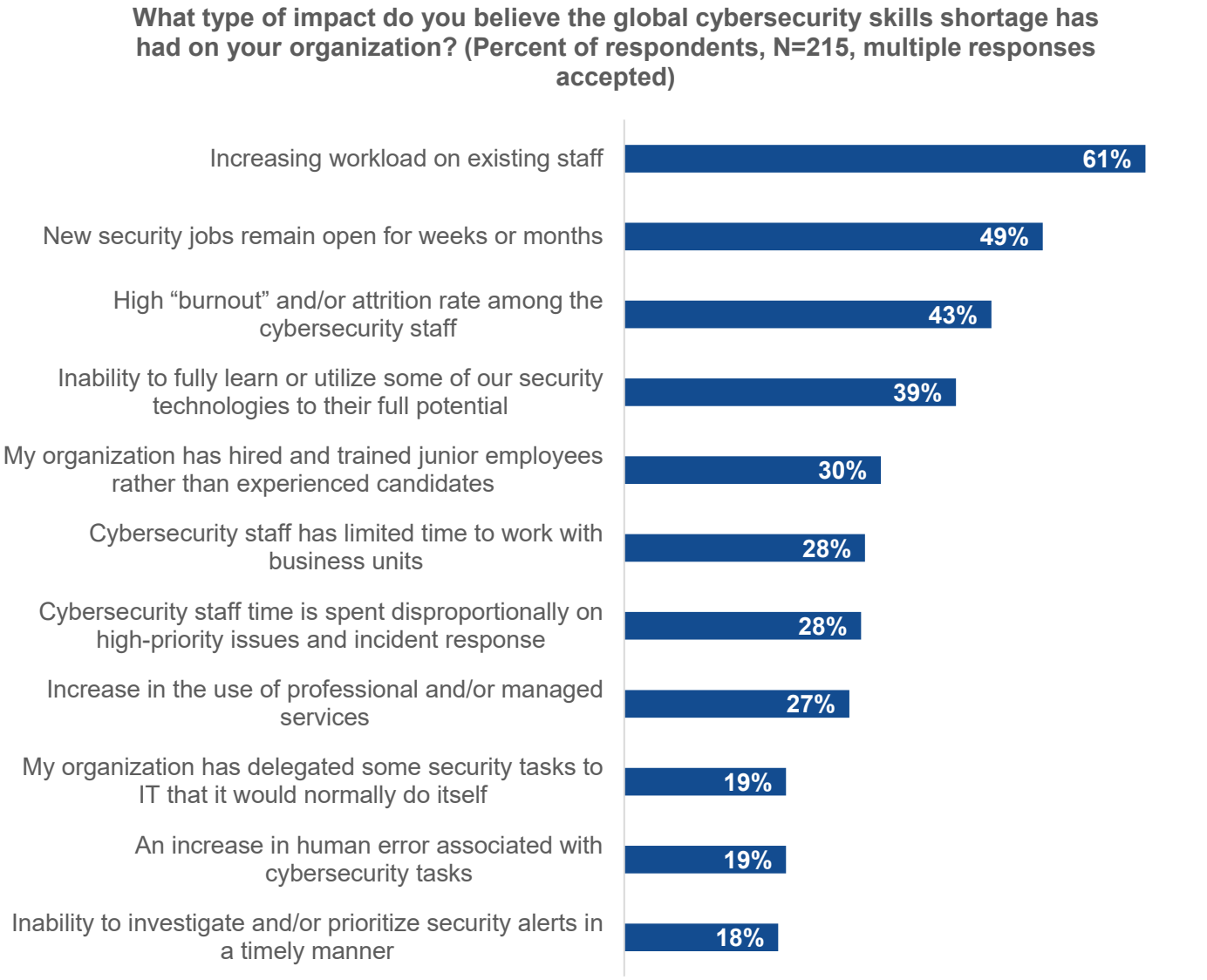
Figure 19. Perception of the Cybersecurity Skills Shortage



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

Those organizations impacted by the cybersecurity skills shortage report ramifications like an increasing workload on existing staff, lengthy job openings, and high burnout rates leading to staff attrition (see Figure 20). Technology alone can't rectify this situation, evidenced by the fact that 39% of organizations claim that the skills shortage leads to the inability to learn or utilize some security technologies to their full potential.

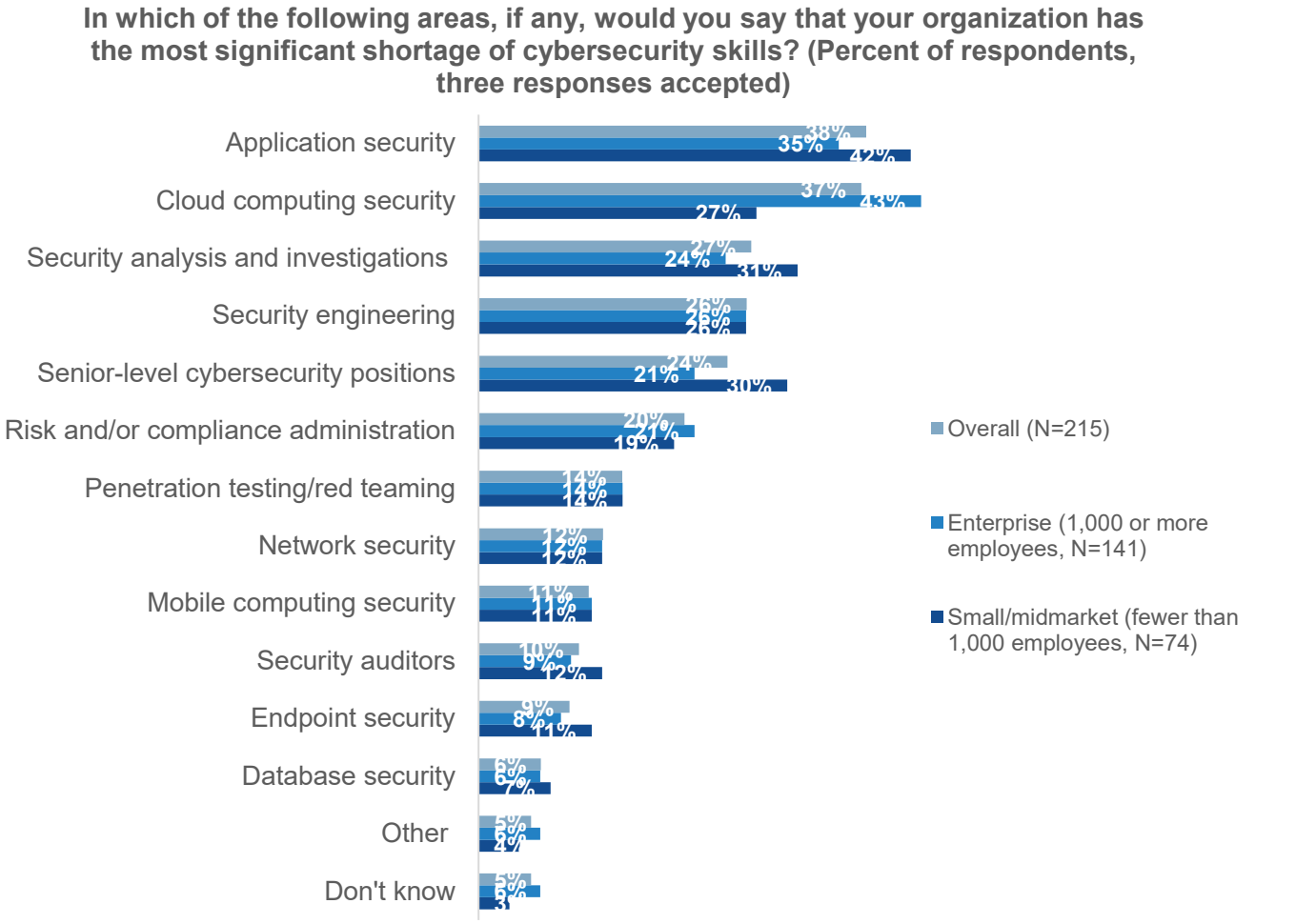
Figure 20. Impact of the Cybersecurity Skills Shortage



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

As in past years, organizations have the most acute skills deficits in areas like application security, cloud security, security analysis, and security engineering (see Figure 21). The cloud computing security skills shortage disproportionally impacts larger organizations, with 43% of enterprises claiming to have a shortage of cloud security skills, compared with 27% of organizations with fewer than 1,000 employees. This reflects the fact that many enterprises are moving workloads and developing cloud-native applications at a faster pace and larger scale than smaller firms. In this scenario, a cloud security skills deficit represents a significant risk.

Figure 21. Impact of the Cybersecurity Skills Shortage

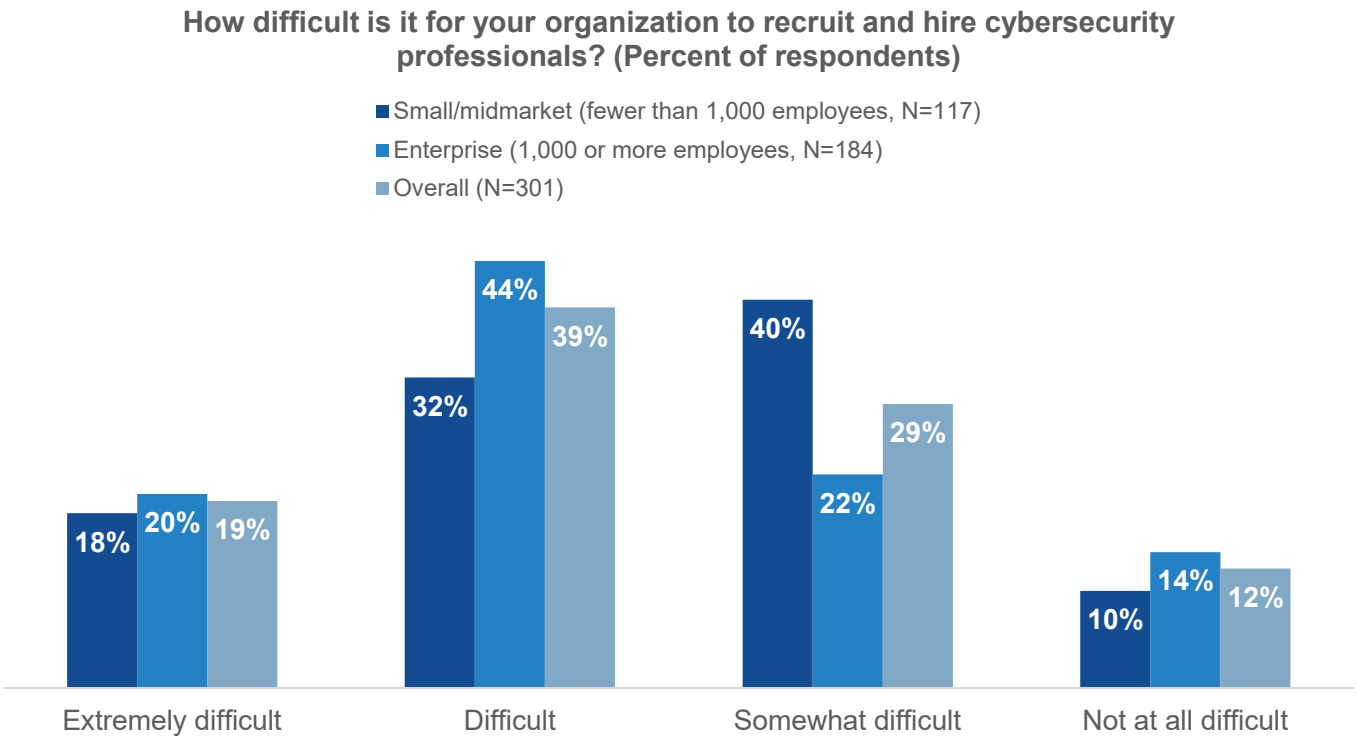


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Within the overall survey population, more than half of respondents say it is difficult (39%) or extremely difficult (19%) to recruit and hire cybersecurity professionals (see Figure 22). Larger organizations have a more difficult time than smaller ones as 64% of enterprises claim it is extremely difficult or difficult to recruit and hire cybersecurity professionals, compared with 50% of those with fewer than 1,000 employees.

Once again, this data reinforces the fact that few if any organizations can hire their way out of staff shortages or skills shortfalls. Piling more work on existing staff is also a recipe for failure. CISOs must embrace a "shift left" mentality in their security programs, adopting initiatives around security hygiene and posture management, exploit management, and a threat-informed defense (i.e., security controls based on the MITRE attack framework, threat intelligence analysis, and continuous security testing).

Figure 22. Degree of Difficulty Recruiting and Hiring Cybersecurity Staff



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

What else could organizations do to better counteract the cybersecurity skills shortage? As seen in Figure 23 and Table 2, some suggestions are obvious, like increasing security staff compensation (up 22% from 2021), providing incentives for certifications or participation in industry events (up 17% from 2021), and increasing training commitments, but others are more nuanced. For example, security professionals recommend educating HR and recruiters (up 11% from 2021) so they have a better idea of how to recruit new candidates, or modifying job requirements so they align better with typical levels of experience. This will take a commitment from the CISO or a senior security manager. Additional suggestions like creating a security internship program will also require a collective effort between security and HR departments.

Overall, these suggestions will require a greater cybersecurity commitment across the organization, and much closer collaboration between CISOs and HR executives.

Figure 23. Compensation, Incentives, and Education Most Common Actions to Address Skills Shortage

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

Table 2. Compensation, Incentives, and Education Biggest Year-over-year Movers

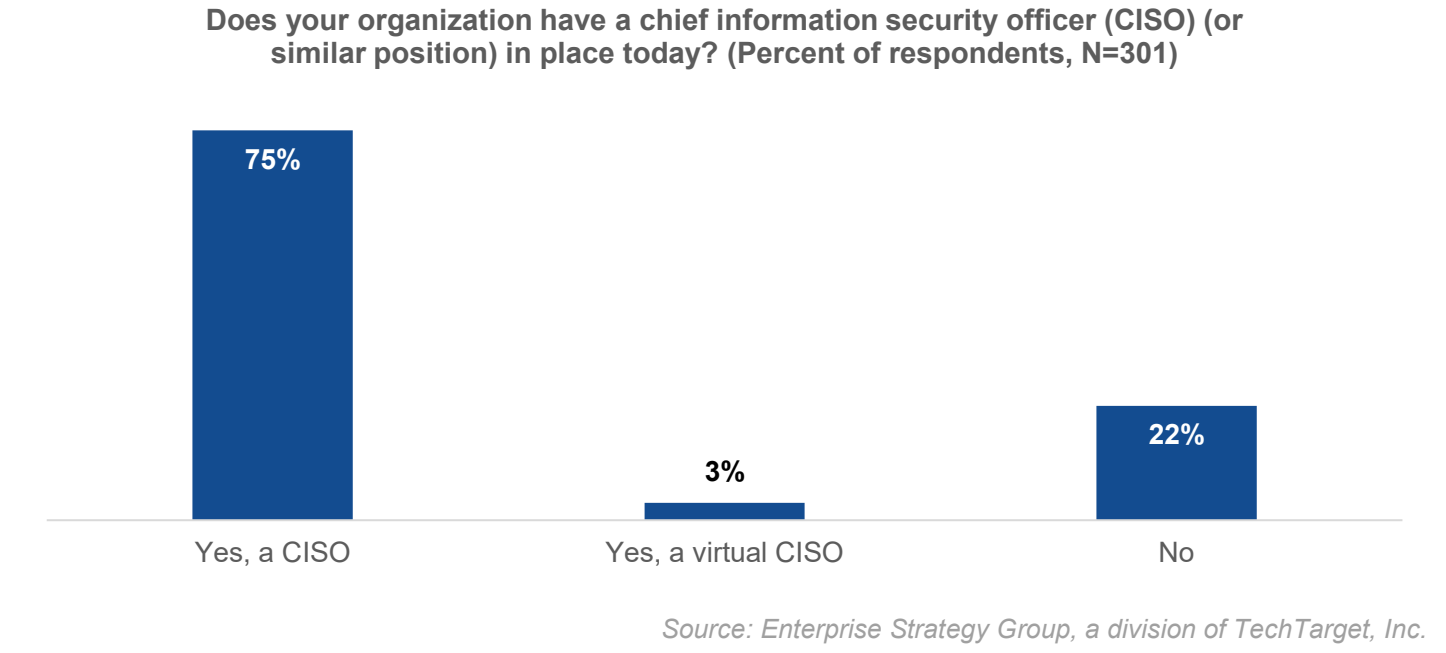
	2021 (N=282)	2023 (N=129)
Increase compensation levels to make them competitive with other organizations in our industry/geography	37%	59%
Provide incentives like paying for certifications and participation in industry events as part of compensation packages	35%	52%
Better educate HR and recruiters on our cybersecurity needs so they can better target recruitment	30%	41%

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

CISO Success Depends Upon Leadership and Communication Skills

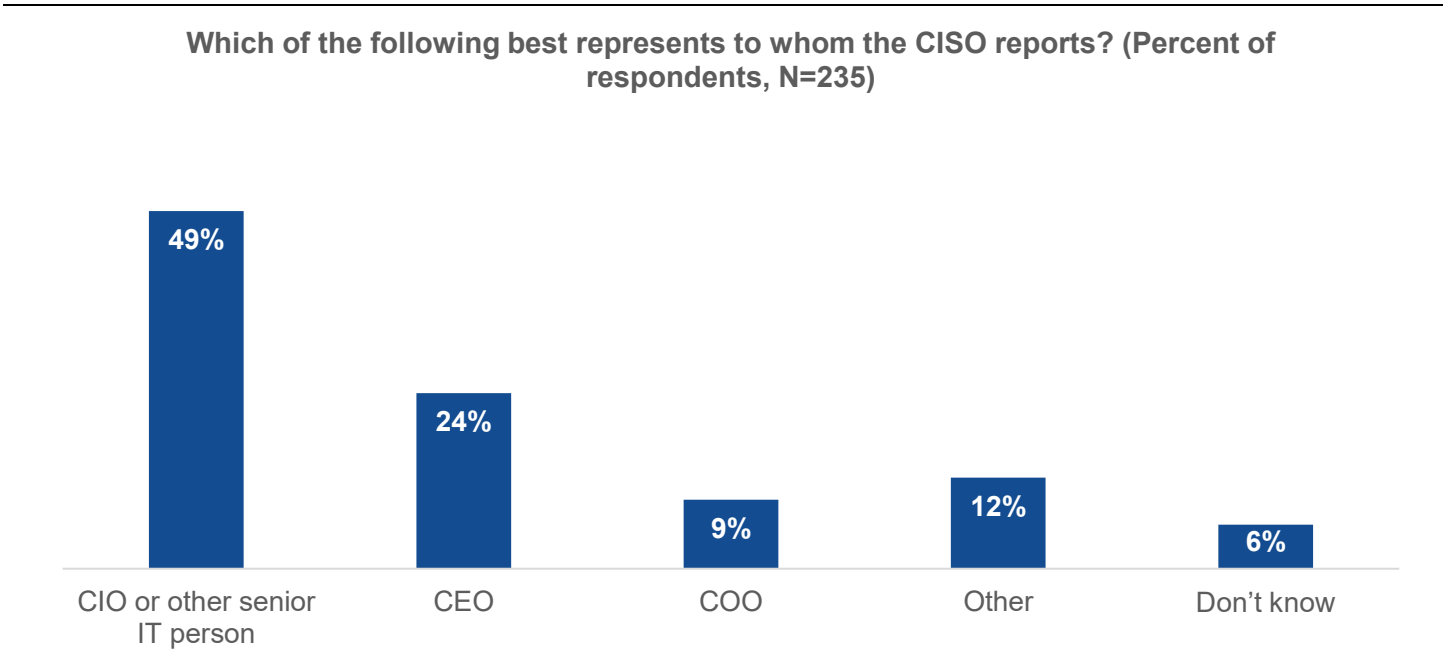
More than three-quarters (78%) of all survey respondents work at an organization with a CISO or virtual CISO (see Figure 24). Almost half (49%) of these CISOs report to the CIO or other senior IT manager, while nearly one-quarter (24%) report directly to the CEO (see Figure 25).

Figure 24. Most Organizations Have a CISO in Place Today



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

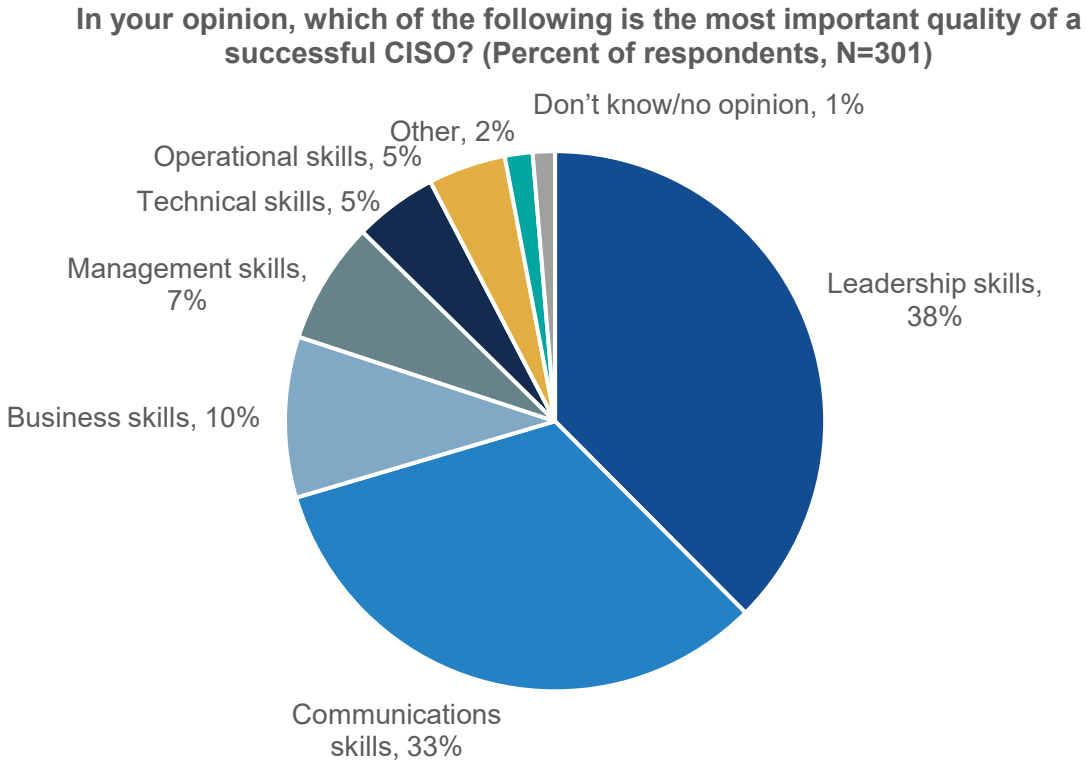
Figure 25. Most CISOs Report to CIOs or Other Senior IT Leadership



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

When asked to identify the qualities that make CISOs successful, nearly three-quarters pointed toward leadership (38%) or communications (33%) skills (see Figure 26). These qualities are certainly important for championing the security program, directing staff, and interacting with executives and the board. Nevertheless, modern CISOs must be equal parts business and technical executive. In other words, they must apply adequate technical controls to critical business processes and assets. Perhaps security professionals believe business and technical skills must be foundational for CISOs, but they are crucial toward the efficacy of aligning security with the organization's mission.

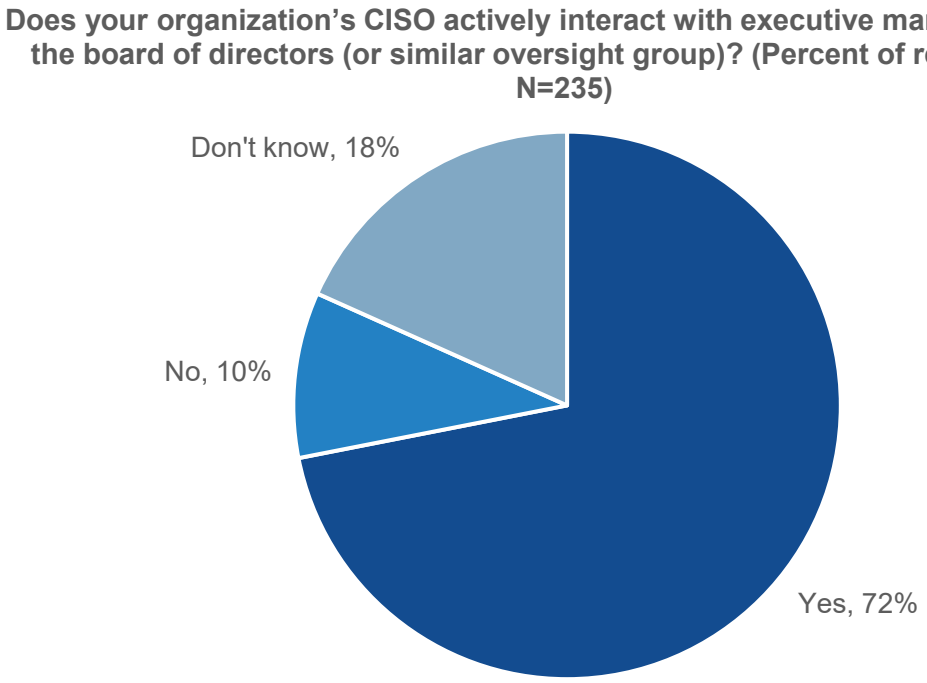
Figure 26. Most Important Quality of a Successful CISO



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

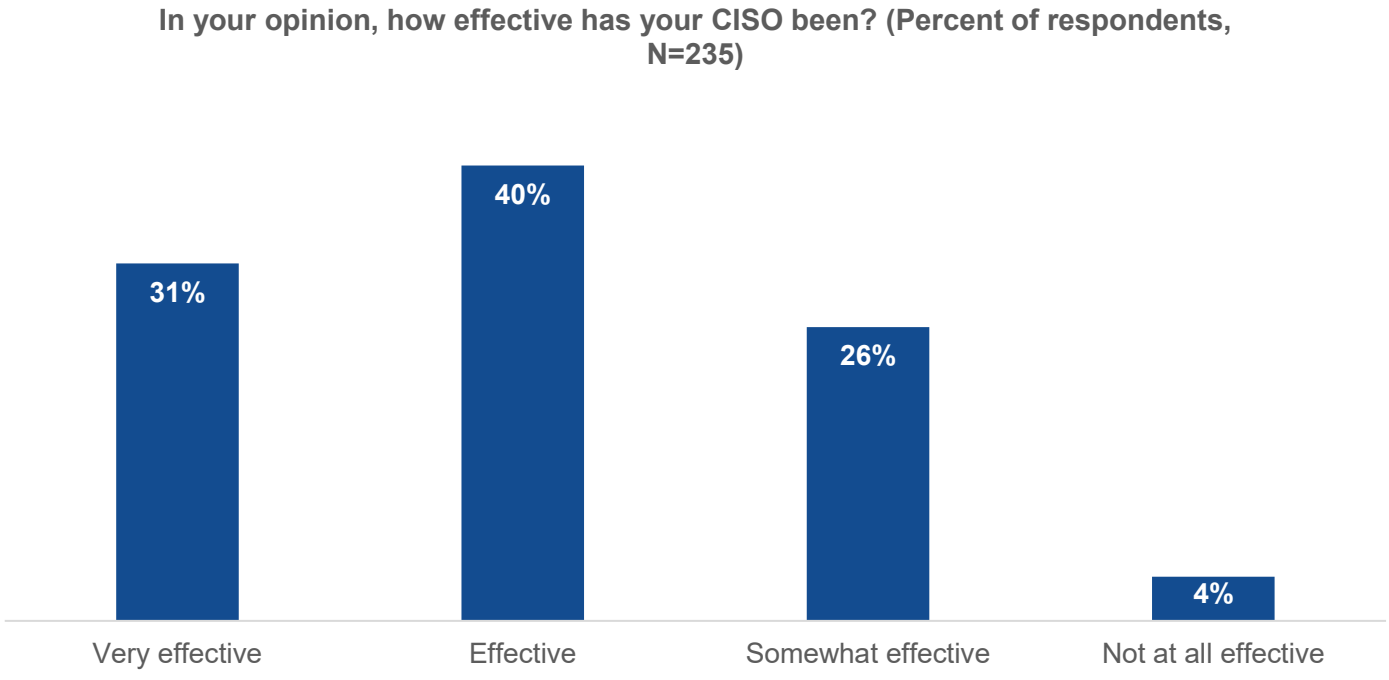
In most cases (72%), the CISO actively interacts directly with the board of directors or similar oversight body. This is a bit of good news as it represents an 11% increase from 2021 (see Figure 27). It's likely that pernicious threats and regulatory requirements have forced this change. According to Figure 28, nearly one-third (31%) of those organizations employing a CISO believe their CISO has been very effective, 40% believe their CISO has been effective, and 26% say their CISO has been somewhat effective. Only 4% categorize their CISO as not at all effective.

Figure 27. Most CISOs Actively Interact With Executive Management and Board of Directors



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

Figure 28. Most Organizations Believe CISOs Are Effective



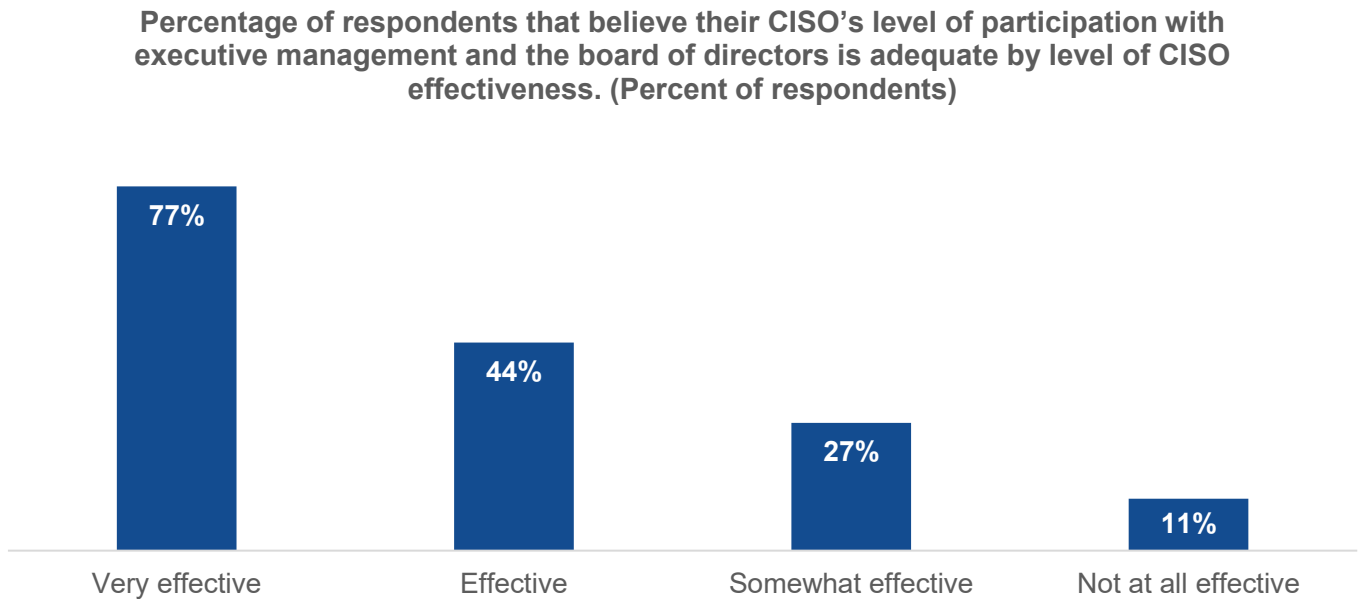
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

While the majority of CISOs interact with their corporate boards, less than half (49%) of survey respondents believe that their CISOs current board-level interactions are at an adequate level (see Figure 29). How often should CISOs interact with their boards? As often as necessary. Leading CISOs often give scheduled presentations to the board on a quarterly basis but engage with board members and executives on an ad-hoc basis regularly. Additionally, Figure 30 reveals there is a strong correlation between CISOs' board-level engagement and their effectiveness; adequate participation with the board equates to more effective CISO performance.

Figure 29. Adequacy of CISO Participation With Executive Management and the Board of Directors

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

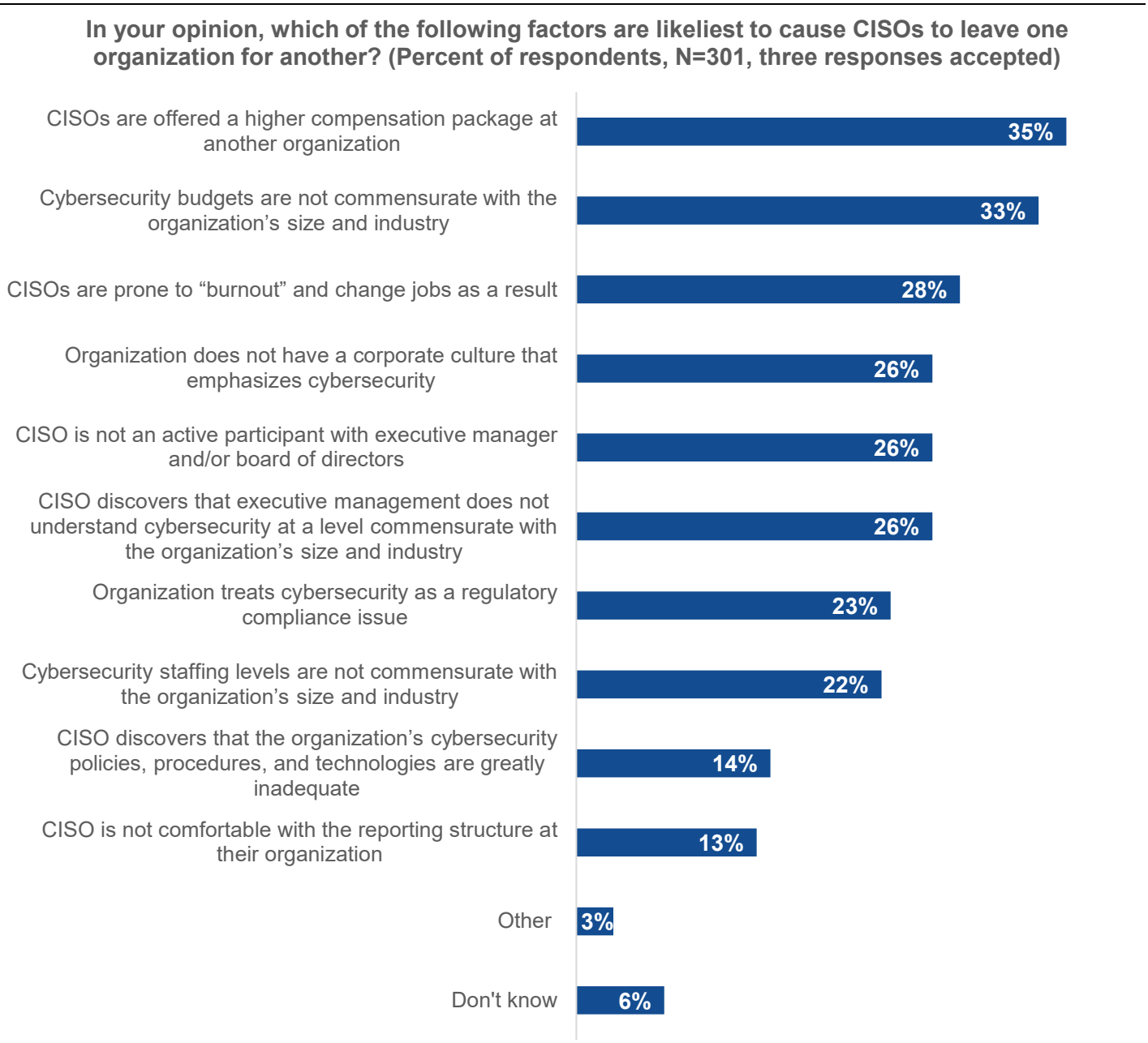
Figure 30. Interaction with C-suite and Board of Directors Correlates With CISO Effectiveness



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

This correlation between CISO board-level participation and their effectiveness speaks volumes. When boards welcome, support, and listen to CISOs, it can lead to effective security programs. On the other hand, those that minimize CISO participation can expect subpar performance and potential CISO attrition. Additionally, CISOs leave their jobs when they are offered higher compensation, when budgets aren't proportionate to corporate needs, when the stresses of their job lead to burnout, and when cybersecurity remains absent from the corporate culture (see Figure 31). These conditions will not only lead to CISO attrition, but also poor cyber-risk management, threat detection, and incident response. Furthermore, cybersecurity will continue to be considered a technical rather than a business issue. Organizations that churn through CISOs likely suffer from these deficiencies as well.

Figure 31. Why CISOs Change Jobs Often

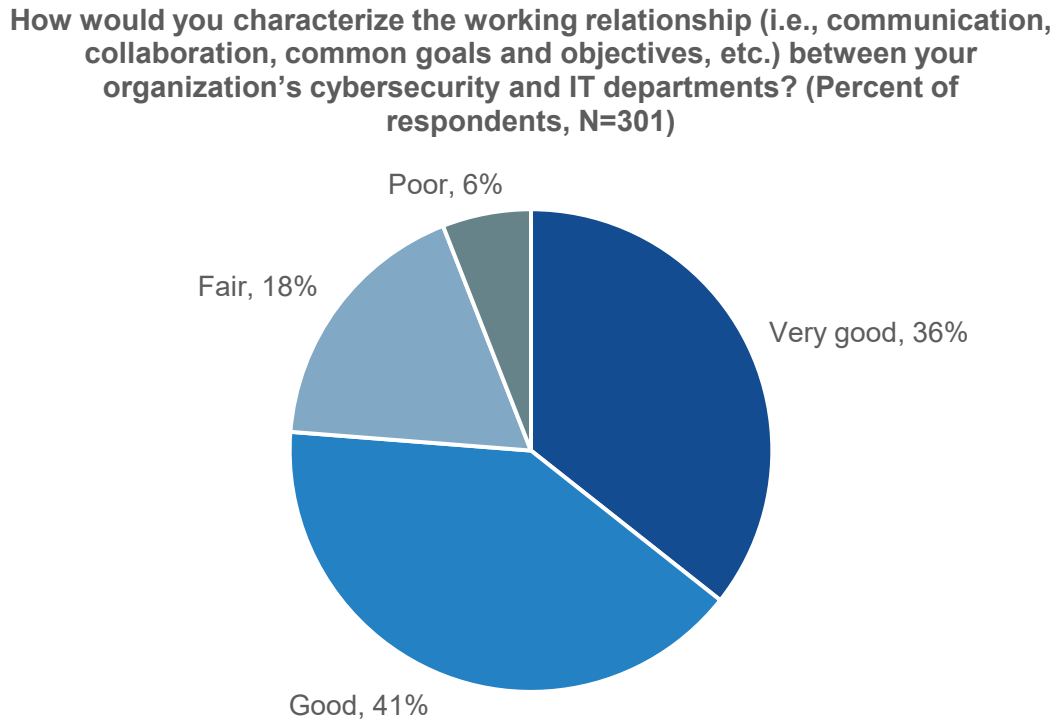


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Organizations Are Working Toward Future Cybersecurity Improvement

Most security professionals believe the relationship between security and IT teams is good. Indeed, Figure 32 reveals that more than three-quarters consider the partnership between these two groups to be good (41%) or very good (36%), but there are exceptions, as 24% rate this relationship as fair or poor.

Figure 32. Most Consider Working Relationship Between IT and Security Teams to Be Good

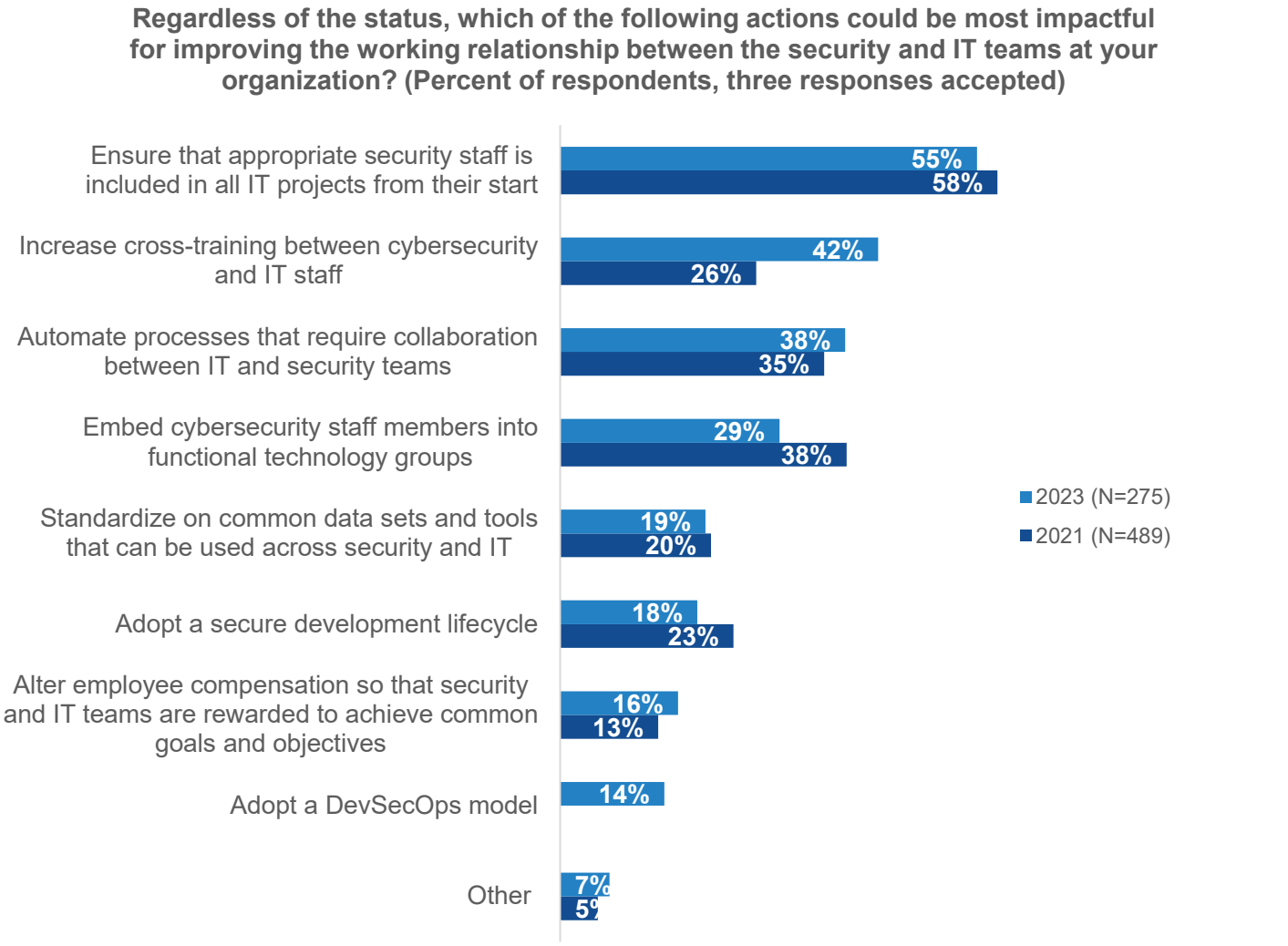


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Survey respondents did offer some suggestions for improvement, such as ensuring security staff involvement in IT projects from their onset, increasing cross-training between IT and security, automating end-to-end processes, and embedding cybersecurity staff members into functional IT groups (see Figure 33). It is noteworthy that increasing cross-training increased from 26% in 2021 to 42% in 2023. This increase is likely driven by the preponderance of technical initiatives like supporting remote workers, connecting IT systems with third parties, and developing cloud-native applications.

Many of these suggestions are critical elements of a DevSecOps program. Projects often begin with threat modeling, proceed to secure software development lifecycles, and include a continuous integration/continuous development (CI/CD) pipeline with automated security testing and tools integration. In this way, DevSecOps represents a model for effective security and IT collaboration.

Figure 33. Steps for Improving Relationships Between Security and IT Teams

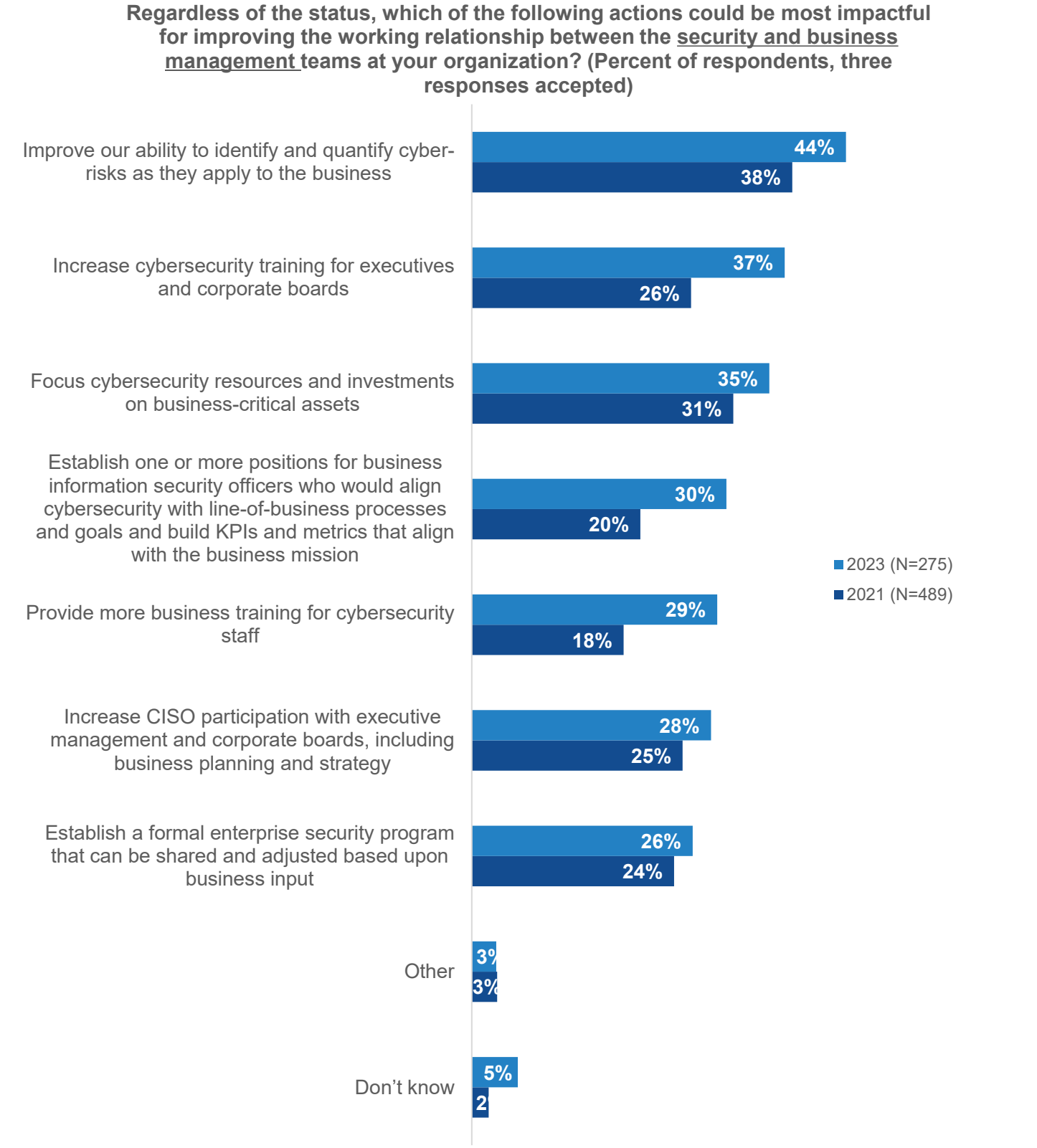


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Cybersecurity professionals also have suggestions for improving the relationship between security and business managers, including better identification of cyber-risks as they apply to the business, increasing executive (and board-level) cybersecurity training, focusing cybersecurity on business-critical assets, and establishing BISOs (or perhaps CISOs) within business units (see Figure 34). The recommendation for more executive cybersecurity training jumped from 26% in 2021 to 37% in 2023. This could be related to new regulatory responsibilities, like changing SEC rules about board-level cybersecurity responsibility. The other side of that coin is the increase in organizations citing more business training for cybersecurity staff (29% in 2023 versus 18% in 2021), indicating that regardless of role, everyone must become more knowledgeable about and familiar with all aspects of the cybersecurity ecosystem, including both what is being safeguarded and how to best accomplish this.

Many organizations use continuous red teaming and penetration testing to help them gain an adversary perspective to assess their security defenses. In this way, they can identify cyber-risks that could impact the business and focus cybersecurity resources on the appropriate business-critical assets. This strategy, often referred to as a threat-informed defense, helps focus business and security teams on critical but vulnerable systems and establish the right priorities for risk mitigation.

Figure 34. Steps for Improving Relationships Between Security and Business Managers



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

Finally, survey respondents were asked how their organizations could improve their overall cybersecurity programs. Some responses seen in Figure 35, like increasing training, creating a better cybersecurity culture, hiring more staff, and increasing cybersecurity budget, are palpable solutions and common themes throughout the research. Others are less obvious. For example, improving basic security hygiene and posture management requires an understanding of the attack surface, strong threat intelligence analysis, and comprehensive vulnerability management practices. In this way, organizations can gain a thorough understanding of what assets they have, which of those assets are vulnerable, and which of those vulnerable assets are most likely to be exploited as part of a cyber-attack. Armed with this knowledge, organizations can make accurate and targeted remediation decisions. Increasing security awareness training may not seem like a novel idea, but organizations can still benefit by shifting from "checkbox" training to more realistic approaches, like synthetic phishing campaigns accompanied by tailored training.

Figure 35. Actions that Could Improve Cybersecurity Programs

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

Conclusion

The 6th annual *The Life and Times of Cybersecurity Professionals* study continues to shed light on the most pressing challenges faced by cybersecurity professionals as they continue to deal with the ongoing cybersecurity skills shortage amid a career that is becoming increasingly difficult over time. This report analyzed the survey results regarding the cybersecurity skills shortage, job stress, workplace culture, hiring and training, CISO and executive level support, and ways organizations are working toward future cybersecurity improvements. The survey findings remain mostly consistent with previous years, once again demonstrating that organizations continue to underinvest in the staffing and training needed to protect themselves from cyber-risk.

Nearly two-thirds (66%) of cybersecurity professionals believe that the profession has become more difficult over the past 2 years. Facing ongoing internal issues and new external challenges, 21% of respondents have occasionally considered leaving the profession over the past 12 to 18 months. Those who consider leaving are frustrated with the high stress of their careers (49%) and tired of feeling that the organizations they've worked for have not taken cybersecurity seriously enough (43%).

With no end to the skills shortage in sight, CISOs need to factor these implications into the decisions they make as part of their cybersecurity strategies. Technology alone can't solve this problem, as evidenced by the fact that 39% of organizations claim that the skills shortage has led to the inability to learn or utilize some security technologies to their full potential.

Organizations have not kept cybersecurity compensation commensurate with the high demand for skilled workers and the increasingly difficult nature of the job. Providing fair and competitive compensation remains the top initiative organizations could pursue to address the skills shortage, according to 59% respondents, an increase of 22% from 2021.

The Life and Times of Cybersecurity Professionals Volume VI shows that the cybersecurity skills crisis continues to worsen with no short- or long-term solutions in sight. With an increasingly hostile cyber-threat landscape, organizations will face new and more dangerous cyber-threats with an understaffed and overstressed workforce. Over the years, it has become increasingly clear that organizations either do not understand or undervalue cybersecurity's role as a business enabler. Investments in increased compensation, training, and building a better cybersecurity culture throughout the organization are all tangible actions organizations can take to play a role in improving the cybersecurity skills gap and strengthen their cybersecurity programs to reduce cyber-risk.

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 7, 2023, and March 12, 2023. 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 301 IT and cybersecurity professionals.

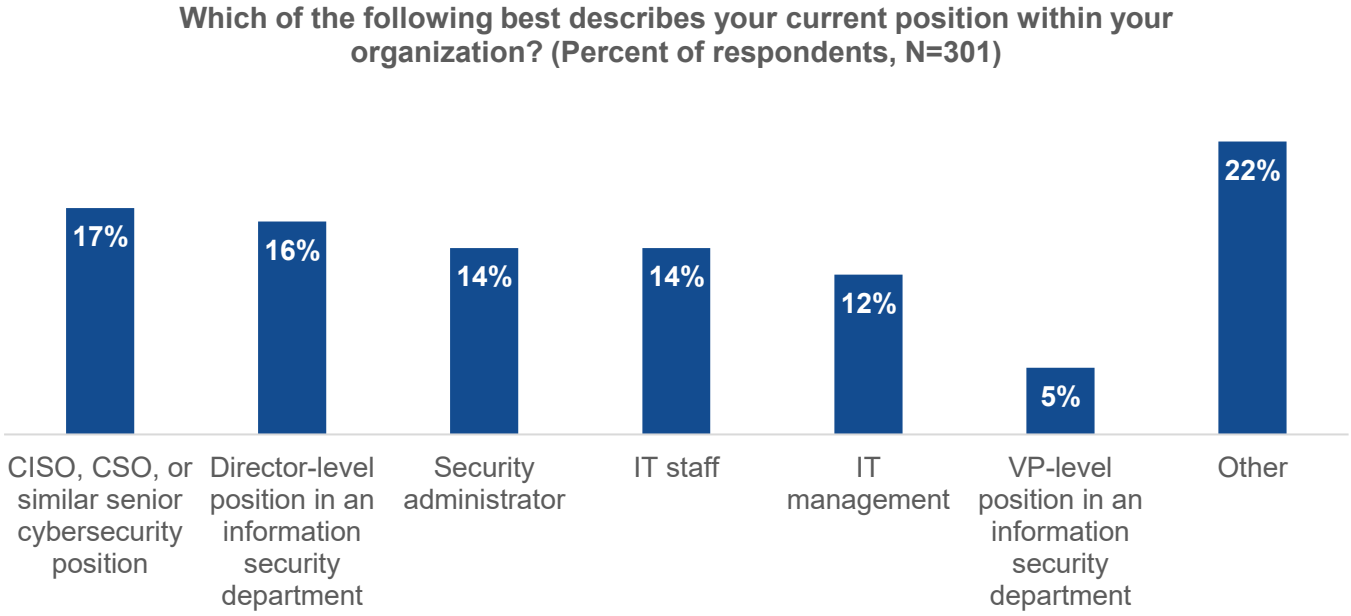
Please see the Respondent Demographics section of this report for more information on these respondents.

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

Respondent Demographics

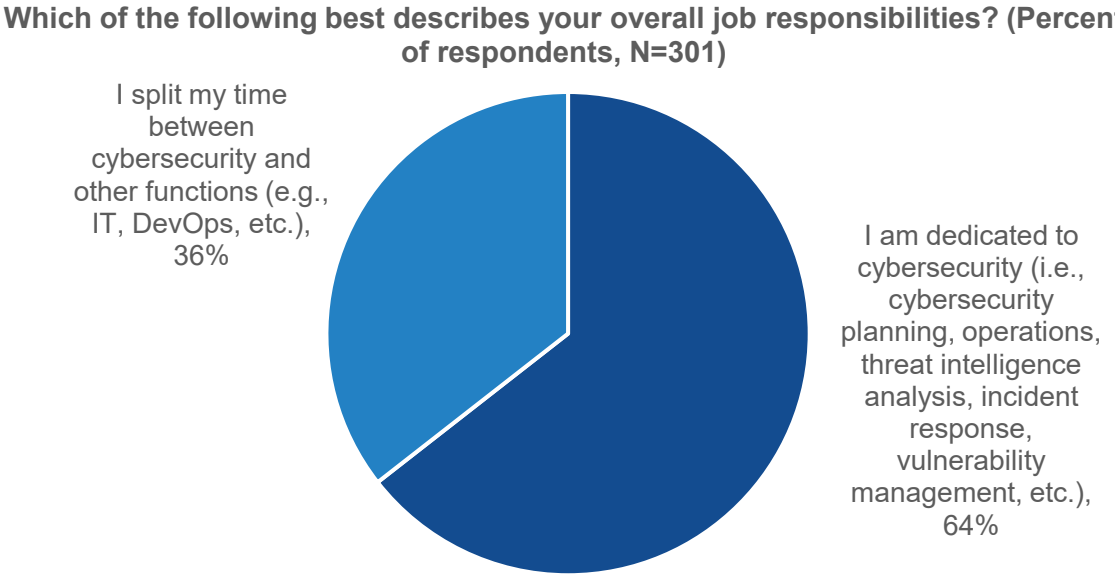
Respondent data presented in this report is based on a survey of 301 qualified respondents. Figure 36 through Figure 41 detail the demographics of the respondent base at an individual and organizational level.

Figure 36. Respondents by Current Position



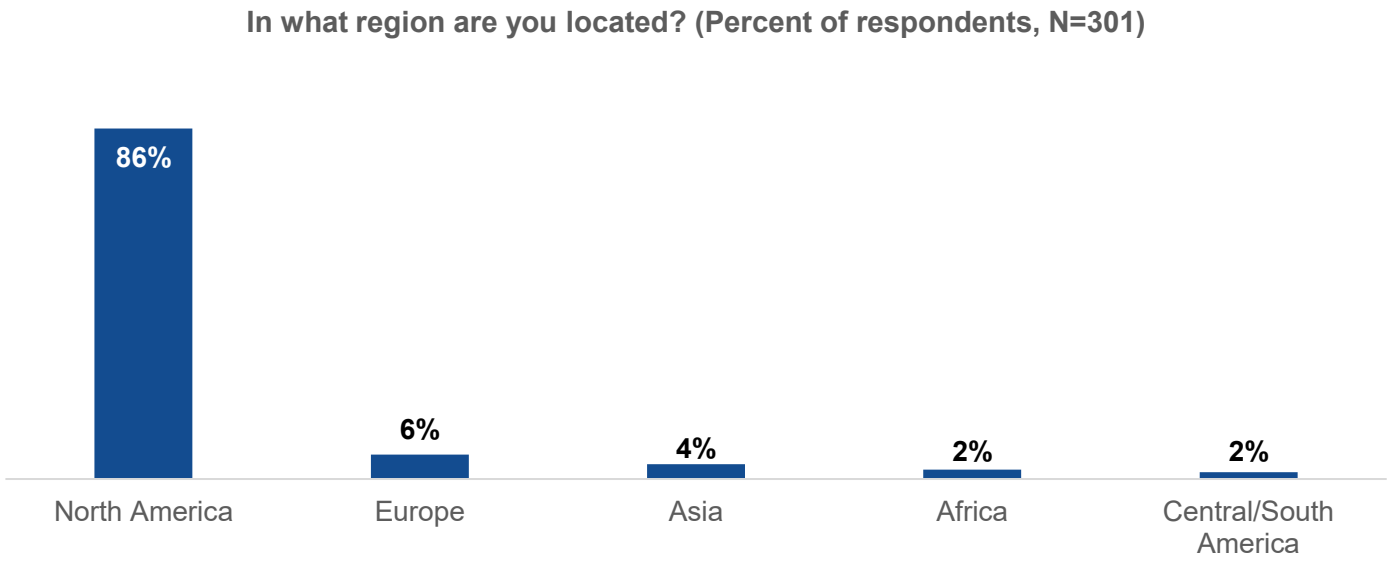
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 37. Respondents by Job Responsibilities



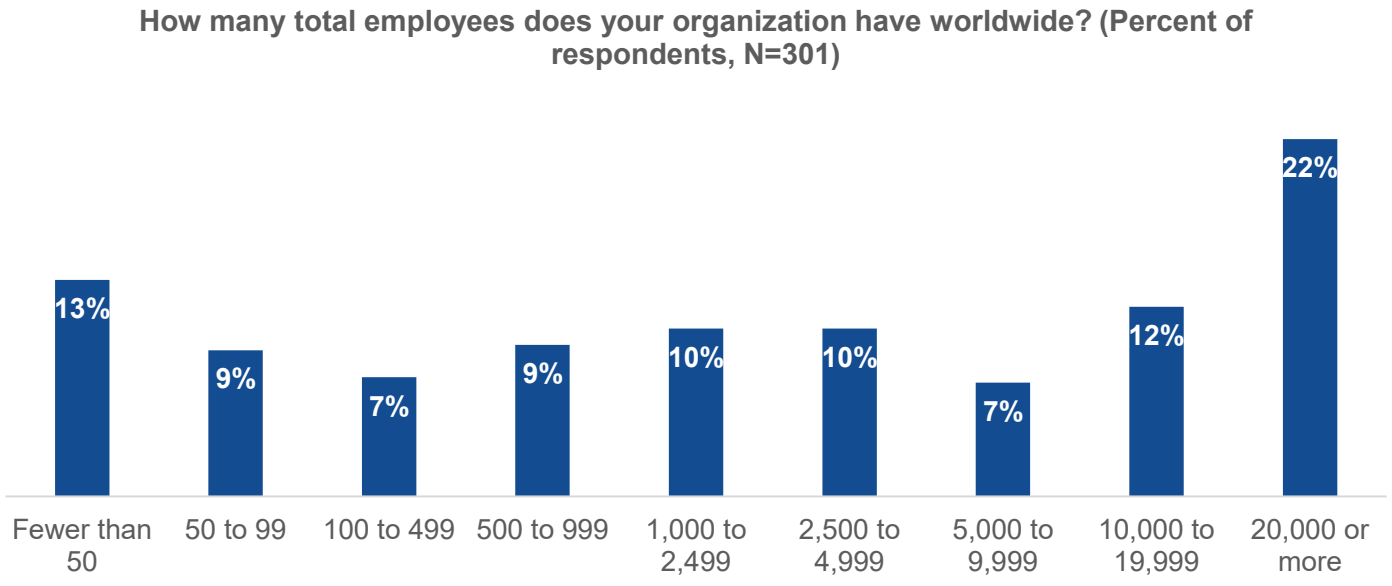
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 38. Respondents by Region



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

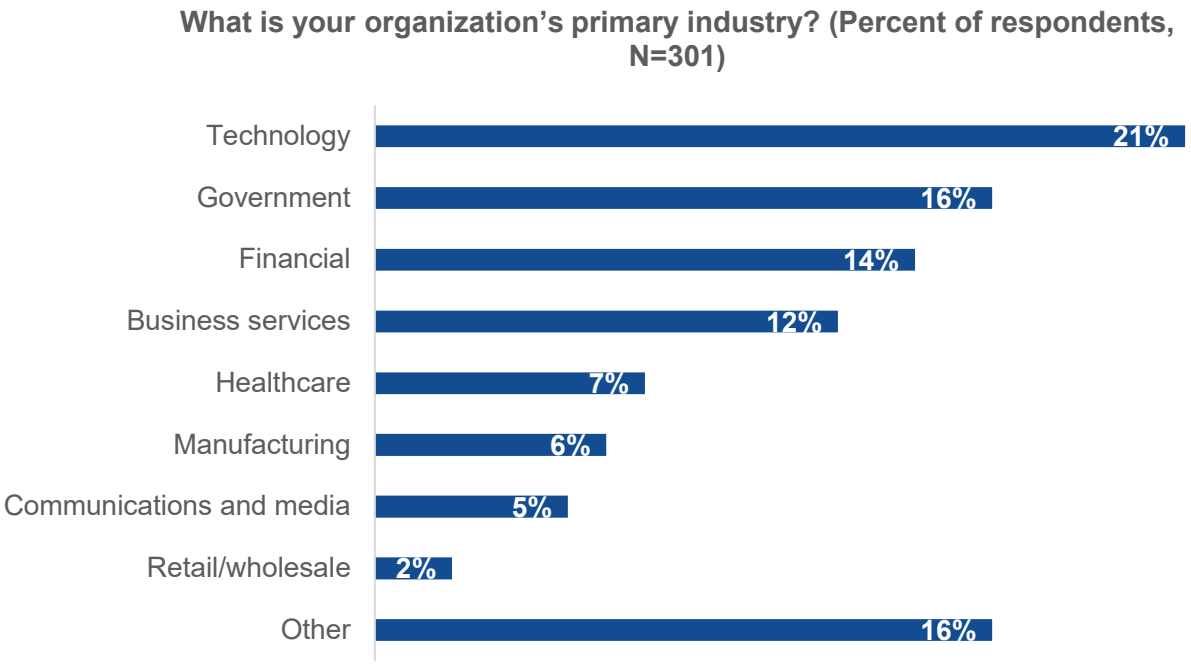
Figure 39. Respondents by Number of Employees



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

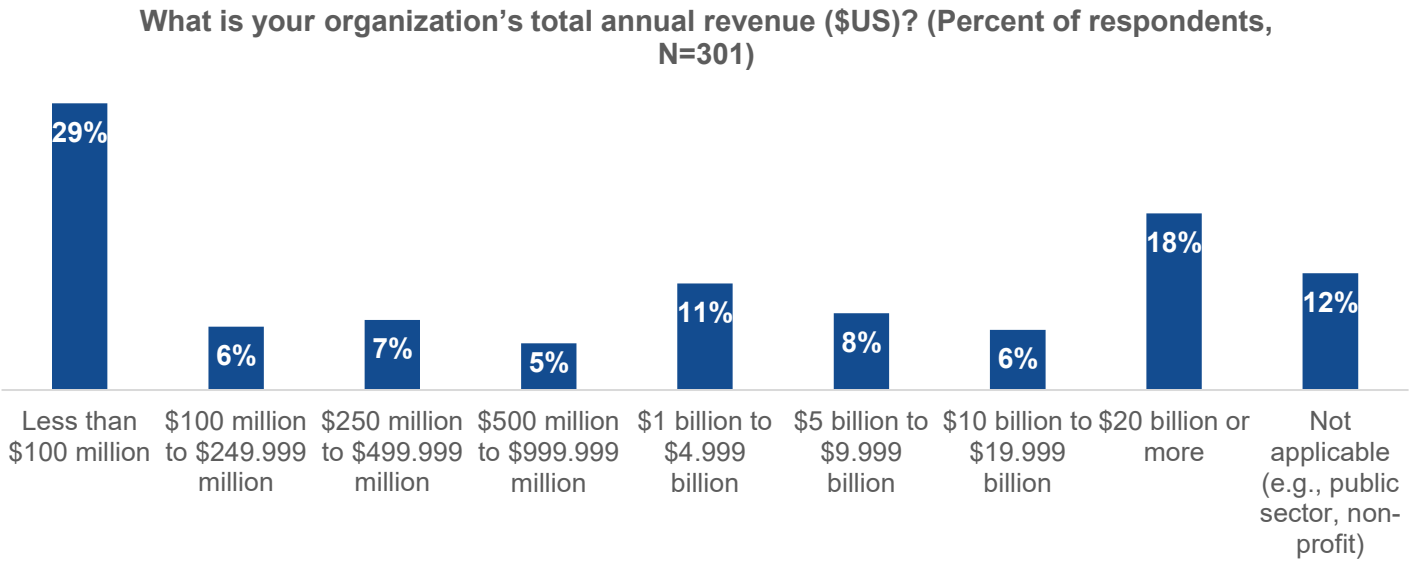
Respondents were asked to identify their organization's primary industry. In total, Enterprise Strategy Group received completed, qualified responses from individuals in 21 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 40.

Figure 40. Respondents by Industry



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

Figure 41. Respondents by Annual Revenue



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

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