Enterprise Strategy Group™ by TechTarget

ISSA Information Systems Security Association International

The Life and Times of Cybersecurity Professionals

VOLUME VI

Jon Oltsik,
Distinguished Analyst & Enterprise Strategy Group Fellow

JULY 2023

CONTENTS

BACK TO CONTENTS

Research Objectives

According to *The Life and Times of Cybersecurity Professionals Volume VI* (2023), the cybersecurity skills shortage continues unabated, leaving a majority of organizations with an ever-growing gap in the cybersecurity skills needed to reduce their cyber-risk from the latest threats. As the void widens, cybersecurity professionals bear the brunt: More than half find their jobs harder than two years ago, with many facing ongoing internal issues and new external challenges from an increase in cybersecurity complexity to a surge in cyber-attacks against an expanding attack surface. Chronic understaffing remains a major contributor to these issues and associated ramifications, with roughly one out of five professionals having even considered making a career switch, mainly out of frustration with what they perceive as organizational neglect and the sheer stress of their jobs.

Despite years of cybersecurity skills shortages, organizations aren't crafting effective strategies to bridge the skills gap. For example, salaries are not aligned to the increasingly difficult and demanding nature of the job nor the competitive job market. Not surprisingly, providing fair and competitive compensation remains the top initiative organizations could pursue to address the skills shortage according to most cyber pros. Additionally, over half want better access to training, certifications, and industry events as part of their compensation package. These simple steps could help organizations better address the skills shortage.

The gravity of the situation remains heavy. Cyber-threats loom large, and organizations remain vulnerable, in part due to under-equipped and overburdened cybersecurity teams. The data echoes a critical message: Unless businesses reevaluate and boost their investment in cybersecurity and recognize its pivotal role as a business driver versus a cost center, the security and safety of the digital realm's future appears perilous. To gain further insight into these trends, TechTarget's Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA) surveyed 301 IT and cybersecurity professionals at organizations all over the world. This eBook serves as the sixth such research project, dating back to 2016.

All references to previous ESG/ISSA research in this ebook can be found in *The Life and Times of Cybersecurity Professionals 2021 Volume V.*

In assessing the life and times of cybersecurity professionals, this study sought to:

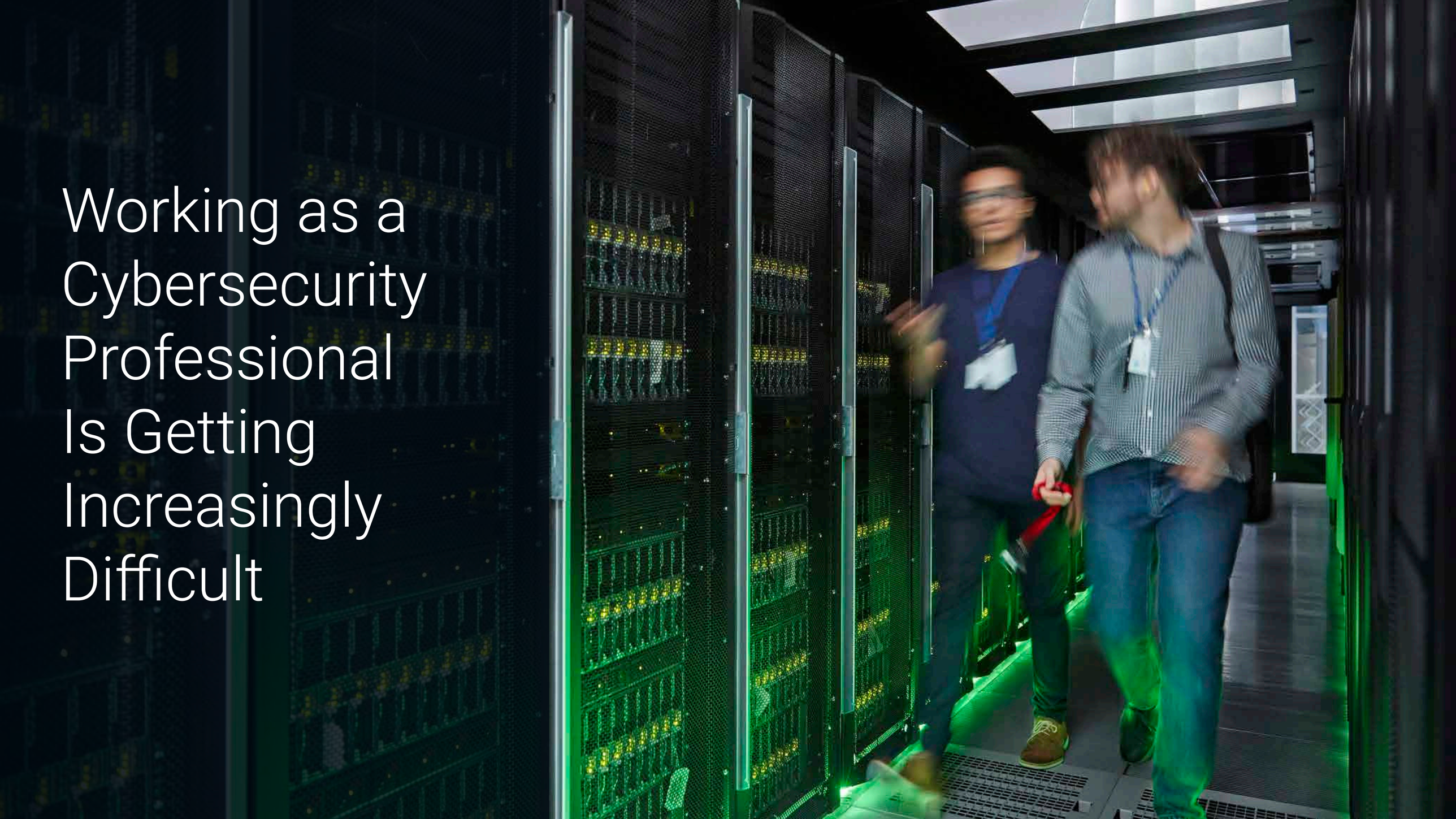
Assess the career progression of cybersecurity professionals.

Measure the impact of the global cybersecurity skills shortage and uncover how organizations are responding.

Determine whether cybersecurity professionals are satisfied with their careers and current jobs.

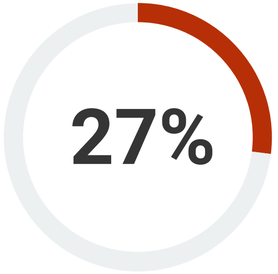
Monitor the status and performance of cybersecurity leadership.

Working as a Cybersecurity Professional Is Getting Increasingly Difficult

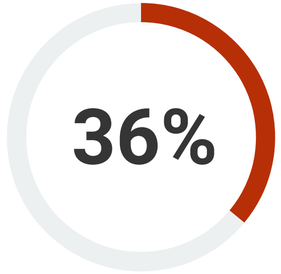


Why a Cybersecurity Career Has Become More Difficult

A majority (63%) of cybersecurity professionals believe that working as a cybersecurity professional has become more difficult over the past two years. When this group was asked why this was the case, they cited reasons like increasing cybersecurity complexity and workloads, 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.

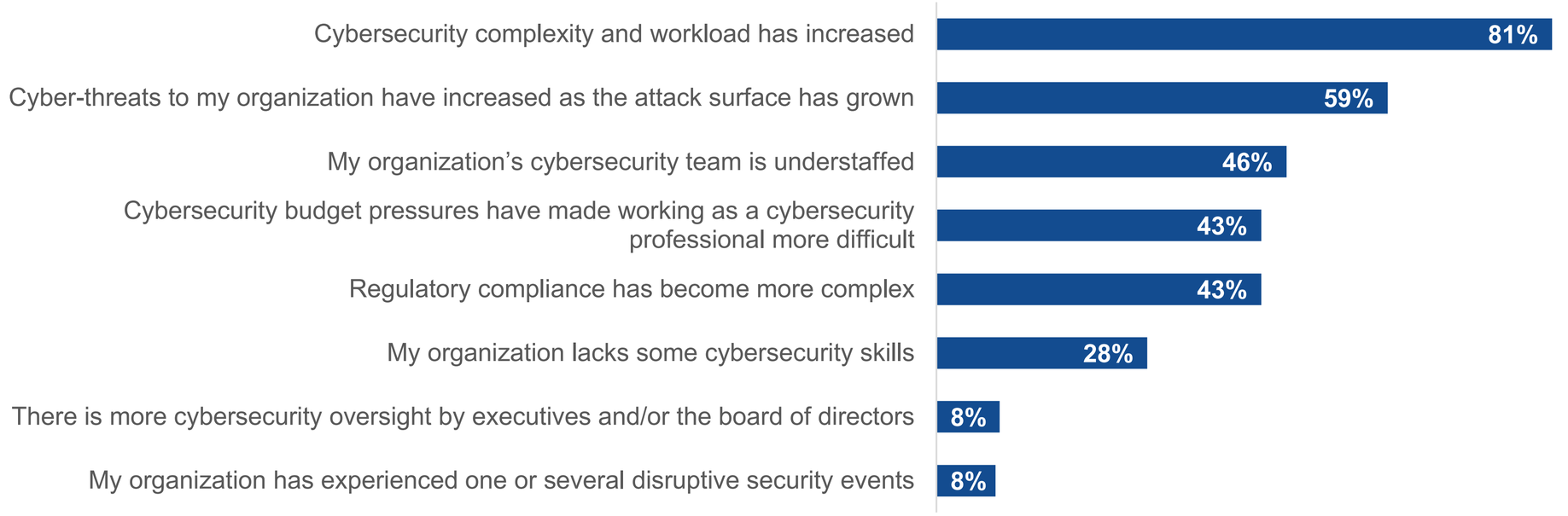


Working as a cybersecurity professional is **much more difficult today than it was 2 years ago.**



Working as a cybersecurity professional is **somewhat more difficult today than it was 2 years ago.**

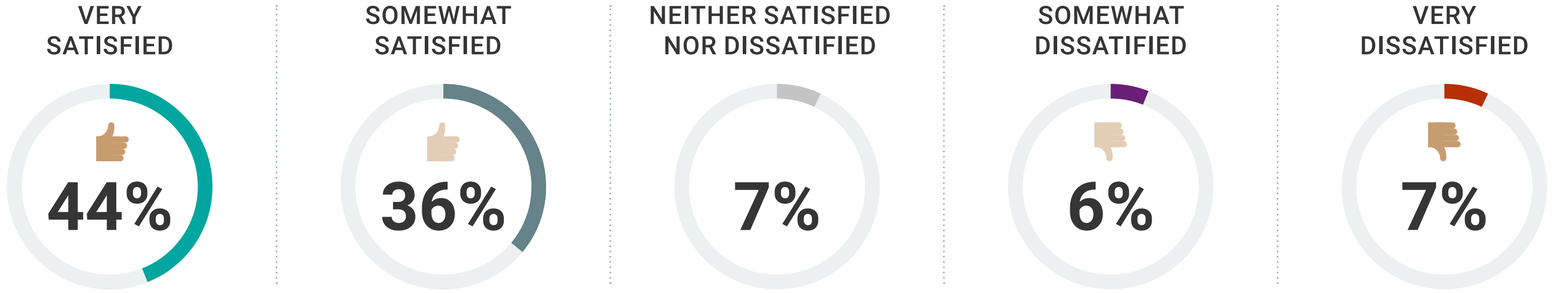
Reasons being a cybersecurity professional is more difficult today.



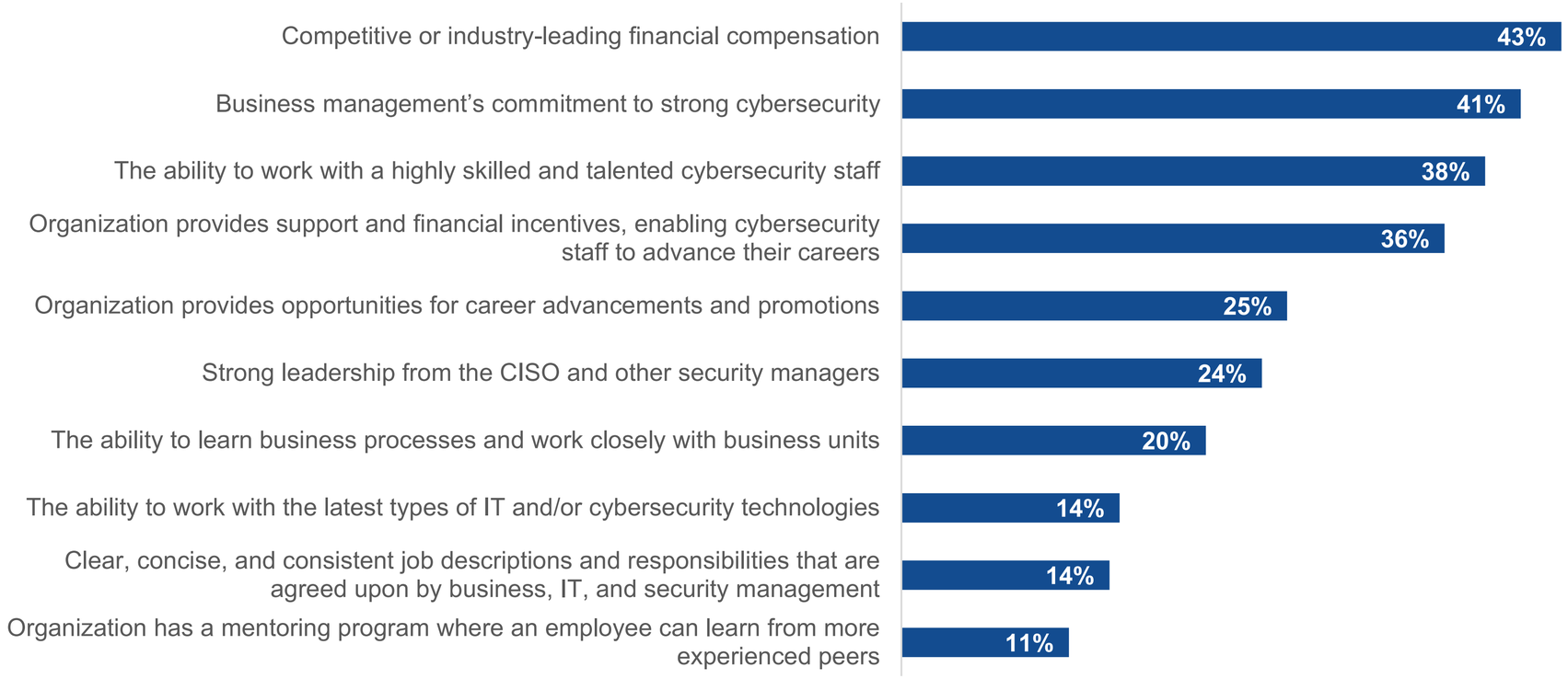
> **"Nearly two-thirds believe that working as a cybersecurity professional has become more difficult** over the past 2 years."

BACK TO CONTENTS

Satisfaction level for current job among cybersecurity professionals.



Biggest factors that determine job satisfaction level.



What Is Driving Cybersecurity Job Satisfaction?

What factors drive job satisfaction? Recognizing their value, cybersecurity professionals want to be paid a competitive salary with commensurate benefits. Beyond 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.

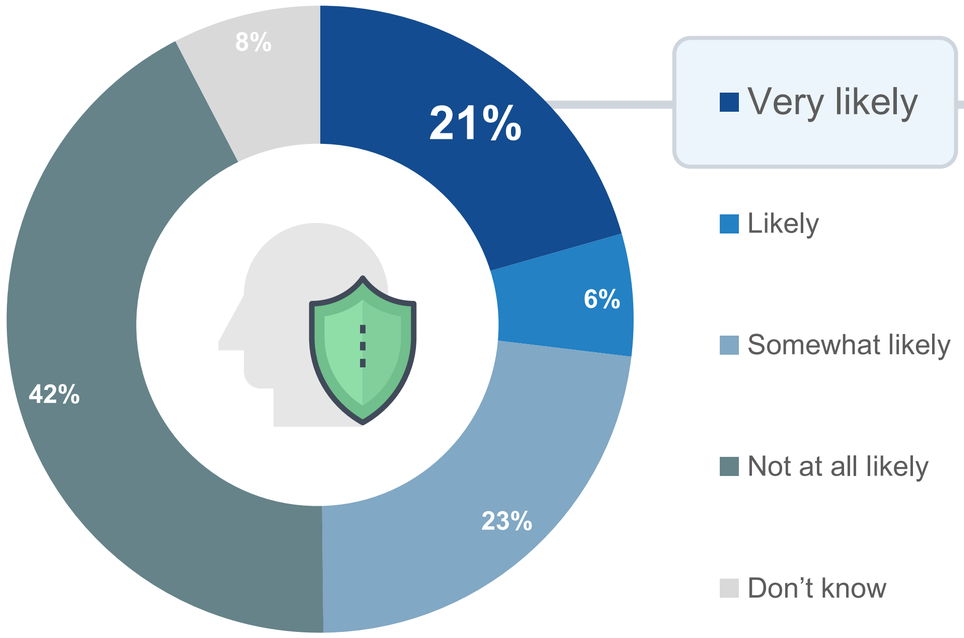
Despite cybersecurity professional challenges, 44% of survey respondents report that they are very satisfied with their current jobs, up slightly from 37% in 2021. This is a testament to cybersecurity professionals' dedication to the mission. However, it is worth noting that 13% of cybersecurity professionals are somewhat or very dissatisfied with their current position, and those very dissatisfied increased from 4% in 2021 to 7% this year. Dissatisfied employees predictably lead to employee attrition, exacerbating the challenges described previously.

BACK TO CONTENTS

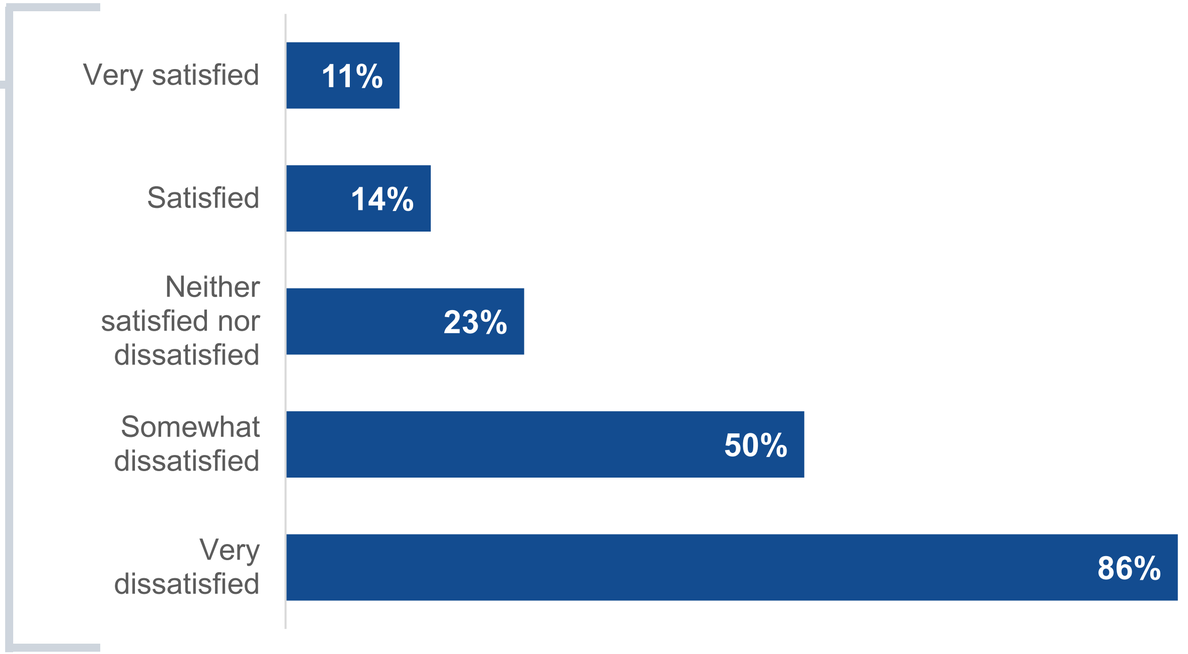
Potential Job Churn Is Pervasive, Especially Among Dissatisfied Cybersecurity Pros

Growing job difficulties and dissatisfaction lead unavoidably to employee attrition as cybersecurity pros seek better opportunities. Indeed, half of survey participants are somewhat likely, likely, or very likely to leave their current jobs this year. Not surprisingly, there is a strong correlation between job churn and job satisfaction as 86% of cybersecurity professionals **very likely** to leave their jobs this year are also very dissatisfied with their current roles. 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.

Likelihood of leaving current cybersecurity job in 2023.



Percentage of cybersecurity professionals who are **very likely** to leave their current job in 2023 based on how satisfied they are with that job. (Percent of respondents)



BACK TO CONTENTS

Stressful Aspects of the Cybersecurity Profession

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. The causes of job stress present a consistent pattern throughout the research: an overwhelming workload and working with disinterested business managers. 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 top 3 stressful aspects of a cybersecurity profession remained consistent in the 2021 and 2023 iterations of this study.

Most stressful aspects of cybersecurity jobs/careers.

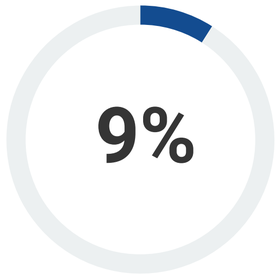
"55% of cybersecurity professionals claim they experience on-the-job stress at least half the time."

BACK TO CONTENTS

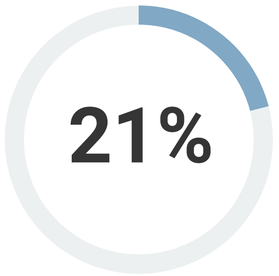
Potential for Leaving the Cybersecurity Profession

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 consider leaving the profession on an occasional (21%) or regular (9%) basis due to the stress factors that are associated with a cybersecurity career, a lack of cybersecurity commitment by their employers, or an impending plan to retire.

Have cybersecurity pros considered leaving the *profession* over the last 12 to 18 months?

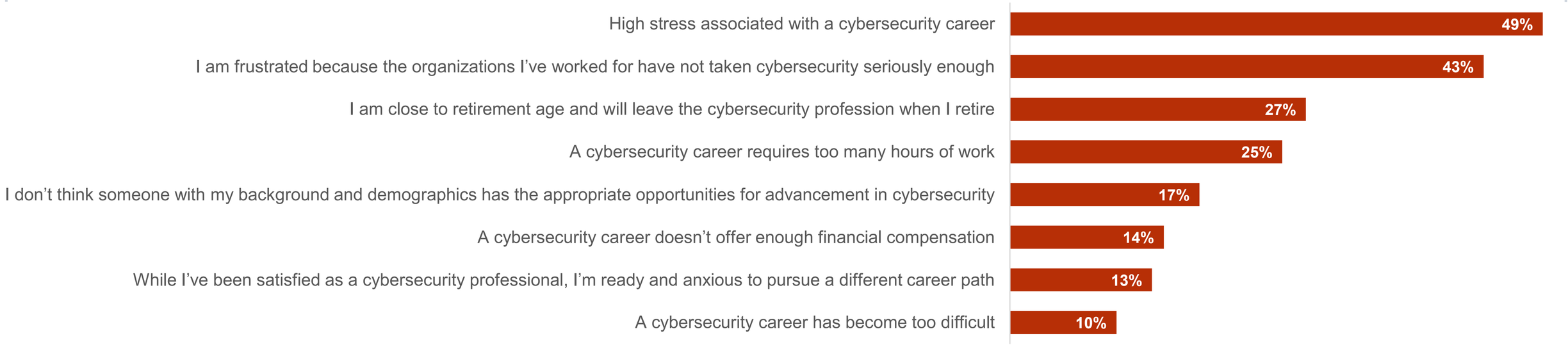


9% **Yes,** regularly



21% **Yes,** occassionally

Reasons for potentially leaving the cybersecurity profession.



BACK TO CONTENTS

Cybersecurity Career Advancement Techniques

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.” Survey respondents believe networking with other cybersecurity professionals, participating in training sessions, attending industry events, and joining cybersecurity professional organizations are part of a career development strategy. It is also advantageous to gain experience across many different roles and attain appropriate security certifications.

| Actions that would be most helpful for cybersecurity career advancement.

62%
Networking with other cybersecurity professionals

49%
Attending more training sessions

47%
Attending more industry events

45%
Joining a cybersecurity professional organization

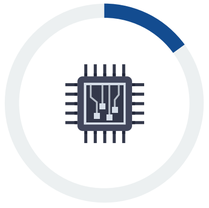
42%
Rotating cybersecurity jobs to gain experience in multiple areas

42%
Pursuing more security certifications

35%
Working for different organizations in different industries

26%
Pursuing an advanced degree in cybersecurity

16%
Working for a cybersecurity services vendor



15%
Working for a cybersecurity technology vendor

BACK TO CONTENTS

“How can entry-level candidates start their cybersecurity careers?”

Primary piece of advice for prospective cybersecurity professionals.

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. While these best practices should help, it still may be difficult for inexperienced (but ambitious) individuals to attain their first job. ESG and ISSA recommend persistence here as a first cybersecurity job can lead to fruitful career opportunities.

BACK TO CONTENTS

Cybersecurity Programs Could Be Improved by Embracing a Cybersecurity Culture

Rating Organizations' Cybersecurity Culture

Not many cybersecurity pros 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. 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.

Characterization of the cybersecurity culture at organizations.

31%

ADVANCED:

Cybersecurity is considered a shared responsibility by all employees and is included in all business/ mission initiatives

43%

AVERAGE:

Cybersecurity is considered a shared responsibility by some employees and is included in some business/mission initiatives

20%

FAIR:

While my organization makes some efforts, cybersecurity is only partially considered a shared responsibility by employees and partially included in business/ mission initiatives

7%

POOR:

My organization makes little cybersecurity efforts, so cybersecurity is hardly considered a shared responsibility by employees and hardly included in business/ mission initiatives

BACK TO CONTENTS

Career History with Organizations Apathetic to Cybersecurity

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.

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. Many seem unwilling to do so and would act as a whistleblower if this state of affairs occurred, as it did recently when a cybersecurity executive at Twitter testified before the judiciary committee of the US Senate about the company's cybersecurity shortcomings. 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.

Do organizations knowingly ignore security best practices and/or regulatory compliance requirements?

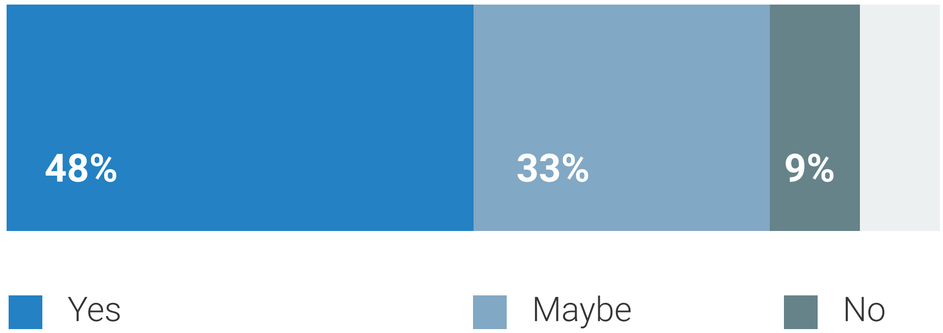
50%
Yes, several times

8%
Yes, once

14%
Maybe, I suspected but wasn't certain that this was happening

23%
No

Would cybersecurity pros act as whistleblowers if their organization knowingly ignored security best practices and/or regulatory compliance requirements?



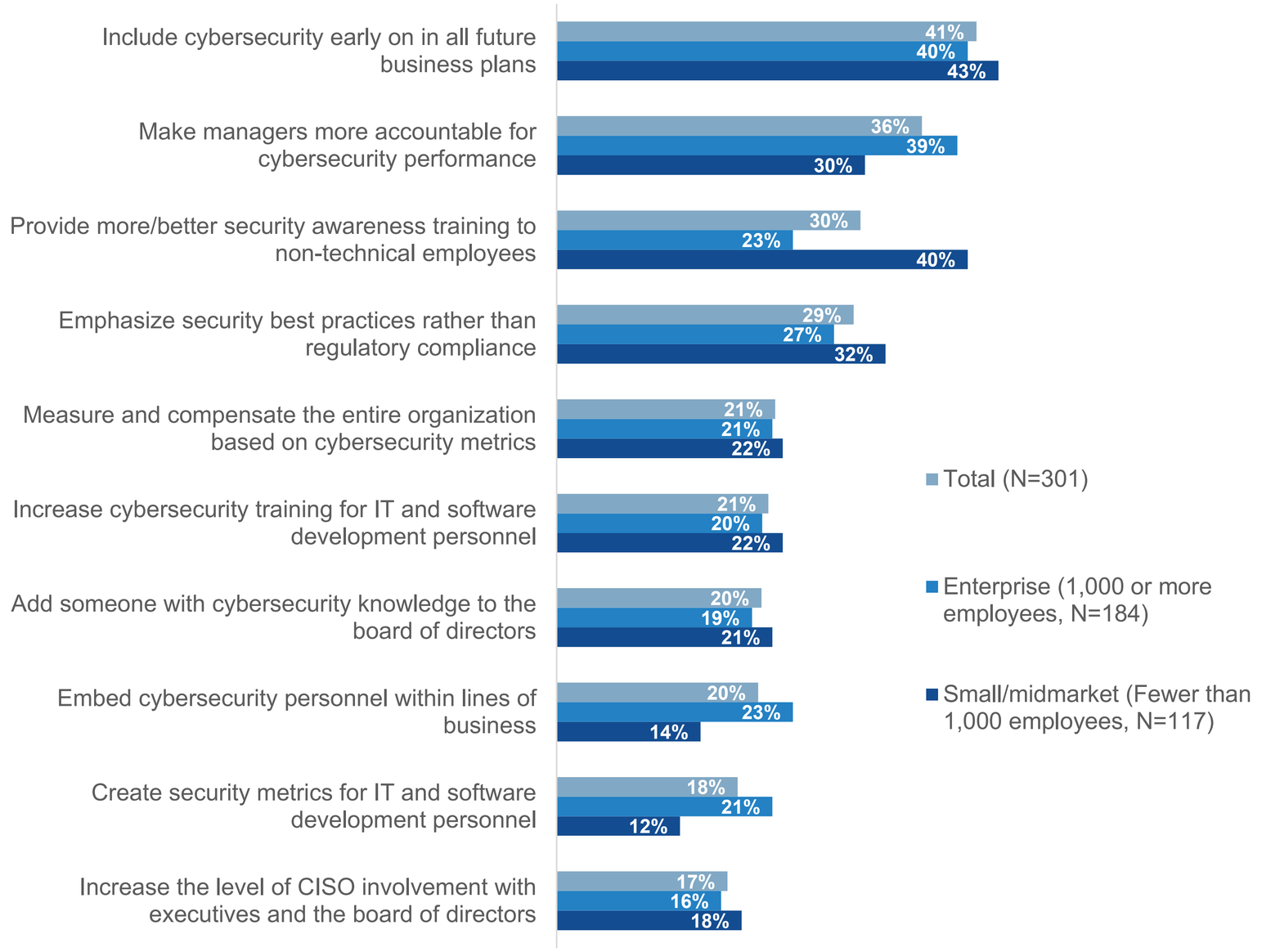
BACK TO CONTENTS

Improving Cybersecurity Culture

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. 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 polices.

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%).

Steps organizations could take to improve cybersecurity culture.



BACK TO CONTENTS

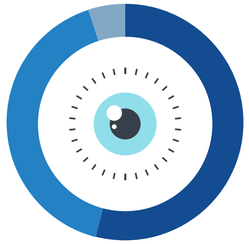
The Cybersecurity Skills Shortage Is Not Improving, and Organizations Are Not Responding with the Right Countermeasures

Impact and Status of the Global Cybersecurity Skills Shortage

After six editions of the Life and Times of Cybersecurity Professionals, this iteration of 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. 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 believe the skills shortage has gotten worse over the past two years (a 10% increase over 2021). Furthermore, 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.

Has the global cybersecurity skills shortage impacted the organization for which you currently work?

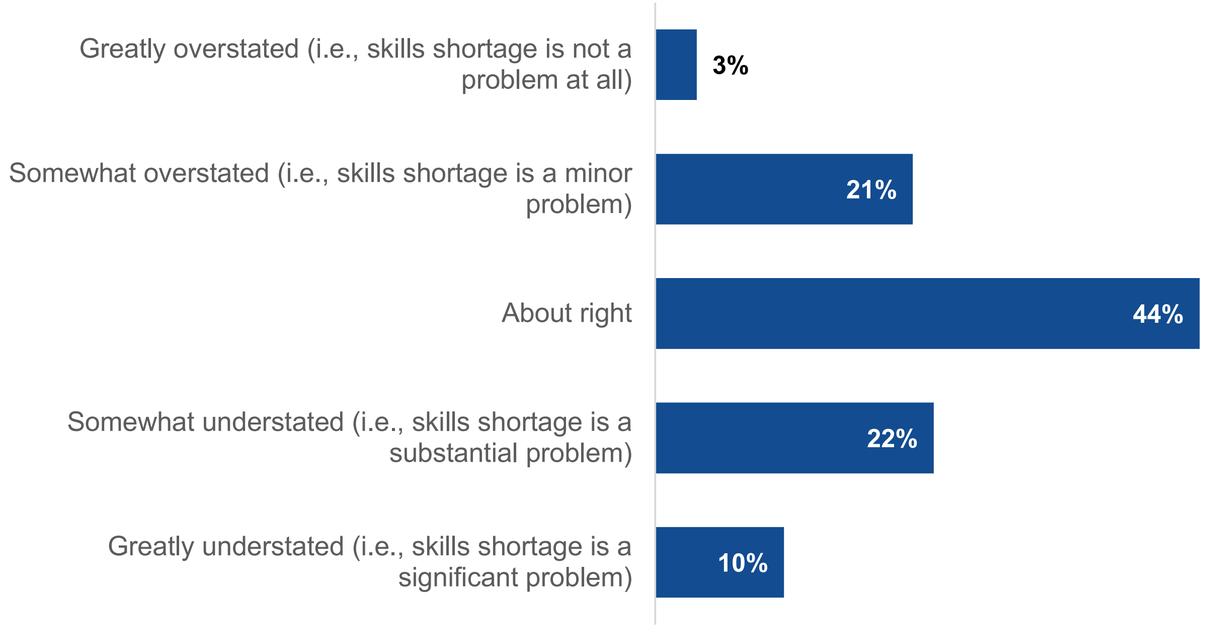
- **27%** Yes, significantly
- **44%** Yes, somewhat
- **23%** No



How has the impact of the global cybersecurity skills shortage on your organization changed over the last two years?

- **54%** It has gotten worse over the past two years
- **41%** It is about the same today as it was two years ago
- **5%** It has improved over the past two years

Perception of the cybersecurity skills shortage.



BACK TO CONTENTS

Impact of the Cybersecurity Skills Shortage

Those organizations impacted by the cybersecurity skills shortage report ramifications like an increasing workload on existing staff, lengthy job openings (a 10% increase over 2021), and high burnout rates leading to staff attrition. 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.

Impact the global cybersecurity skills shortage has had on organizations.

61%
Increasing workload on existing staff

49%
New security jobs remain open for weeks or months

43%
High "burnout" and/or attrition rate among the cybersecurity staff

39%
Inability to fully learn or utilize some of our security technologies to their full potential

30%
My organization has hired and trained junior employees rather than experienced candidates

28%
Cybersecurity staff has limited time to work with business units

28%
Cybersecurity staff time is spent disproportionally on high-priority issues and incident response

27%
Increase in the use of professional and/or managed services

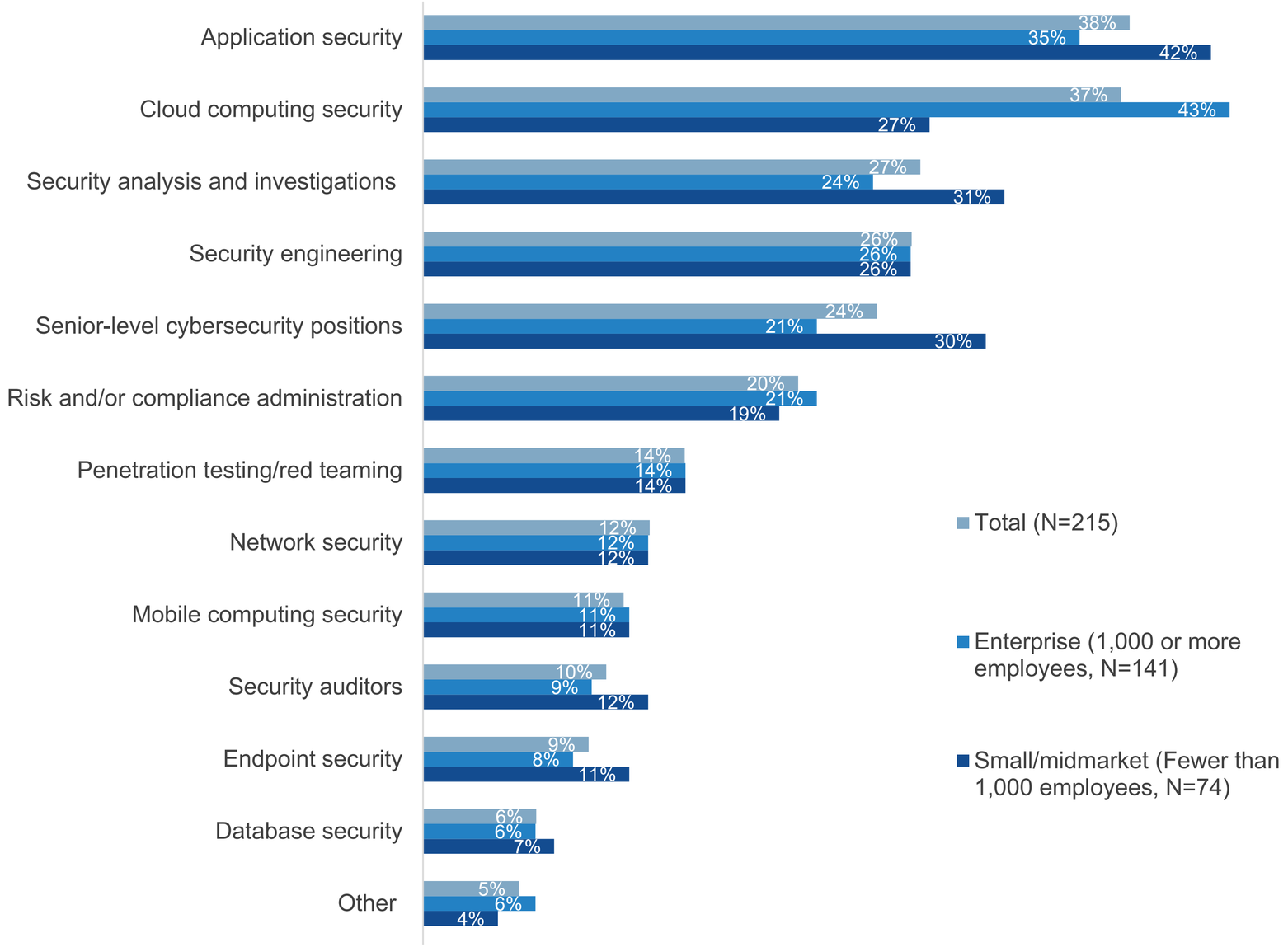
19%
My organization has delegated some security tasks to IT that it would normally do itself

19%
An increase in human error associated with cybersecurity tasks

18%
Inability to investigate and/or prioritize security alerts in a timely manner

BACK TO CONTENTS

Areas of cybersecurity with most significant shortage of skills.



Most Significant Skills Shortage Areas

As in past years, organizations have the most acute skills deficits in areas like application security, cloud security, security analysis, and security engineering. 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.

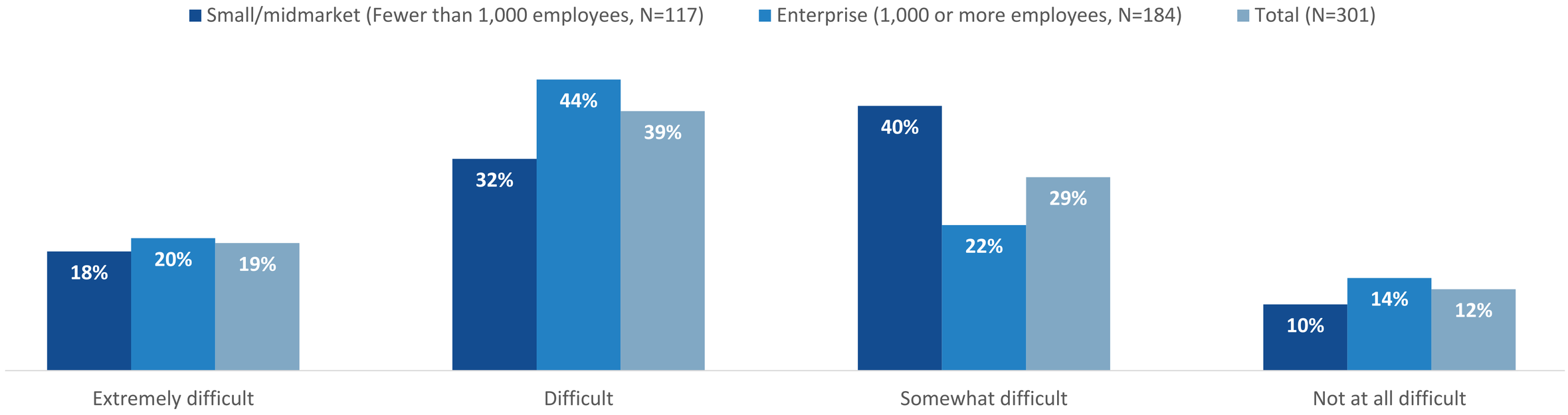
BACK TO CONTENTS

Degree of Difficulty Recruiting and Hiring Cybersecurity Staff

Within the overall survey population, a majority (88%) of respondents say it is extremely difficult, difficult, or somewhat difficult to recruit and hire cybersecurity professionals, representing a 12% increase over 2021. Larger organizations have a more difficult time than smaller ones as 66% 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).

Level of difficulty recruiting cybersecurity professionals.



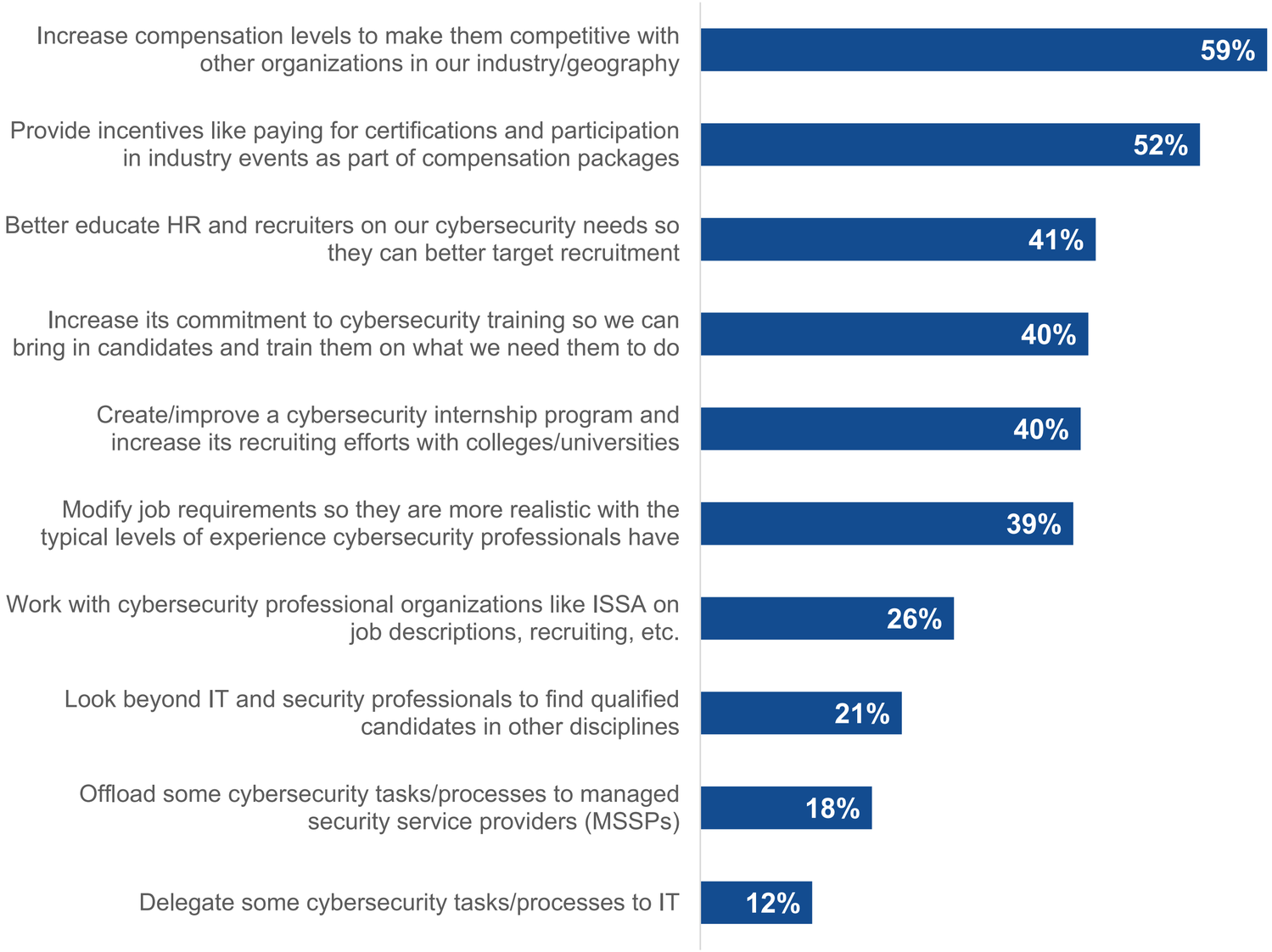
BACK TO CONTENTS

Addressing the Impact of the Cybersecurity Skills Shortage

What else could organizations do to better counteract the cybersecurity skills shortage? 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.

Actions organizations could take to address the cybersecurity skills shortage.



BACK TO CONTENTS

CISO Success Depends Upon Leadership and Communication Skills

Important Qualities for Successful CISOs

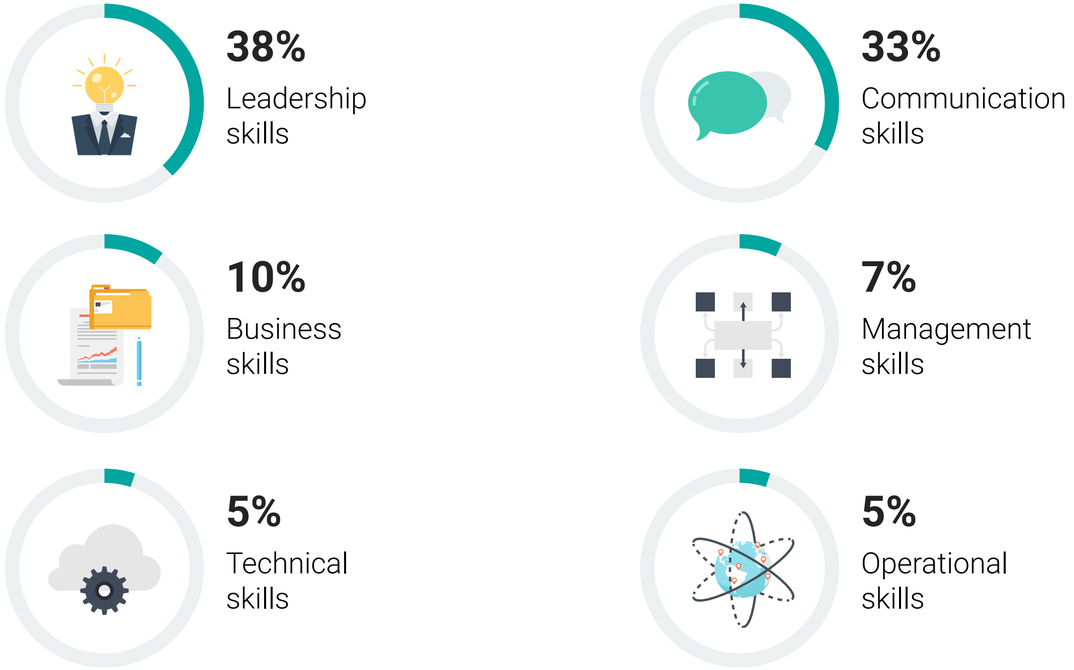
More than three-quarters (78%) of all survey respondents work at an organization with a CISO or virtual CISO. Almost half (49%) of these CISOs report to the CIO or other senior IT manager, while nearly one-quarter (24%) report directly to the CEO.

Do organizations have a CISO in place today?

Whom do CISOs report to?

When asked to identify the qualities that make CISOs successful, nearly three-quarters (71%) pointed toward leadership or communications skills. 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.

Most important quality of a successful CISO.

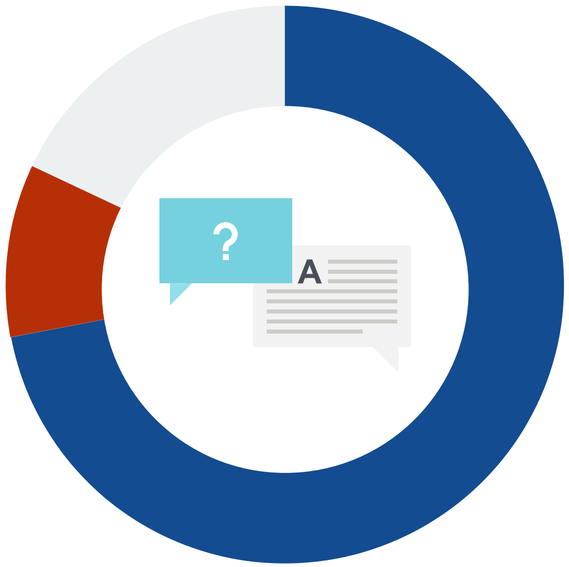


BACK TO CONTENTS

Effective CISOs Interact Frequently with Executives and Corporate Boards

In most cases (72%), the CISO actively interacts directly with their board of directors or similar oversight body. This is a bit of good news as it represents an 11% increase from 2021. It's likely that pernicious threats and regulatory requirements have forced this change. 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 30% say their CISO has been either somewhat effective or not at all effective.

Does CISO actively interact with executive management and the board of directors?



72% Yes

10% No

Effectiveness of CISO.

31% Very effective

40% Effective

26% Somewhat effective

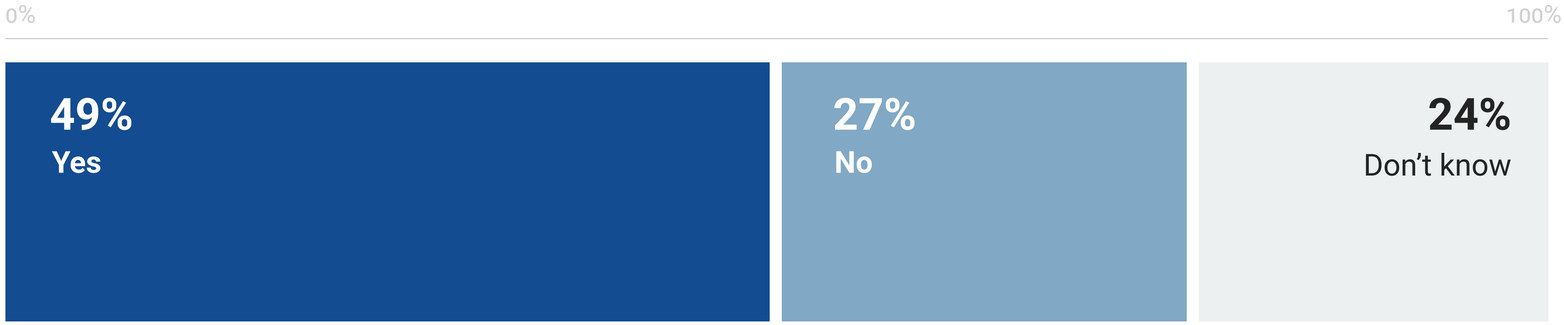
BACK TO CONTENTS

Interaction with C-suite and BoD Correlates with CISO Effectiveness

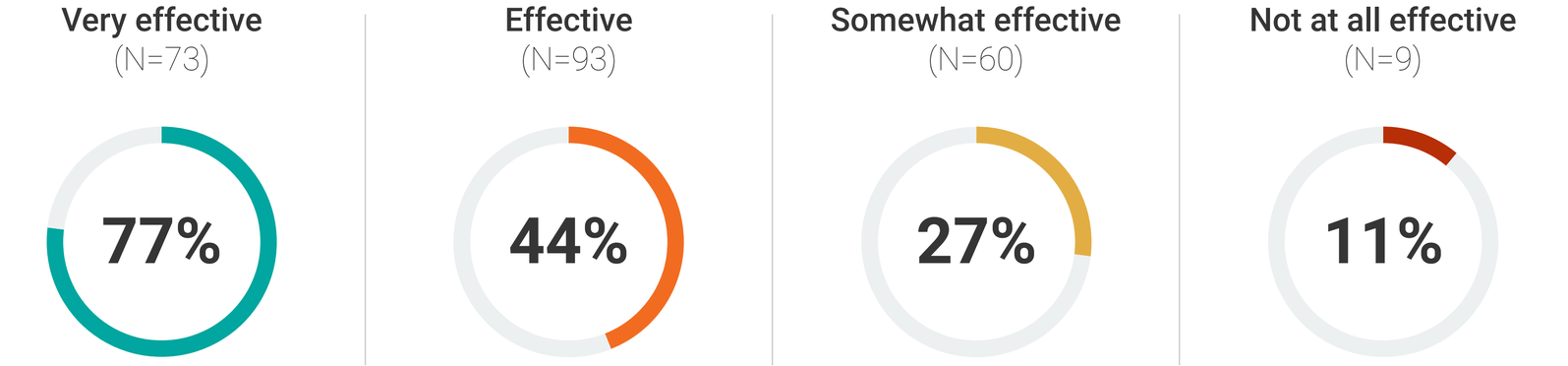
While the majority of CISOs interact with their corporate boards, less than half (49%) of survey respondents believe that their CISOs' current board-level interactions are at an adequate level. How often should CISOs interact with their boards? As often as necessary. Leading CISOs often conduct scheduled presentations to the board on a quarterly basis but engage with board members and executives on an ad-hoc basis regularly.

Additionally, there is a strong relationship between CISOs' board-level engagement and their effectiveness; adequate participation with the board equates to more effective CISO performance.

Is CISO's level of participation with executive management and the board of directors adequate?

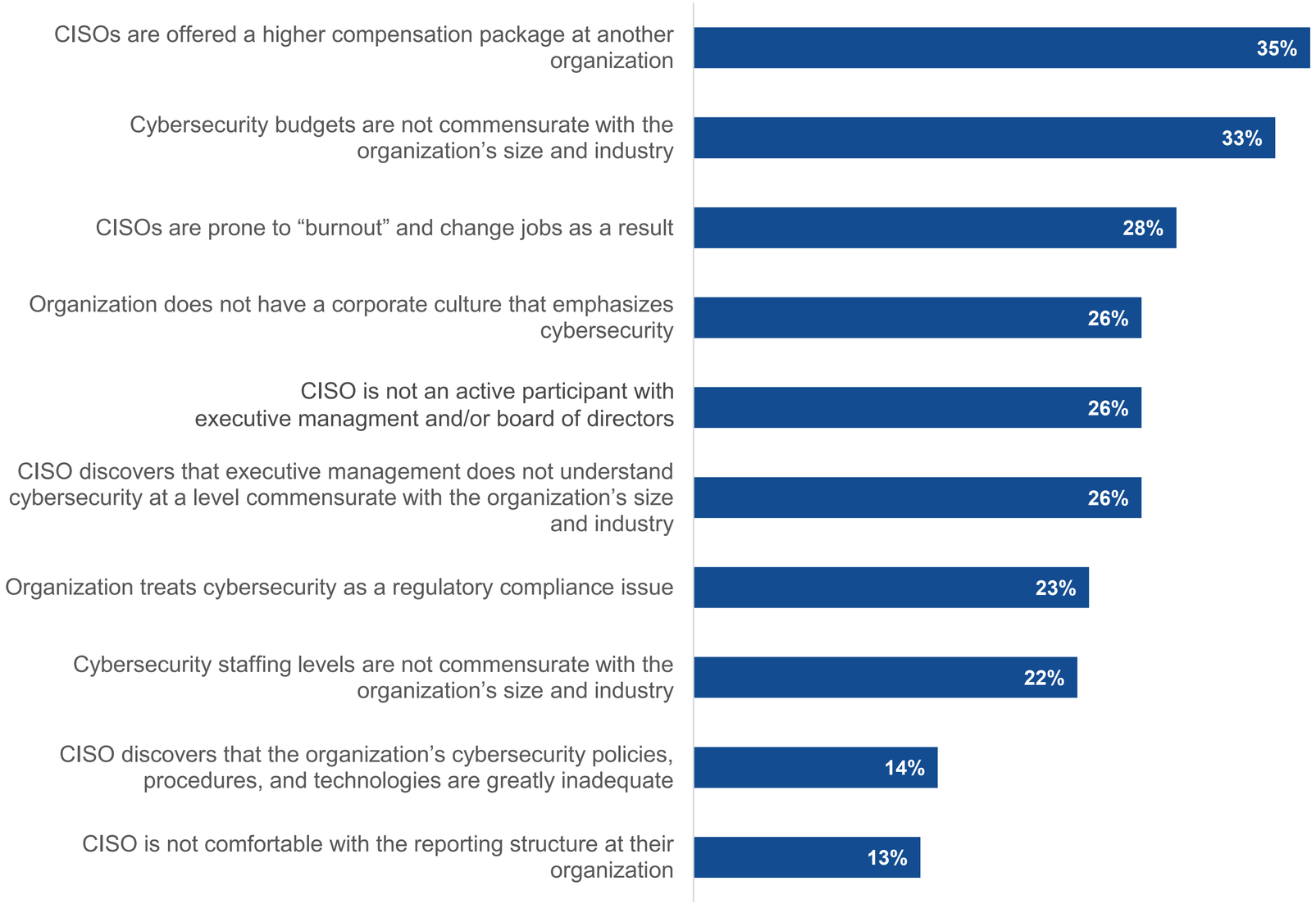


Percentage of respondents who believe their CISO's level of participation with executive management and the board of directors is adequate **by level of CISO effectiveness.** (Percent of respondents)



BACK TO CONTENTS

Likeliest causes for CISOs to leave one organization for another.



Why CISOs Change Jobs Often

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.

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.

BACK TO CONTENTS

Organizations Are Working Toward Future Cybersecurity Improvement

Improving Relationships Between Security and IT Teams

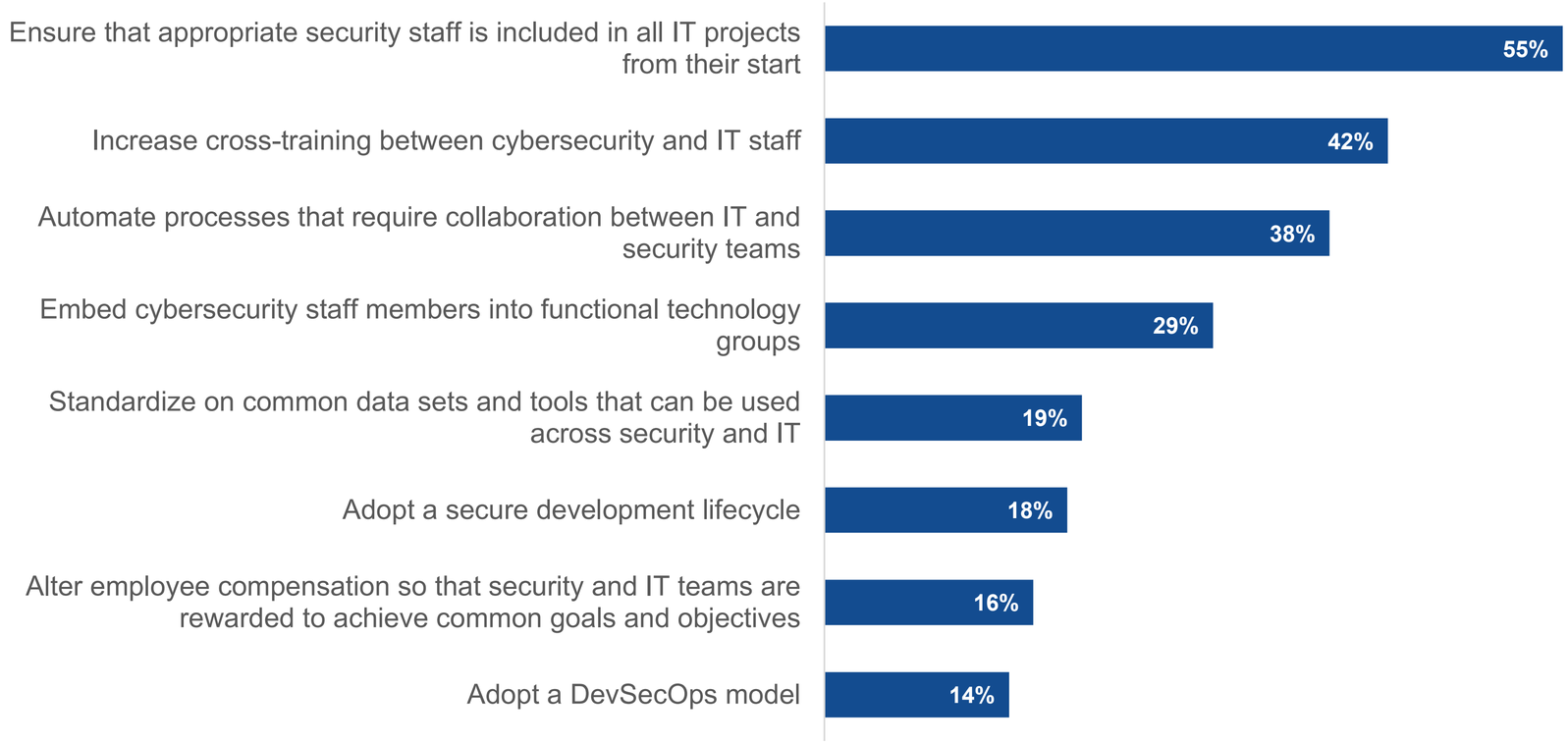
Most security professionals believe the relationship between security and IT teams is good, but there are exceptions as 24% rate this relationship as fair or poor. Survey respondents did offer some suggestions for improvement, such as ensuring security staff involvement in IT projects from their onset, increasing cross-training between IT and security, automating end-to-end processes, and embedding cybersecurity staff members into functional IT groups. 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 suggestion 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.

24%

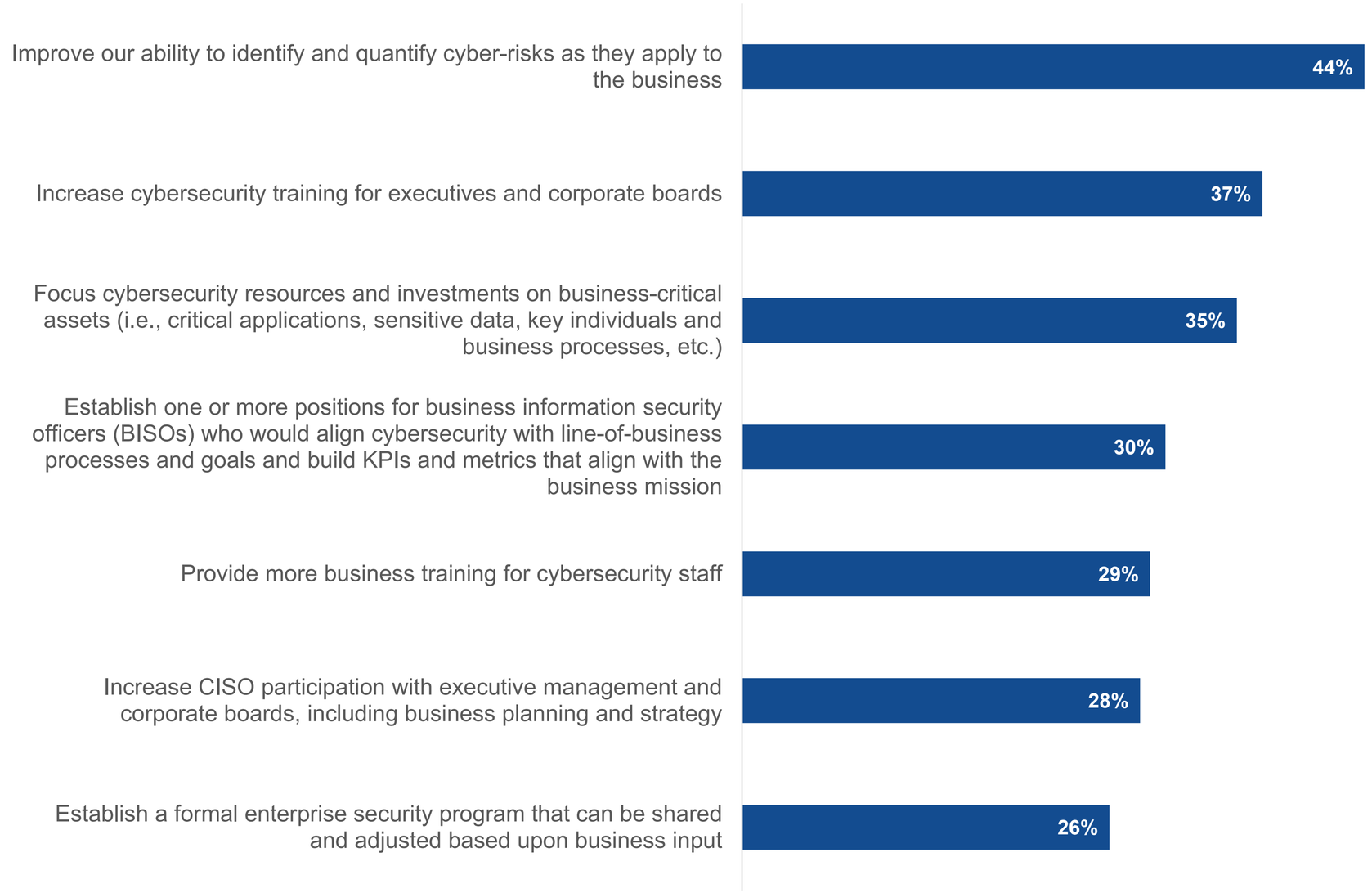
of organizations rate the **relationship between security and IT teams as fair or poor.**

Most impactful actions for improving the working relationship between the security and IT teams.



BACK TO CONTENTS

Most impactful actions for improving the working relationship between the security and business management teams.



Improving Relationships Between Security and Business Managers

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. 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.

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.

BACK TO CONTENTS

Improving the Cybersecurity Program

Finally, survey respondents were asked how their organizations could improve their overall cybersecurity programs. Some responses, 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 is vulnerable, and which of those vulnerable assets is 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.

Actions that could improve cybersecurity programs.

50%
Increase training for cybersecurity and IT professionals

45%
Strive to create a better cybersecurity culture throughout the organization

44%
Hire more staff

39%
Increase the cybersecurity budget

35%
Improve our basic security hygiene and posture management

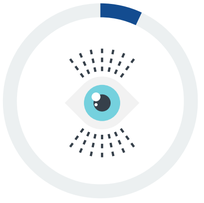
33%
Increase security awareness training for non-technical employees

33%
Improve our ability to prevent, detect, and respond to threats in a timely manner

29%
Conduct more frequent testing to validate our security controls and identify areas of weakness

29%
Get executives and the board of directors more involved in cybersecurity oversight and decision making

18%
Change the reporting structure so the CISO reports directly to the CEO



7%
Outsource more security responsibilities to third-party security service providers

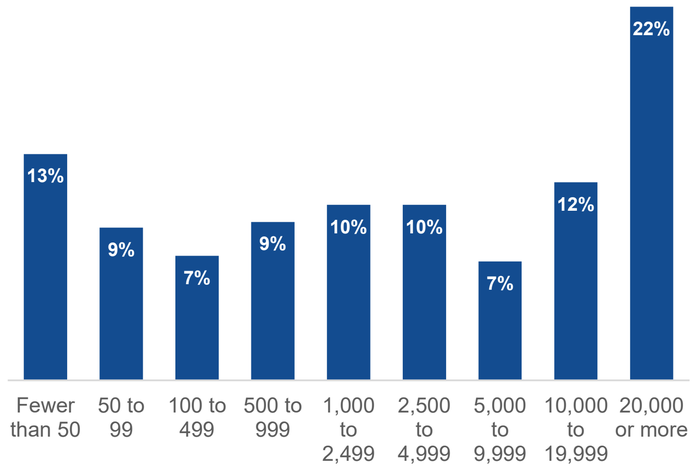
BACK TO CONTENTS

Respondent Demographics and Research Methodology

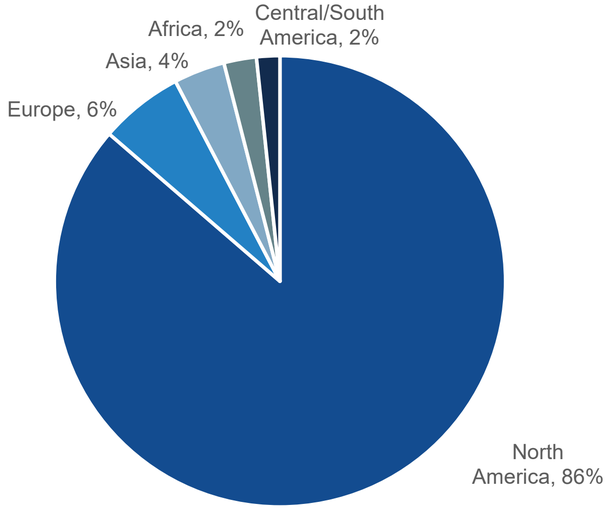
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations across the globe between February 7, 2023, and March 12, 2023. To qualify for this survey, respondents were required to be information security and 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.

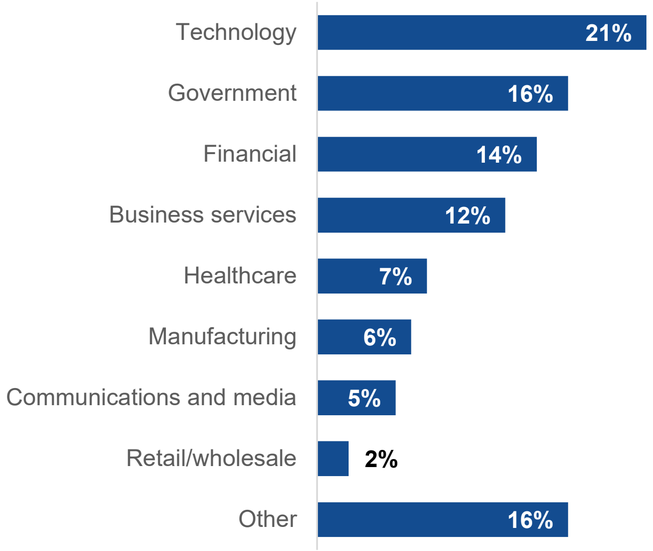
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY REGION

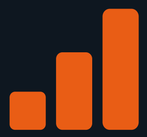


RESPONDENTS BY INDUSTRY



BACK TO CONTENTS

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.



Enterprise Strategy Group™
by TechTarget

ISSA
Information Systems Security Association International