Enterprise Strategy Group by TechTarget

ISSA Information Systems Security Association International

The Life and Times of Cybersecurity Professionals

VOLUME VII

Jon Oltsik | Analyst Emeritus

ENTERPRISE STRATEGY GROUP

SEPTEMBER 2024

Research Objectives

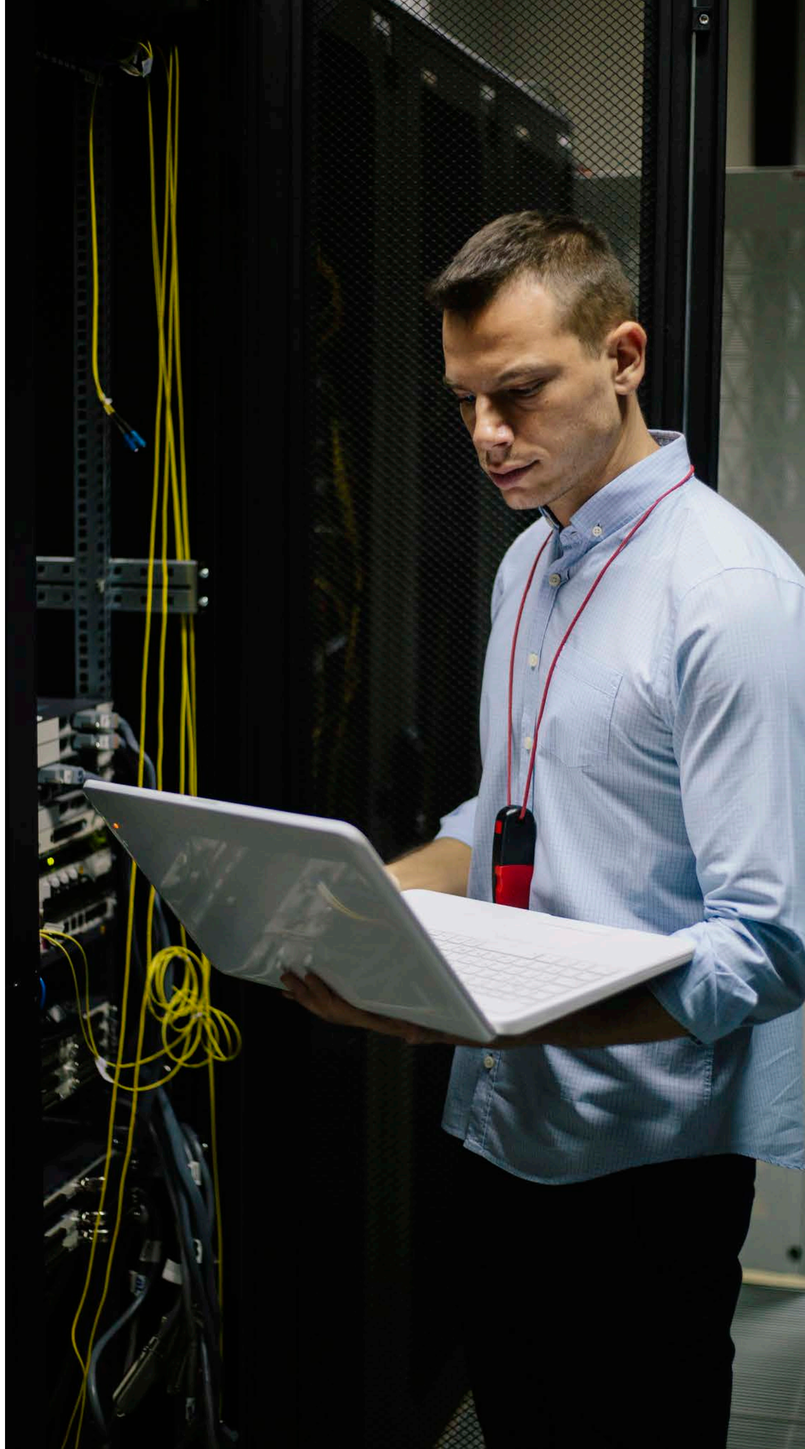
The seventh annual *Life and Times of Cybersecurity Professionals* study continues to pinpoint many of the same issues as past editions, underscoring persistent challenges such as rising cyberthreats, IT complexity, ubiquitous vulnerabilities, heavy workloads, and difficulties embedding cybersecurity 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 ebook can be found in *The Life and Times of Cybersecurity Professionals Volume VI.*

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.



Key Findings

Cybersecurity Professionals Face Growing Challenges in Their Field

PAGE 4

Job Satisfaction in Cybersecurity Is More Than Just a Paycheck

PAGE 8

Boosting Cybersecurity Programs Calls for More Training and a Cultural Shift

PAGE 17

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

PAGE 24

CISO Success Hinges on Top Notch Leadership and Communications Skills

PAGE 30

BACK TO CONTENTS

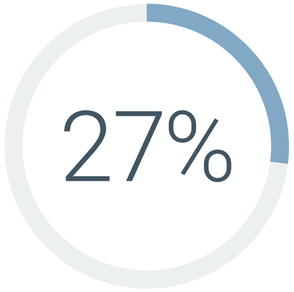
Cybersecurity Professionals Face Growing Challenges in Their Field

Cybersecurity Career Difficulty Over Time

Cybersecurity careers seem to grow more difficult each year. Indeed, 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.

Cybersecurity professionals face growing career difficulties due to various factors, including complex workloads, targeted threats, a growing attack surface, and regulatory compliance complexity overhead. Rapid technology evolution and adoption also introduce new vulnerabilities and attack vectors at an unprecedented pace, requiring continuous learning and adaptation from cybersecurity teams. These teams are often burdened by staff and skills shortages as well.

Perspectives on change in difficulty of cybersecurity career.



Working as a cybersecurity professional is much more difficult today than it was two years ago

Working as a cybersecurity professional is somewhat more difficult today than it was two years ago

Reasons working as a cybersecurity professional is more difficult today than it was two years ago.

BACK TO CONTENTS

Stressful Aspects of the Cybersecurity Profession

In this year's study, 57% of those surveyed claim their job is stressful at least half the time, slightly higher than 2023 (55%).

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. Nearly one-quarter of respondents citing keeping up with the security needs of new IT initiatives illustrates the need for security oversight of digital transformation and AI-based projects and initiatives.

Top five most stressful aspects of cybersecurity jobs/careers.

31%

Overwhelming workload

29%

Working with disinterested business managers

29%

Finding out about IT initiatives/ projects that were started by other teams within my organization with no security oversight

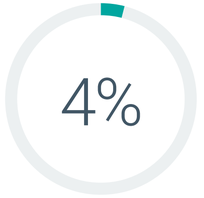
25%

Constant emergencies and disruptions that take me away from my primary tasks

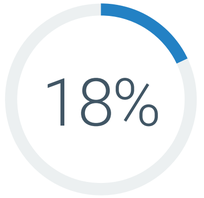
24%

Keeping up with the security needs of new IT initiatives

Stress level typically associated with cybersecurity careers.



Stressful **all the time** (i.e., stressful nearly 100% of the time)



Stressful **most of the time** (i.e., stressful 76% to 99% of the time)

Stressful **much of the time** (i.e., stressful 51% to 75% of the time)

Stressful **some of the time** (i.e., stressful 25% to 50% of the time)

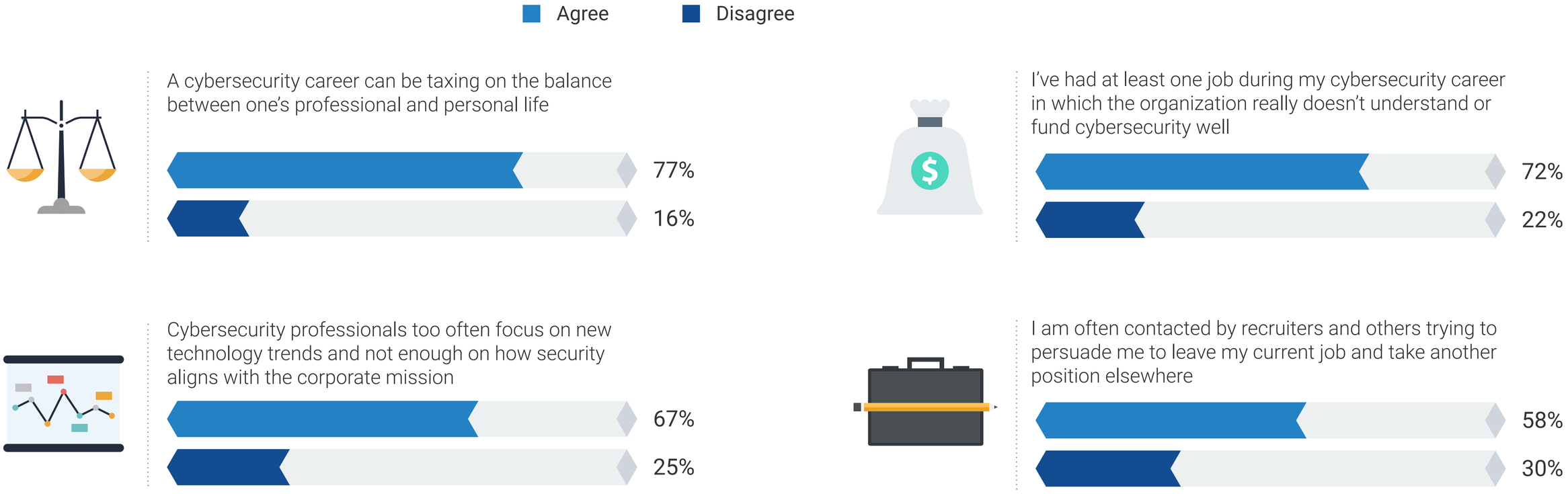
Stressful **only occasionally** (i.e., stressful less than 25% of the time)

BACK TO CONTENTS

Cybersecurity Professionals' Opinions on the Cyber Landscape

While cybersecurity careers grow more difficult and stressful, survey respondents face several other occupational hazards. A majority of those surveyed (77%) 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.

Perspectives on the cybersecurity landscape.



BACK TO CONTENTS

Job Satisfaction in Cybersecurity Is More Than Just a Paycheck

"One can only surmise that cybersecurity professionals are **willing to battle through occupational obstacles** in their commitment to the global cybersecurity mission."

What Is Driving Cybersecurity Job Satisfaction?

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, 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.

Satisfaction level for current job among cybersecurity professionals.

BACK TO CONTENTS

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. 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.

Biggest factors for determining job satisfaction level.

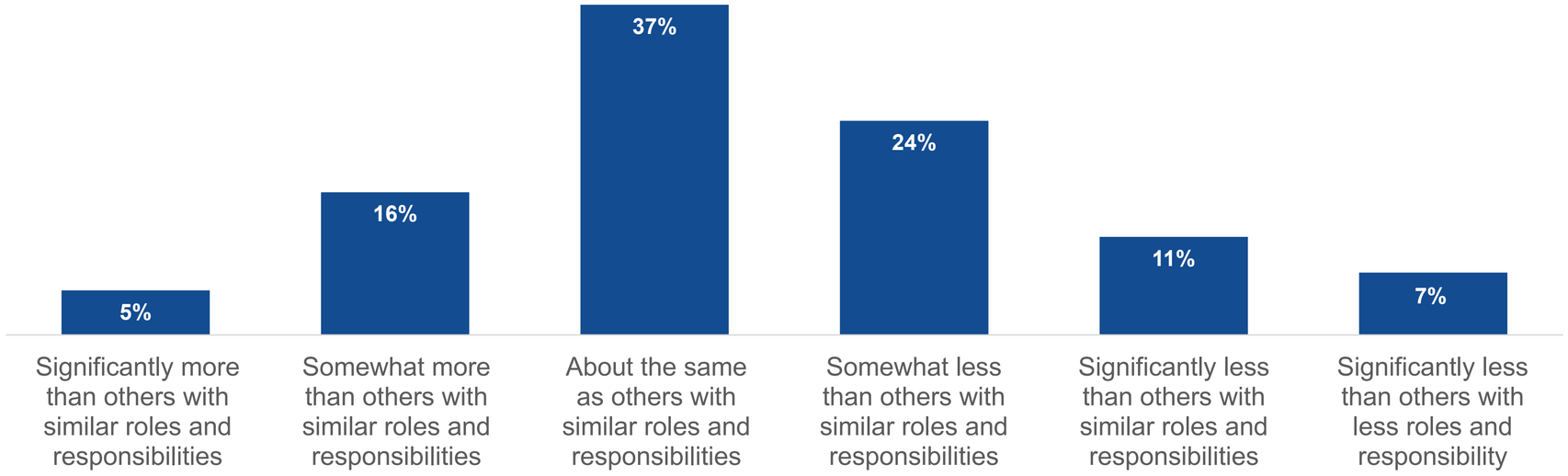
BACK TO CONTENTS

Expectations of a Salary Increase in 2024

As previously stated, compensation is one of the key factors in determining cybersecurity professional job satisfaction. The largest percentage of survey respondents (37%) believe their current compensation is in line with that of others with similar roles and responsibilities, but that is only part of the picture as the rest of the data skews in the wrong direction. More than four in ten (42%) cybersecurity professionals surveyed believe they make *less* than others with similar roles and responsibilities, compared with 21% who believe they make more than others in similar positions.

Many (53%) of those surveyed do expect their compensation to increase this year, but most anticipate only a slight upturn. Worse yet, 24% are unsure about a raise, while 22% don't think it will happen. CISOs, HR professionals, and recruiters should note this data, and align current and future compensation packages with competitive market offerings. Those who ignore this data are likely to face dissatisfied staff and constant attrition.

How cybersecurity professionals believe their compensation packages compare with peers' compensation packages.



Expected change in salary or other incremental benefits from current employers in 2024.

BACK TO CONTENTS

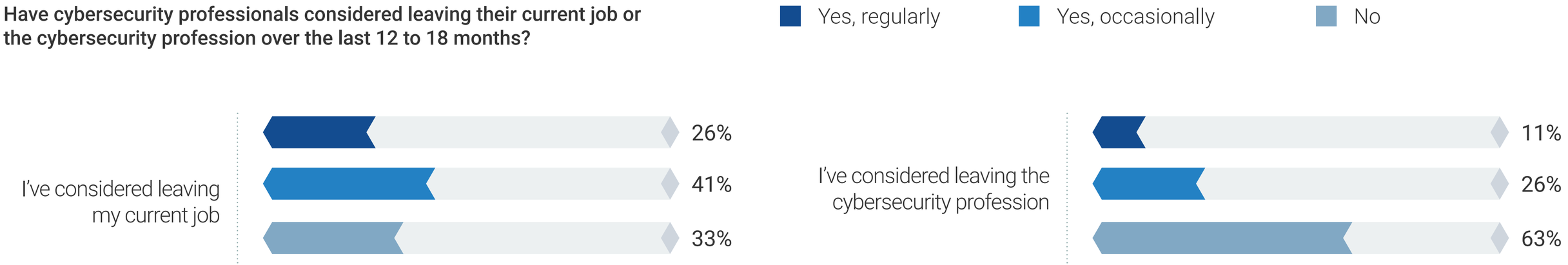
Potential for Leaving Current Cybersecurity Job or Even Entire Profession

Job stress, dissatisfaction, and compensation inequity are simply too much for many current cybersecurity professionals. Two-thirds 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.

Alarmingly, more than one-third (37%) have considered leaving the cybersecurity profession altogether (compared with 30% in 2023).

Percentage of cybersecurity professionals who have *regularly* considered leaving their current job based on how satisfied they are with that job.

Have cybersecurity professionals considered leaving their current job or the cybersecurity profession over the last 12 to 18 months?



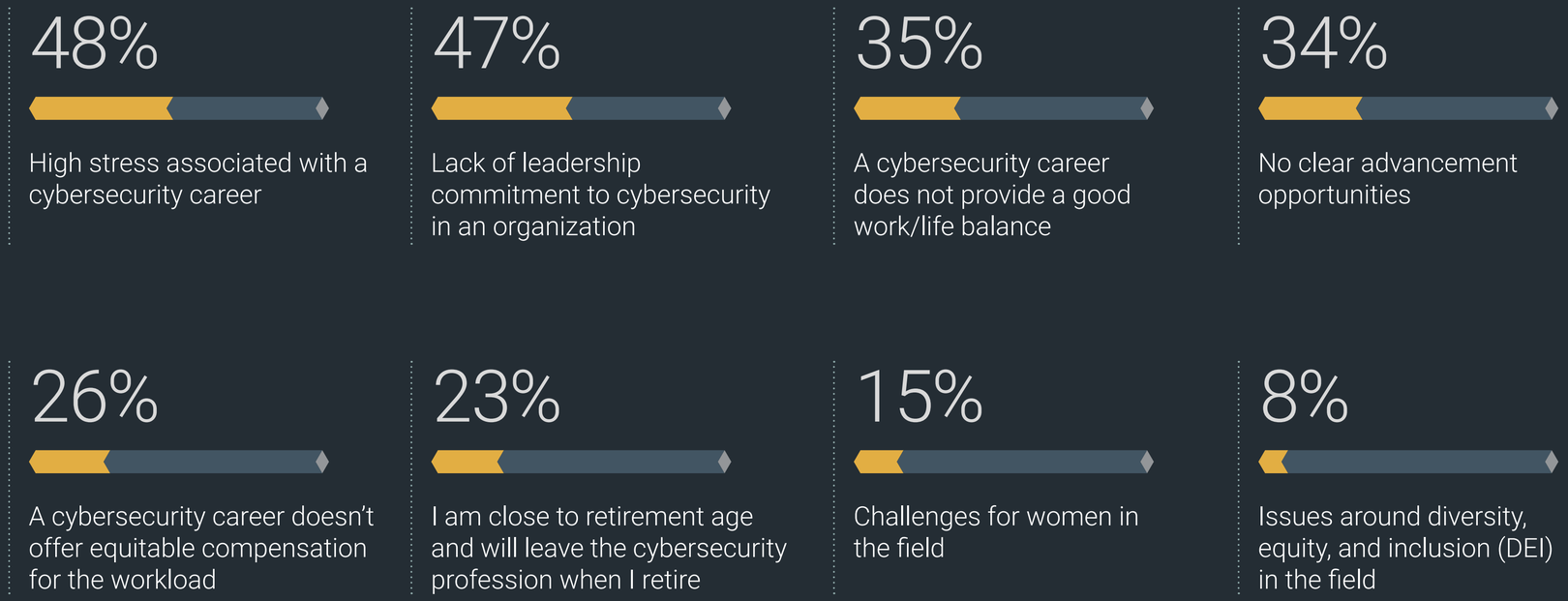
BACK TO CONTENTS

Why Leave Cybersecurity?

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.

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 "burn out," 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.

Considerations for leaving the cybersecurity profession over the last 12-18 months.



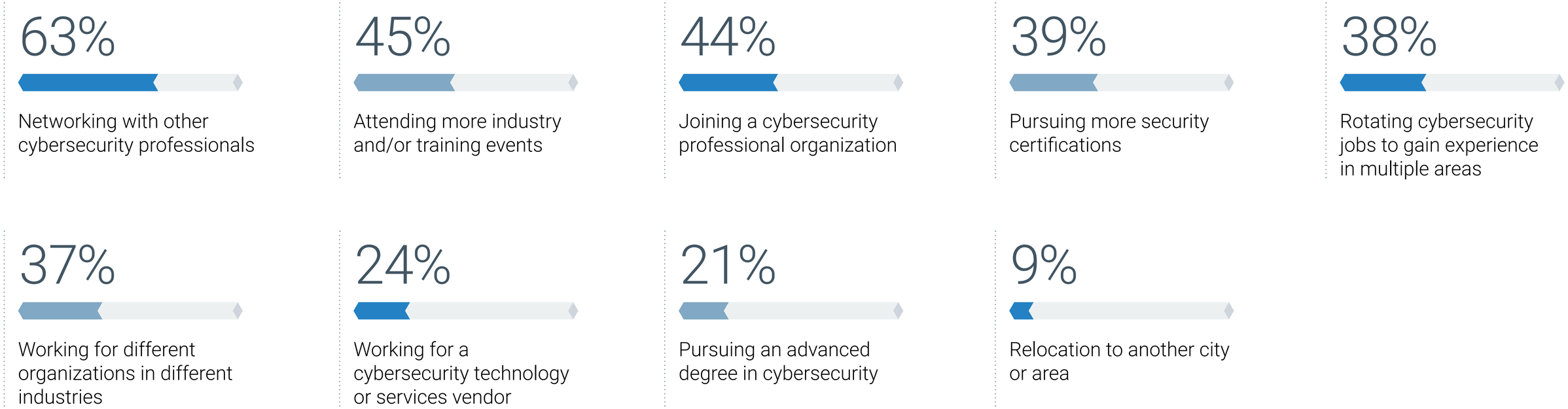
BACK TO CONTENTS

Career Advancement Techniques

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

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.

Most helpful actions for the advancement of cybersecurity careers.



BACK TO CONTENTS

Preferred Job Seeking Resources

When survey respondents do seek other job opportunities, they also rely on their peers and other cybersecurity professionals for guidance. Most tap into professional networks, social networks, professional associations, and even cybersecurity professionals who may be total strangers.

In aggregate, this data suggests that cybersecurity career flexibility and opportunity is inextricably linked to one's outreach and participation within the cybersecurity community. Cybersecurity professionals willing to network and engage with their peers will find ample opportunity for career development, continuous education, and compensation growth.

Resources cybersecurity professionals would rely upon to find a new job.

77%

Professional network (i.e., reaching out to past colleagues)

67%

Social networks/ platforms (e.g., LinkedIn, Facebook, etc.)

63%

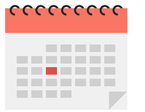
Professional cybersecurity associations

55%

Recruiters

54%

Networking (i.e., reaching out to people you don't know to try to find leads)



34%

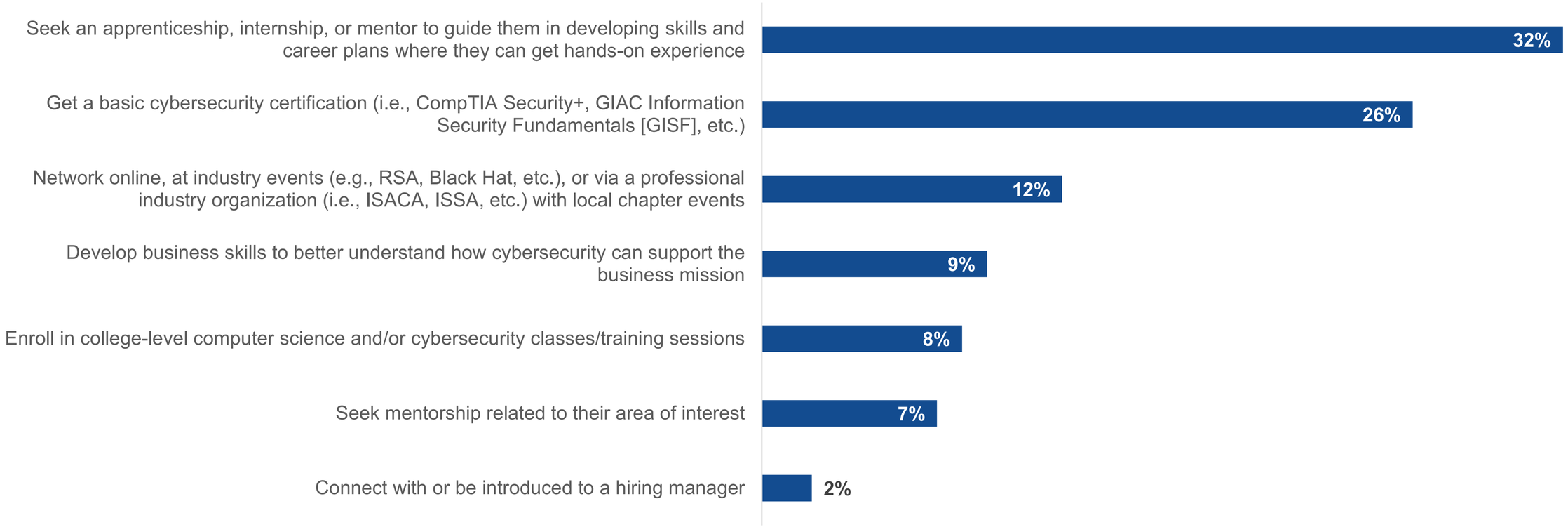
Industry events

BACK TO CONTENTS

Career Advice for Prospective Cybersecurity Professionals

Survey respondents also have advice for those trying to enter the cybersecurity field. Nearly one-third (32%) suggest seeking an apprenticeship, internship, or mentor as a starting point for getting hands-on experience. Additionally, cybersecurity professionals recommend a basic security certification and networking with others already in the field. These propositions are all intended to help entry-level candidates get a foot in the door. Once this occurs, they should be able to grow their career through networking, training, joining a professional organization, and remaining diligent with continuous education.

***Primary* piece of advice current cybersecurity professionals would give to prospective candidates.**



BACK TO CONTENTS

Boosting Cybersecurity Programs Calls for More Training and a Cultural Shift

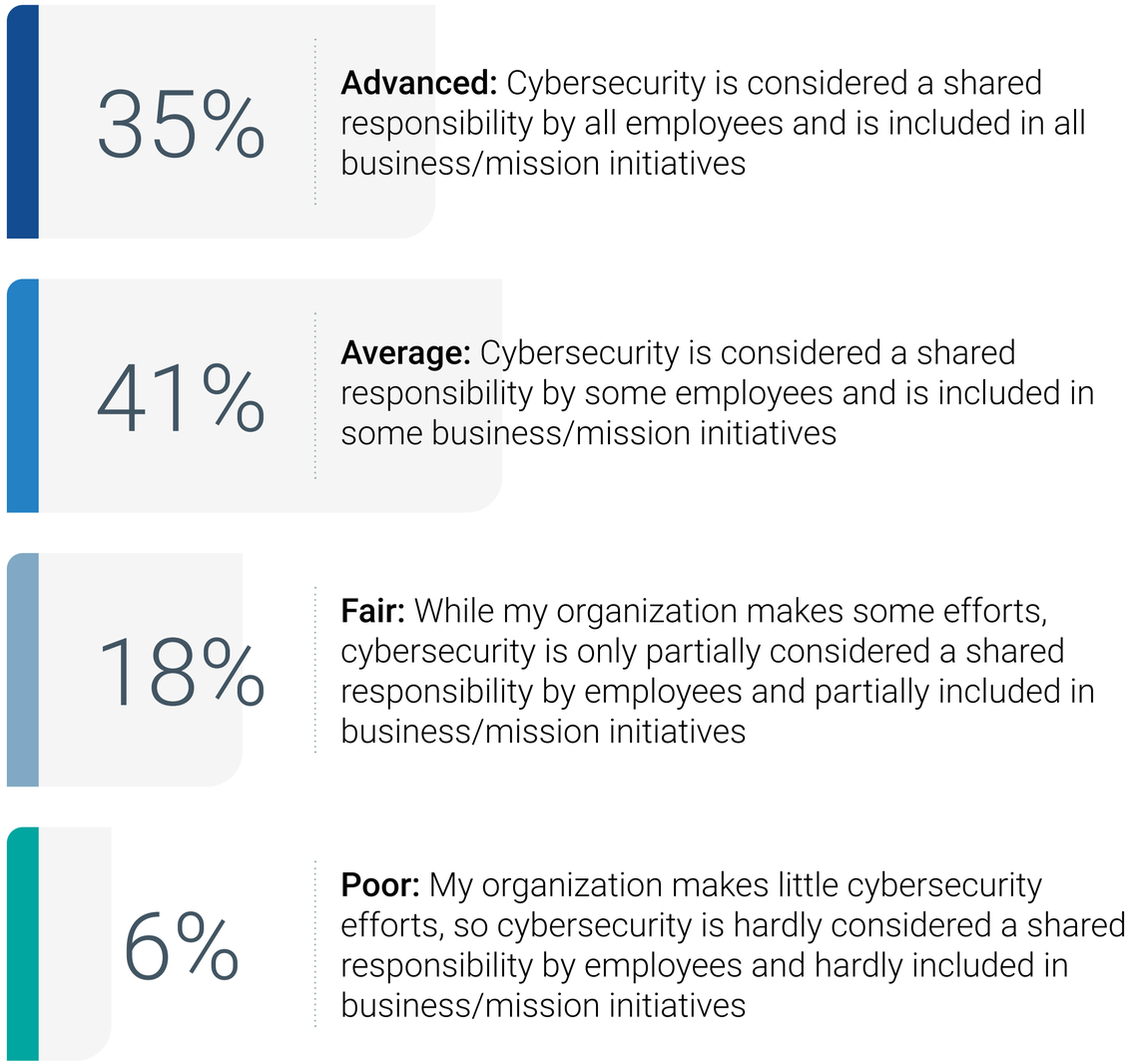
"While the data appears to be trending in the right direction, **Enterprise Strategy Group and ISSA view the results with caution."**

Rating the Organization's Cybersecurity Culture

When asked to rate their organization's cybersecurity culture, respondents provided ratings that are quite similar to last year's. Specifically, 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.

Characterization of organizations' cybersecurity culture.



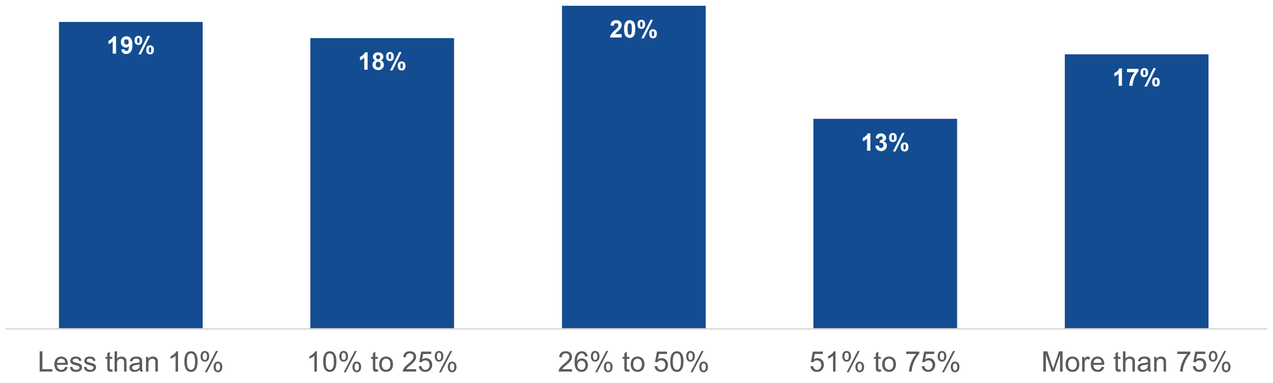
BACK TO CONTENTS

IT Staff Is Bearing a Cybersecurity Workload Burden, Confirming the Need for Collaborative Relationships

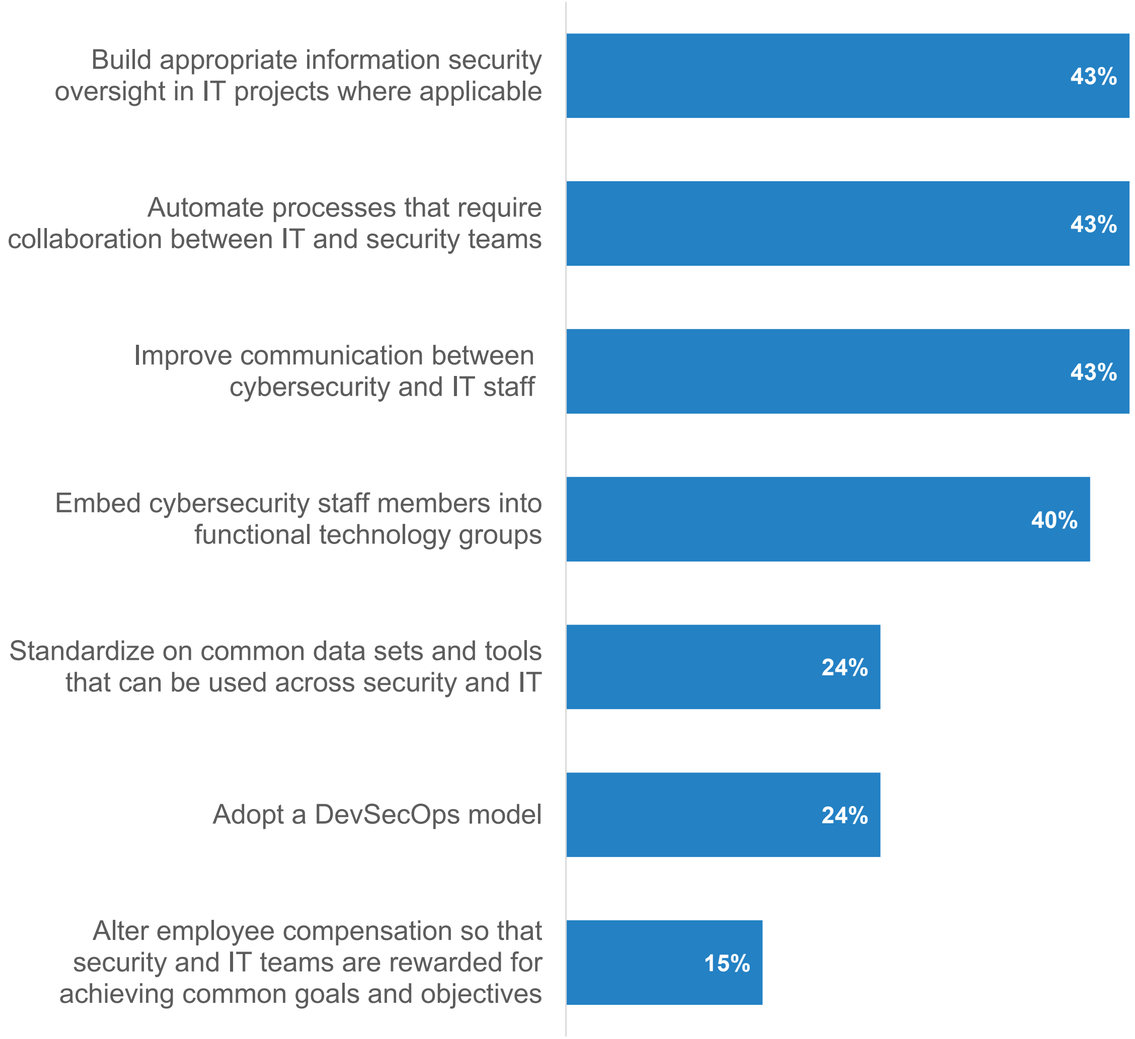
In a progressive organization, cybersecurity is everyone's job. For example, security professionals tend to monitor cyber-risks, identify technical vulnerabilities, and prioritize critical remediation actions. Upon executing these tasks, security teams often rely on IT operations, DevOps, and software 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 the research. According to survey respondents, 30% of cybersecurity professionals conclude 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. These recommendations are intended to implant security within IT people, processes, and technologies.

Approximate percentage of day-to-day security tasks done by people with IT titles.



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



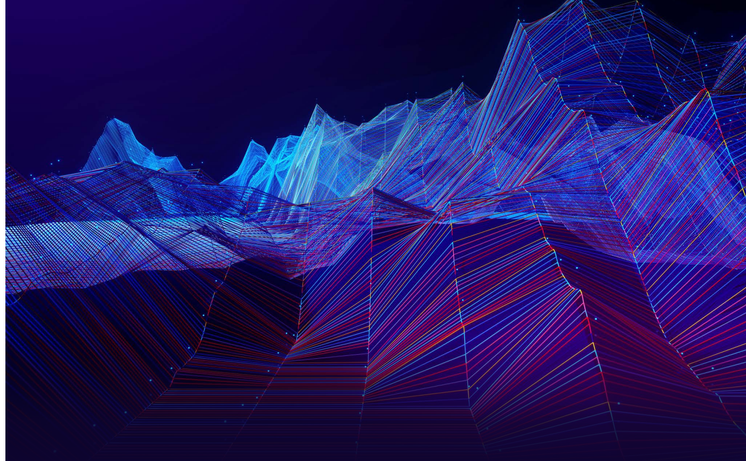
BACK TO CONTENTS

Improving Relationships Between Security and Business Managers

Cybersecurity professionals also offered multiple ideas for improving 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.

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.

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



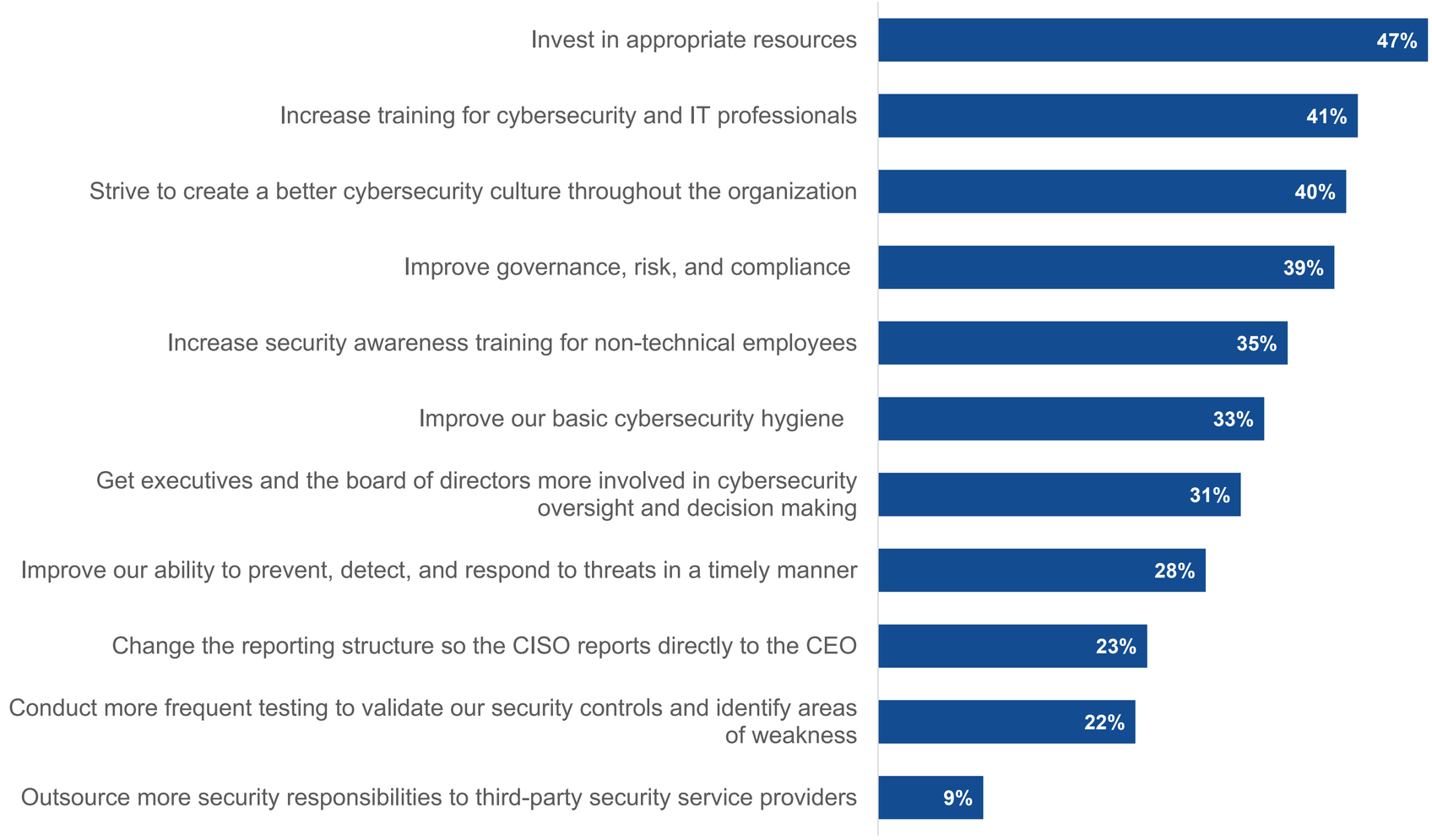
"By coming to a mutual agreement, business management and security teams can **better identify and monitor cyber-risk and use this cooperative effort to guide cybersecurity decisions.**"

Jon Oltsik,
Analyst Emeritus

Improving the Cybersecurity Program

According to survey respondents, 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.

Actions that could improve cybersecurity programs.



BACK TO CONTENTS

Improving Cybersecurity Culture

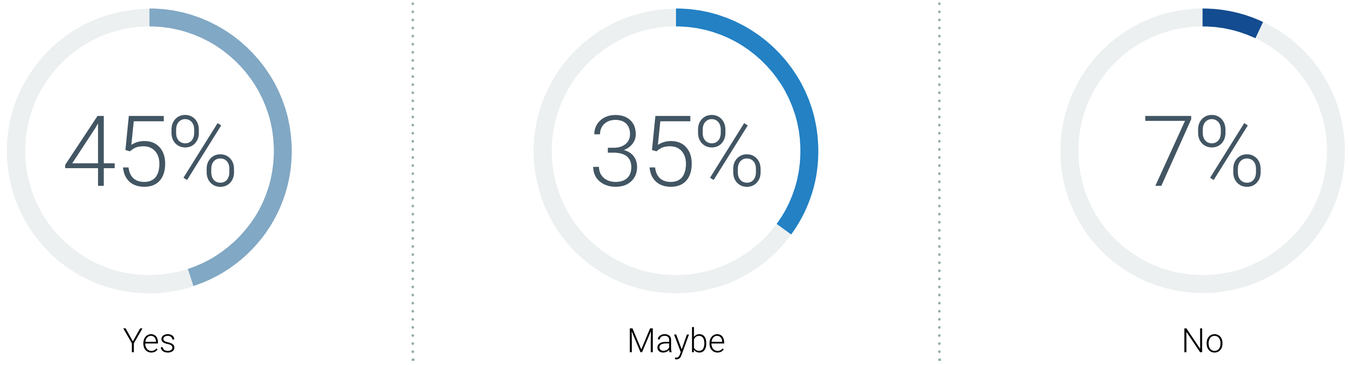
As in the past, survey respondents were asked what their organizations could do to improve cybersecurity culture. Forty-one percent said making managers more accountable for cybersecurity performance, an increase from 36% in 2023. Other suggestions included creating or adopting security standards and 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.

Actions that could improve cybersecurity culture.

Willingness to Act as a Cybersecurity Whistleblower

Throughout the history of the Enterprise Strategy Group and ISSA research on cybersecurity professionals, a clear pattern emerges: Cybersecurity professionals are extremely dedicated to the mission at hand. Indeed, many see themselves in an altruistic role as part of an existential battle between good and evil. Given this mindset, many cybersecurity professionals may take it personally if they are asked to compromise their ethics or ignore blatant cyber-risks. This may be why nearly half (45%) of survey respondents would willingly act as a whistleblower if they were put in a situation in which the organization they worked for knowingly ignored security best practices or regulatory compliance requirements, while another 35% would consider doing so (compared with 33% in 2023). Like last year, 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. In other words, dedication to the mission remains a core characteristic of the vast majority of cybersecurity professionals.

Would cybersecurity professionals be willing to act as whistleblowers?



"Throughout the history of the Enterprise Strategy Group and ISSA research on cybersecurity professionals, a clear pattern emerges: **Cybersecurity professionals are extremely dedicated to the mission at hand.**"

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

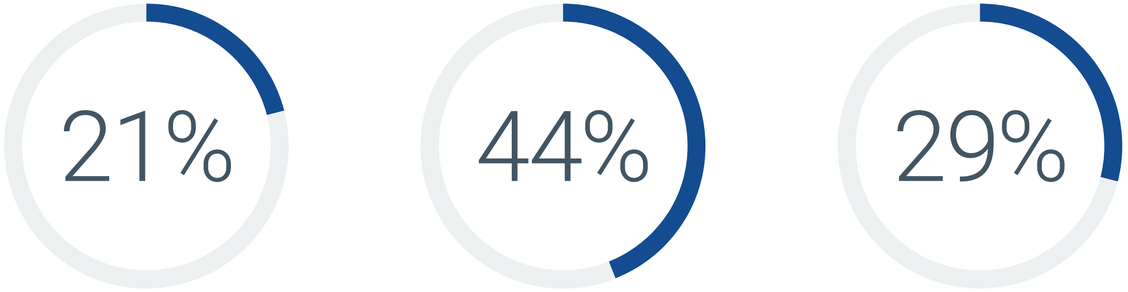
Impact of the Global Cybersecurity Skills Shortage

The cybersecurity skills shortage remains a perpetual problem. In 2024, 65% of survey 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%).

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 increasing use of managed security services.

Has the global cybersecurity skills shortage impacted organizations?



Change in cybersecurity skills shortage over the last two years.

BACK TO CONTENTS

Impact of the Cybersecurity Skills Shortage

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). 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 burn out 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.

Type of impact the global cybersecurity skills shortage has had.

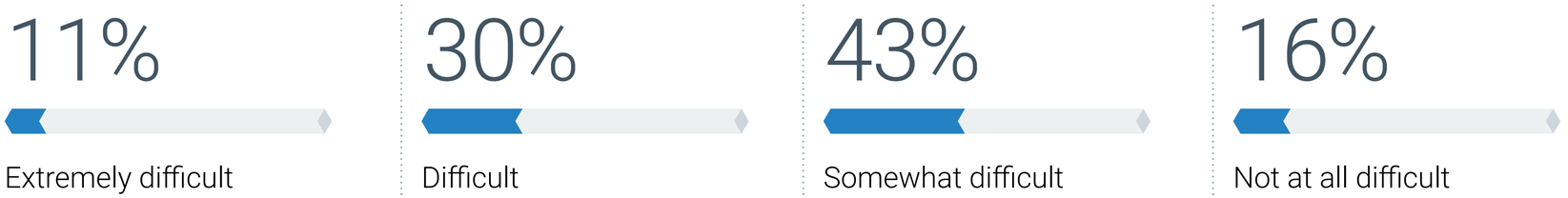
BACK TO CONTENTS

"Organizations that can't find or hire mid-career or senior practitioners **have no choice but to invest in continuous training for existing staff or seek managed security alternatives."**

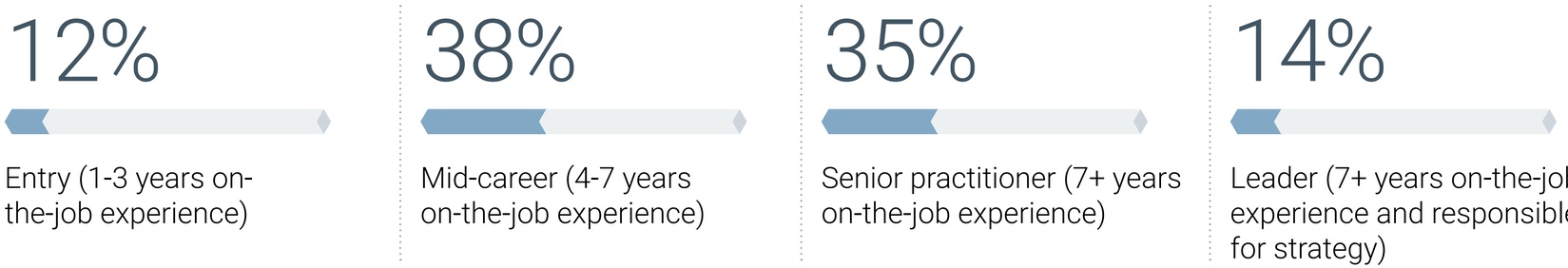
Degree of Difficulty Recruiting and Hiring Cybersecurity Staff

Difficulty with recruiting and hiring cybersecurity staff is yet another consequence of the cybersecurity skills shortage. In 2024, more than eight in ten (84%) organizations find it difficult to some extent to recruit and hire cybersecurity professionals (compared with 88% in 2023). The data also suggests that it is especially difficult to recruit and hire mid-career and senior practitioners. Individuals who fit this description are in high demand and often enjoy premium compensation packages. Organizations that can't find or hire mid-career or senior practitioners have no choice but to invest in continuous training for existing staff or seek managed security alternatives.

Level of difficulty recruiting and hiring cybersecurity professionals.



Group of cybersecurity professionals that organizations have the hardest time recruiting and hiring.



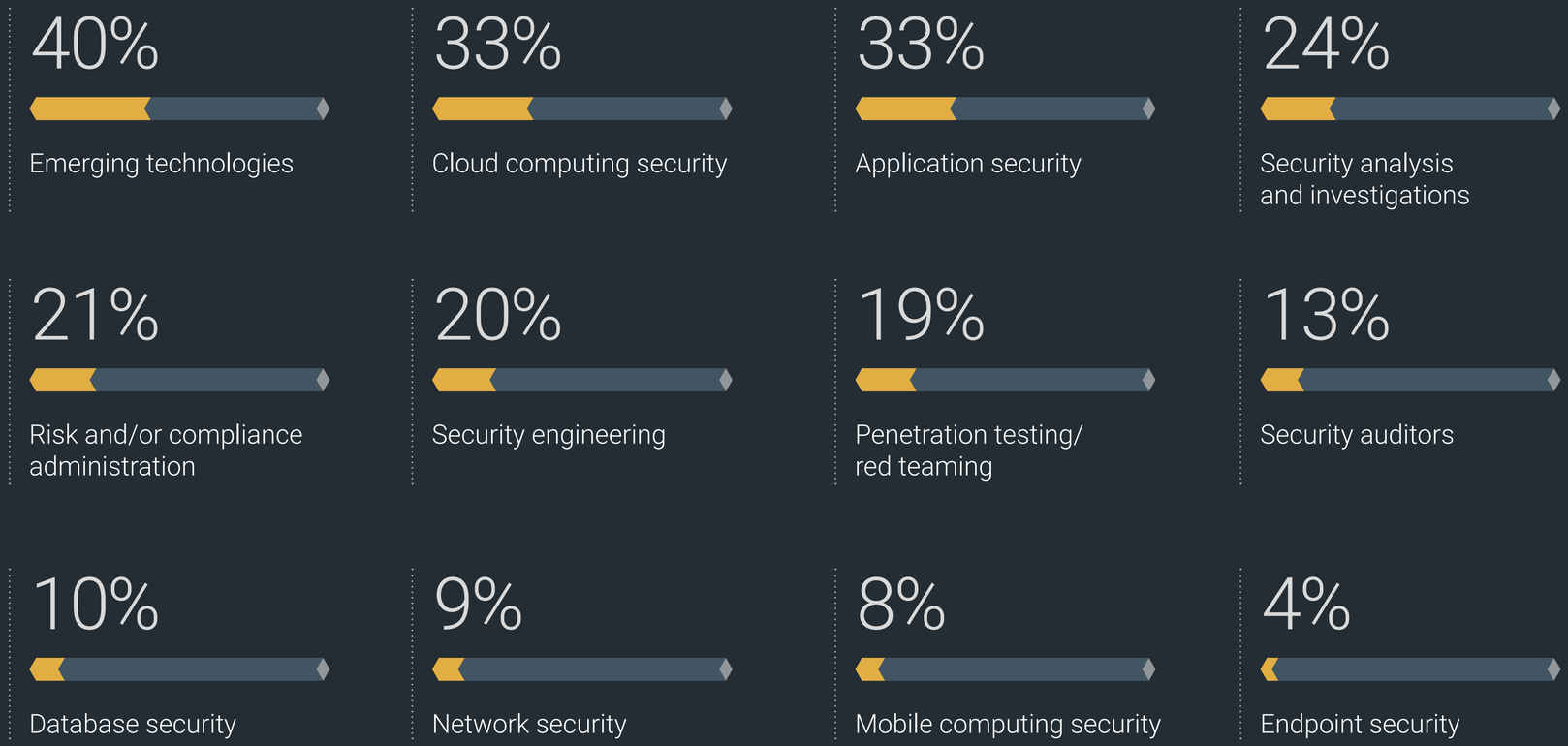
BACK TO CONTENTS

Most Significant Skills Shortage Areas

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.

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.

Areas with most significant shortage of cybersecurity skills.



BACK TO CONTENTS

Addressing the Impact of the Cybersecurity Skills Shortage

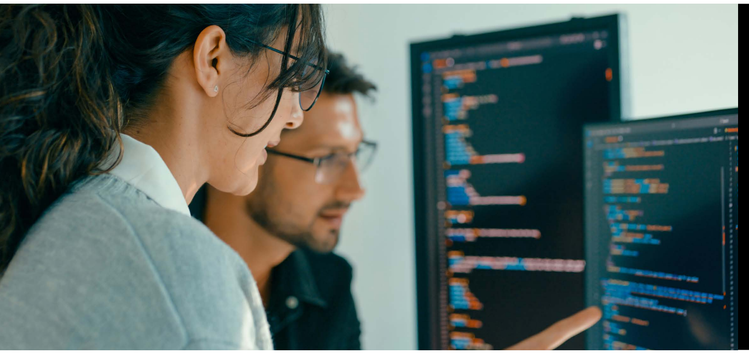
The security skills shortage remains omnipresent with no end in sight. Therefore, survey respondents were asked what their organizations could do to better address this ongoing challenge. Increasing compensation packages is an understandable response, but others are a bit less obvious. For example, survey 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.

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.

Actions organization could take to address the impact of the cybersecurity skills shortage.

BACK TO CONTENTS

CISO Success Hinges on Top Notch Leadership and Communications Skills



CISOs Commonly Report to CIOs

CISOs typically report to the CIO, although 27% of CISOs report directly to the CEO in this year's research. Additionally, 21% of those surveyed indicate there has been a change in the reporting structure over the past two years. This may be a function of the changing role of the CISO, from security technology steward to business executive.

Position to whom CISO reports.

- **42%** CIO or another senior IT person
- **27%** CEO
- **7%** COO
- **5%** Board of directors
- **12%** Other

Has the CISO reporting structure changed over the past two years?

21%

Yes

79%

No

BACK TO CONTENTS

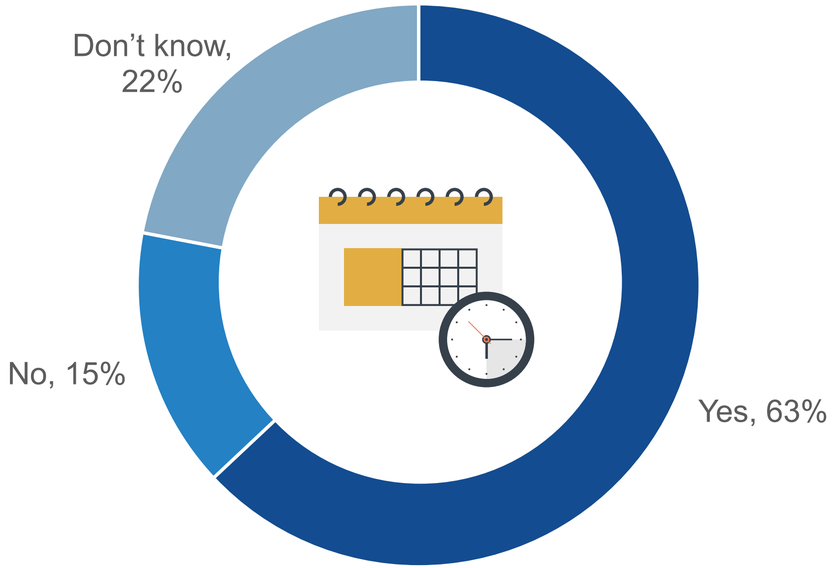
The Interaction of CISOs With the Board of Directors Is Mostly Considered Adequate

Nearly two-thirds (63%) of respondents report that their CISO regularly interacts with the board of directors, slightly lower than last year's result (75%), though this is probably a function of the fact that 21 of those surveyed work at smaller organizations (less than 500 employees) that may not have a board of directors or their CISO may also own IT.

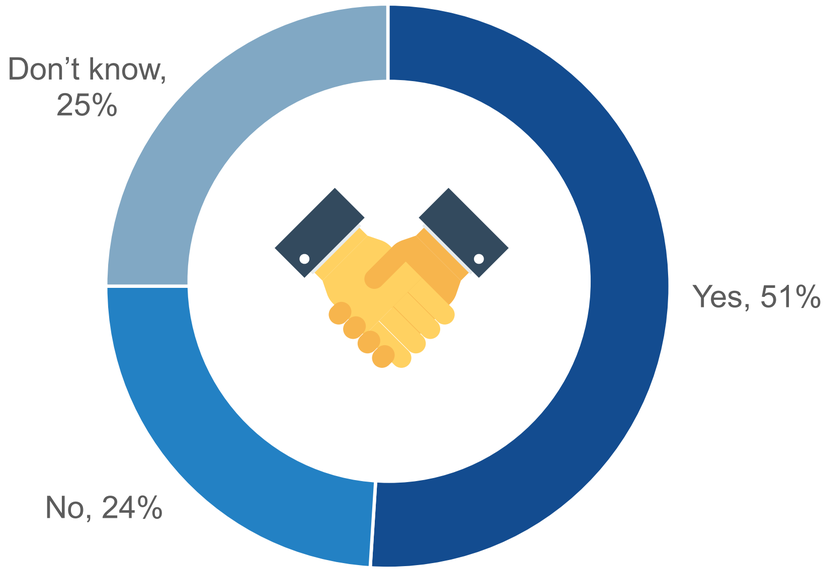
When asked if the CISO's level of interaction was adequate, just over half (51%) of respondents said it was. What's troubling is that nearly one-quarter (24%) of cybersecurity professionals don't believe the level of interaction is sufficient (27% in 2023).

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., NIS2). Corporate boards, executives, and CISOs should be working harmoniously to improve cyber-risk management, bolster cybersecurity awareness training, and protect business-critical assets.

Do CISOs regularly meet with executive management and the board of directors?



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



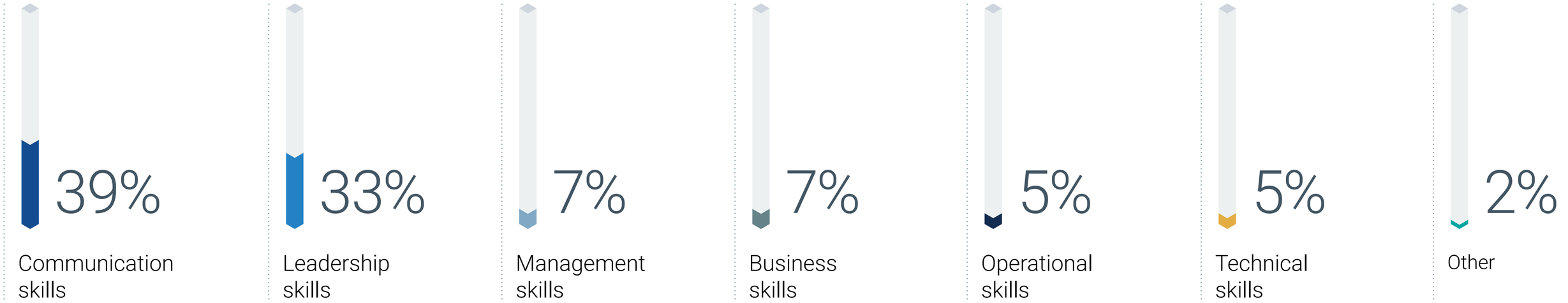
BACK TO CONTENTS

Important Qualities for Successful CISOs

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.

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.

Most important quality of a successful CISO.



BACK TO CONTENTS

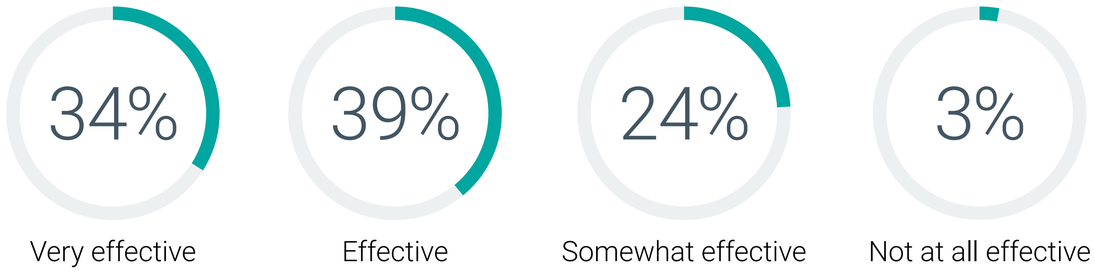
Effectiveness of CISO and What Causes Churn

Nearly three-quarters (73%) of respondents claim that their CISO is very effective or effective, similar to 2023 (71%). There is room for improvement, as 27% believe their CISO is somewhat effective or not effective at all, a slight improvement over 2023 (30%).

Regardless of effectiveness, many CISOs change jobs frequently, averaging between two and four years of tenure at each organization. Why is this the case? According to those surveyed, there are numerous reasons, many of which reflect on cybersecurity culture or the lack thereof. Indeed, respondents often believe CISOs change jobs when they discover that executive management doesn't prioritize cybersecurity, when budgets are not commensurate with the organization's size and industry, and/or when the CISO is not an active participant with executive management or the board of directors.

There are lessons to be learned here. CISOs should be extremely meticulous when performing due diligence on prospective employers so they can judge whether organizations take cybersecurity seriously or not. Executives and corporate boards have a similar task. They must honestly reflect on whether they provide the right commitment and resources to support a CISO's mission. Those who cannot have a choice: Step up or live with unacceptable levels of cyber-risk.

How effective are CISOs?



Factors that influence CISOs to leave one organization for another.

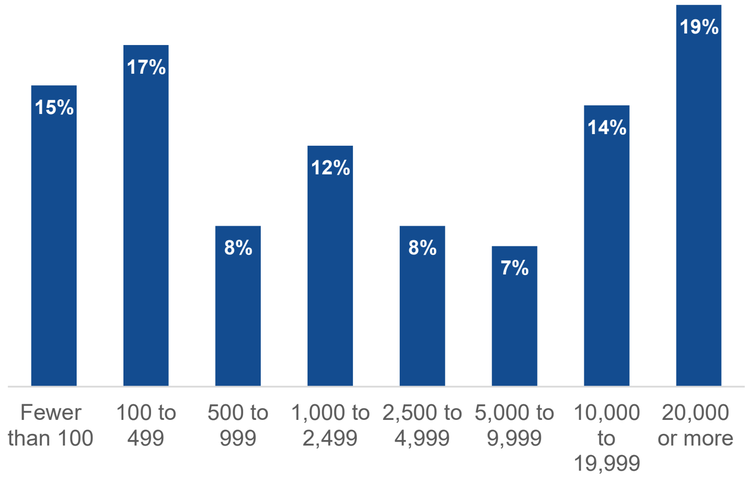
BACK TO CONTENTS

RESEARCH METHODOLOGY AND DEMOGRAPHICS

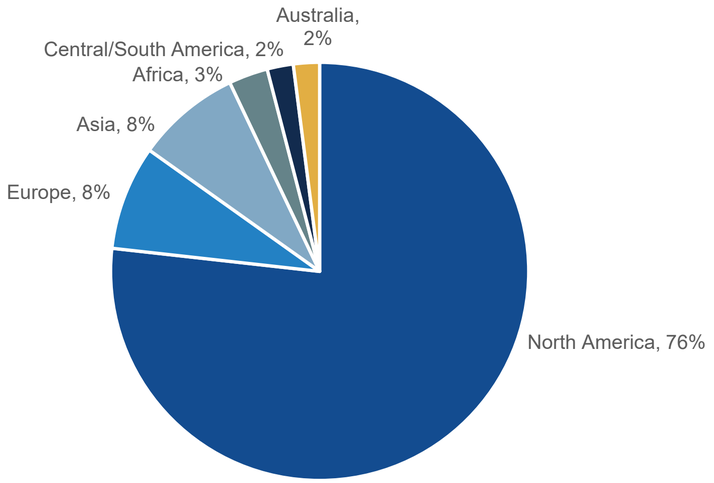
To gather data for this report, Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations across the globe between February 21, 2024 and March 18, 2024. To qualify for this survey, respondents were required to be information security 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 369 IT and cybersecurity professionals.

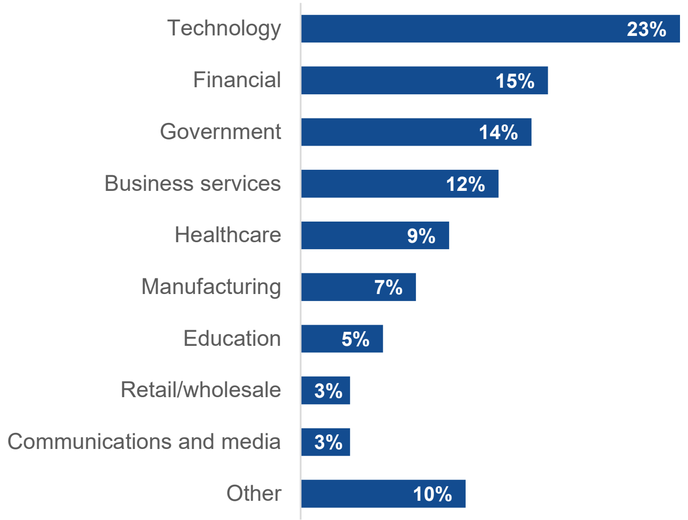
Respondents by number of employees.



Respondents by region.



Respondents by industry.



Enterprise Strategy Group and the Information Systems Security Association would like to thank the Cloud Security Alliance for supporting this research project.

BACK TO CONTENTS

Enterprise Strategy Group™
by TechTarget

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.