ISC2 CYBERSECURITY WORKFORCE STUDY

Cybersecurity Professionals Navigate Evolving Workplaces While Seizing New Opportunities

2025

Introduction

The cybersecurity workforce continues to navigate a range of disruptive economic, technological, skills and resource challenges. As last year's study revealed, cybersecurity teams are now equally exposed to the layoffs and hard-hitting budget cuts that have affected other teams when economic challenges emerge. However, the 2025 ISC2 Cybersecurity Workforce Study suggests that while cybersecurity budget cuts, layoffs, hiring freezes and other economic impacts remain, these pressures have leveled off and are not reported at higher rates this year. While signs of stabilization are at an early stage, this could be an indicator of a reset, as organizations take stock of their ability to deal with new technologies and economic realities.

In addition to these resource constraints, which a significant proportion of respondents expect to continue through the year ahead, the workforce faces increased cybersecurity risk while it attempts to keep pace with rapid change in cybersecurity technologies for both defense and offense. Artificial intelligence (AI) cybersecurity tools are being implemented across many organizations, impacting the way cybersecurity professionals carry out their roles, as well as evolving the core skills they need to remain effective and relevant. At the same time, automation is also driving the sophistication and frequency of AI-powered attacks.

Aware of both the challenges and opportunities presented by AI, cybersecurity professionals are taking a pragmatic approach to these new technologies. Traditional roles like SOC analyst and incident responder, among others, are evolving. Security professionals are optimistic about AI and its short- and longer-term implications for them. Rather than replacing jobs, cybersecurity personnel expect roles to emerge and evolve in order to manage this new, increasingly complex landscape. Looking ahead, they are prioritizing AI skills development and qualifications.

The Cybersecurity Workforce is Evolving

In addition to AI, this year's study also highlights growing skills needs within cybersecurity teams. Findings also suggest a mindset shift by professionals in how they view their skills needs when compared to a shortage of people. Addressing specific needs is no longer solved just by adding people but by investing in the professional development of existing team members. The need for technical and nontechnical skills remains high, with many reporting a need for specialized skills such as incident response and security engineering. Some organizations are meeting these needs with external contractors or service providers, while others are upskilling and multiskilling personnel to support cybersecurity needs.

Finally, economic challenges, skills and staff shortages and the rapid evolution of the workplace are challenging the morale of cybersecurity professionals. There are indications of improving job and career satisfaction after two years of decline, but employers should be mindful of warning signs that professionals are unsatisfied with organizational leadership and are considering finding new roles with other employers. Our findings explore how stagnant wages, increased workload and lack of professional advancement opportunities impact workforce satisfaction.

A record 16,029 cybersecurity practitioners and decision-makers participated in the 2025 study from across North America, Latin America, the Asia-Pacific region and Europe, the Middle East and Africa.

Research Note

For years, the ISC2 Cybersecurity Workforce Study has been informed by cybersecurity professionals' view that the shortage of qualified people in the field was the most prominent factor impacting their ability to effectively defend their organizations. In recent years and more clearly in 2025, professionals participating in our study are evolving their opinions. Respondents to the 2024 and 2025 studies have prioritized the need for critical skills as more important than the need for more people.

Therefore, ISC2 has not included an estimate of the cybersecurity workforce gap this year. Previous years have included a measure of the difference between the number of cybersecurity professionals that study participants say their organizations require to properly secure themselves and the number of active cybersecurity professionals. While cybersecurity professionals continue to report workforce shortages within their teams, we have been led by participant responses that highlight a range of more pressing and specific measures of skills and staffing needs.

Key Findings

Economic uncertainty continues to weigh heavily on cybersecurity teams

The surge in hiring freezes, layoffs, budget cuts and promotions reported in 2024 shows signs of stabilizing in 2025. Figures are beginning to level off rather than significantly diminishing, intimating the economic drivers that are forcing caution on spending to remain, adding pressure on existing cybersecurity teams. Many in the cybersecurity workforce are worried that economic austerity will harm the security resilience of the organizations in which they work.

Skills and staff shortages are raising cybersecurity risk levels and challenging business resilience

The economic and budget issues that have held back or diminished hiring and investment in skills have also contributed to knowledge and competency deficits within organizations and their cybersecurity teams. Organizations must find ways to widen their skills base and talent pools — including investing in existing personnel through multiskilling and skills investment — despite budgetary constraints, to bolster cybersecurity capability and meet demand.

AI has shaken up the cybersecurity workforce, but positivity remains high as professionals foresee career opportunities

AI is redefining both cybercrime and cybersecurity. However, far from being daunted, those within the cybersecurity workforce who are actively using AI tools are positive about the current and future impact of the technology, seeing opportunities for skills development, along with the creation of more and new jobs. They continue to see a symbiotic future where AI enhances the cybersecurity working experience rather than replacing skilled personnel.

Job satisfaction is positive in the face of extensive disruption, but warning signs exist for team leaders and employers

Workers remain passionate and fulfilled by their career choice, but do not necessarily feel the same about their wider organizations. Employers and hiring managers need to ensure that cybersecurity professionals feel seen and heard, and that they have access to opportunities to advance in their careers and knowledge to remain relevant. Retention may become a challenge when the job market improves.

Economic Factors Weigh Heavily on Cybersecurity Resources

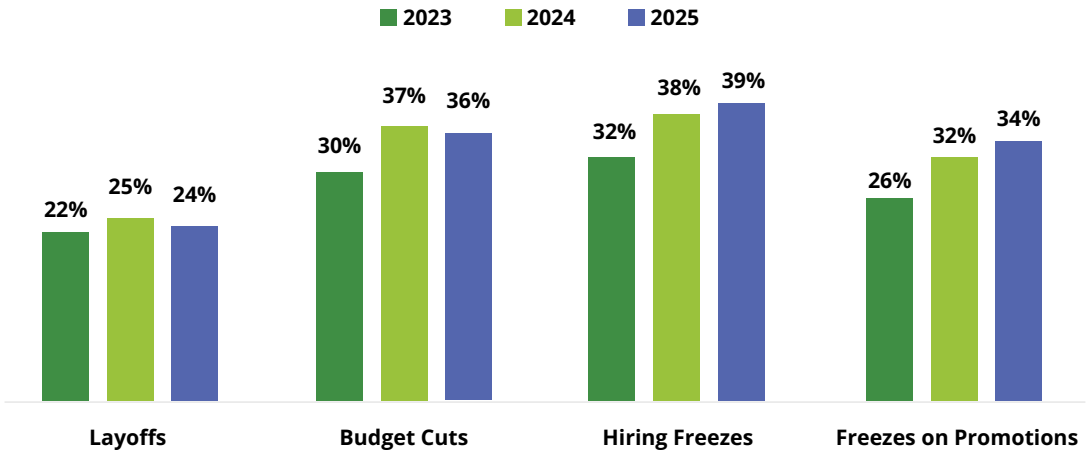
In previous iterations of the study, we acknowledged cybersecurity teams were experiencing a degree of protection from the economic and headcount pressures impacting their colleagues outside cybersecurity roles and across the wider organization. However, across 2023 and 2024, it became clear that these pressures had begun to reach cybersecurity teams, with respondents reporting year-on-year decreases in hiring and increased layoffs and pay freezes.

While respondents continue to highlight issues with budget constraints, staffing levels and investment in people and supporting resources, 2025 has seen the first signs that the situation is starting to level out rather than get considerably worse.

Respondent organizations experiencing budget cuts, for example, rose by 7% from 30% in 2023 to 37% in 2024. In 2025, this figure fell, but only by 1% to 36%. Hiring freezes also remained broadly flat, increasing by 1% from 2024 to 39%. Meanwhile, promotion freezes slowed, increasing by just 2% in 2025 to 34%.

Respondents reported that cybersecurity layoffs in 2025 fell by 1% to 24%, further supporting the notion that economic and operational pressure on cybersecurity teams and budgets are leveling off. While respondents are not suggesting any marked improvement in organizational cuts and freezes, they have expressed that conditions remained broadly flat year-on-year. This was alongside still reporting ongoing problems related to the diminished resources, capabilities and skills that previous years' organizational cuts have had on the field.

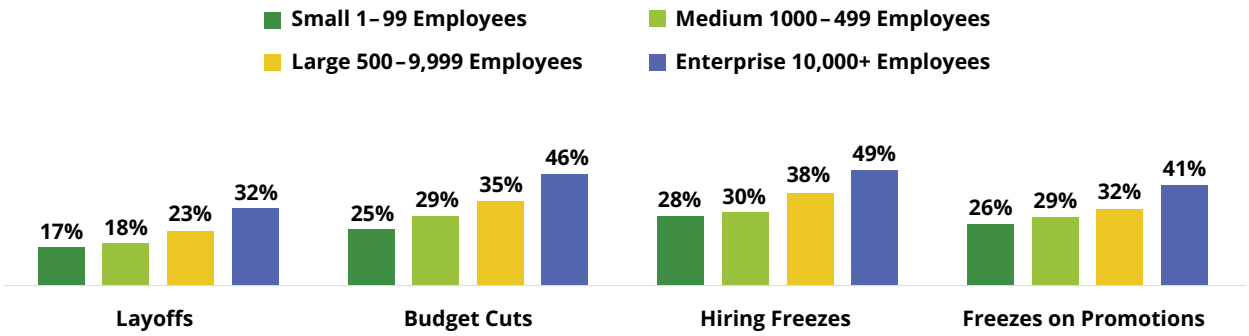
Cybersecurity Cutbacks Experienced by Organizations in the Past 12 Months



The overall picture varies considerably when we look at respondents' organizations by size. The largest enterprise organizations (10,000+ staff) are reporting cybersecurity layoffs at significantly higher rates (32%) than their small- (1–99 staff — 17%) and medium-sized (100–499 staff — 18%) counterparts. Nearly half (49%) of enterprise organizations are still implementing cybersecurity hiring freezes, significantly higher than the overall average of 34%, and almost double that of the smallest organizations included in the study (28%).

Cybersecurity Cutbacks Over the Past 12 Months by Organization Size

In all cases, small organizations fared better than larger ones, experiencing cutbacks to a lesser extent.



All four measures of cutbacks increase as organization size grows. Smaller organizations, the bedrock of most economies, have traditionally struggled with hiring and retaining cybersecurity staff. As a result, they have less capacity to cut relative to their larger counterparts, which have bigger teams as well as higher operating costs that need more extensive economizing to maintain fiscal targets.

Technology-driven sectors are feeling the most economic pain, with layoffs being reported across cloud services (33%), hardware and software development (31%), aerospace (31%), automotive (29%) and non-security hardware and software development (28%). In contrast, those with the lowest exposure to layoffs were more diverse, with education reporting 11%, legal at 12% and the nonprofit sector at 13%, followed by construction (18%) and manufacturing (19%).

Industries MOST Affected by Cybersecurity Layoffs

33%	Hosted/Cloud Services
31%	Security Software/ Hardware Development
31%	Aerospace
29%	Automotive
28%	Nonsecurity Software/ Hardware Development

Industries LEAST Affected by Cybersecurity Layoffs

11%	Education
12%	Legal
13%	Nonprofit
18%	Construction
19%	Manufacturing

Budget cuts by sector do not directly mirror what has happened with layoffs, with agriculture experiencing the highest percentage of reported cybersecurity budget cuts (43%), ahead of non-security hardware and software development, telecommunications, hospitality and government (all at 41%). In contrast, the sectors with the lowest exposure to budget cutting broadly map to the same ones that experienced lower rates of cybersecurity layoffs, with legal having the lowest percentage of budget cuts (19%), followed by education (26%), construction (28%) and nonprofits (31%).

Industries MOST Affected by Cybersecurity Budget Cuts

43%	Agriculture
41%	Nonsecurity Software/ Hardware Development
41%	Telecommunications
41%	Food/Beverage Hospitality
41%	Government (Nonmilitary)

Industries LEAST Affected by Cybersecurity Budget Cuts

19%	Legal
26%	Education
28%	Construction
31%	Nonprofit
33%	Real Estate

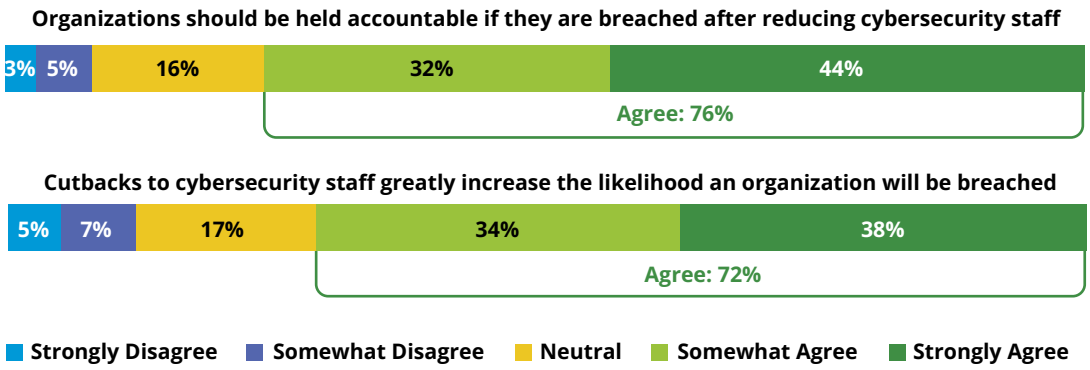
Many expect these issues to continue, with 31% of respondents anticipating more cybersecurity cutbacks over the next 12 months — similar to what participants in our 2024 survey forecast. Within the same period, 26% also predict more layoffs — higher than 2024 participants predicted (22%).

According to study participants, sustained economic cutbacks impact the cybersecurity posture and readiness of organizations. Budget reductions are the key driver of staff shortages, as 33% of organizations don't have the budget to adequately staff their teams, while 29% cannot afford to hire staff with the skills they need. A recurring theme throughout this year's study is the impact of lower budgets on the ability to hire the people and add the skills needed to deliver critical cybersecurity capabilities.

At present, more than half (55%) agree their organizations have the resources necessary to address security incidents in the next 2–3 years (with less than a quarter strongly agreeing). Reductions in staff numbers, however, significantly raise respondents' organizational risk factors. As staff numbers decline, so do the available skills within an organization needed to leverage the latest cybersecurity tools and technologies, as well as to understand and combat rapidly evolving threats and attack tactics.

The majority of respondents believe this to be the case, as 72% of respondents agreed that reducing cybersecurity personnel significantly increases the risk of a breach, demonstrating the relative link between negative economic pressure and reduced cybersecurity resilience. This view is further elevated by 76% of respondents stating that organizations should be held accountable if they suffer a breach after cutting cybersecurity staff. Most respondents agree that if cybersecurity leaders are forced to eliminate people and skills to achieve cost savings, the cyber risk profile of their organizations will increase significantly, leaving them more vulnerable to attack.

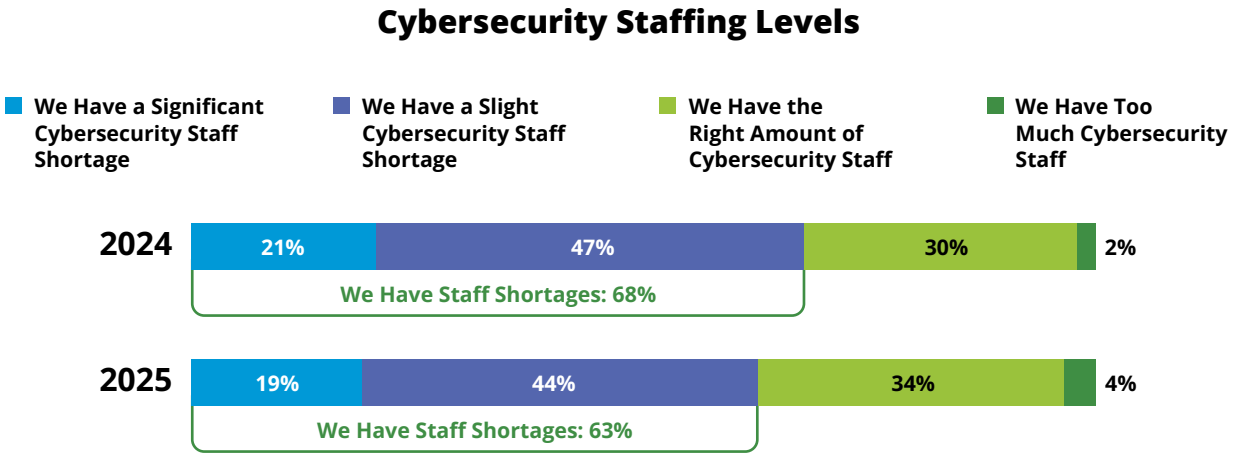
Dealing with the Effects of Cybersecurity Setbacks



Skills Shortages Eclipse the Impact of Staff Shortages Alone

The ability to operate an effective cybersecurity program is reliant on two primary assets: skills and qualified people. Traditionally, we have reported cybersecurity professionals' view that the shortage of qualified people in the field was the most prominent factor impacting their ability to effectively defend their organizations. This outlook seems to be evolving as respondents to the 2025 study have highlighted that the need for critical skills within the workforce is outweighing the need to increase headcount.

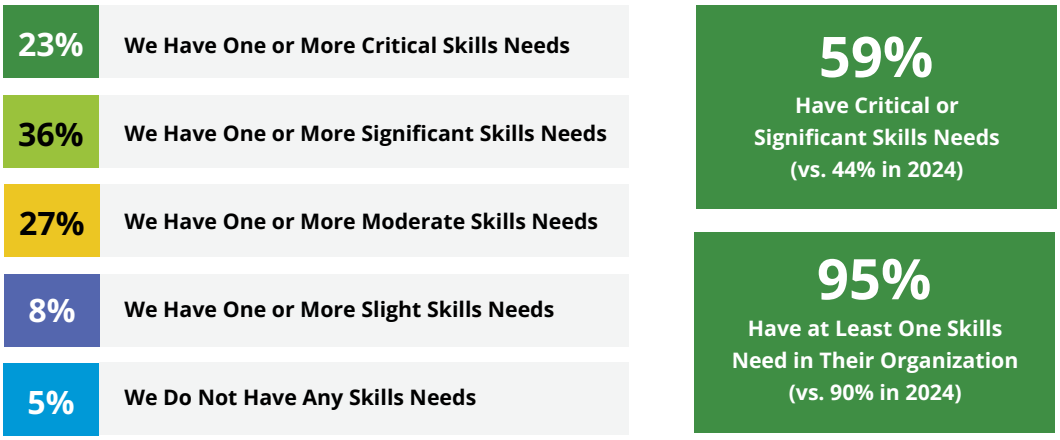
Contributing to this tipping point between skills growth and headcount growth is a modest improvement in the overall state of staffing levels compared to 2024. Those reporting significant shortages were down 2% year-on-year, with slight shortages down 3%. Encouragement comes from the fact that 4% more respondents (34%) in 2025 said they have the right level of cybersecurity staffing, a figure that has held at 30% since 2023. Only 4% believe their organizations have a surplus of staff across cybersecurity functions (separate from any measure of skills availability). However, it should be noted that this figure has doubled from both 2024 and 2023, where it sat at just 2%.



Despite these modest staffing level improvements, teams are struggling to develop or find the skills they need to address the jobs and tasks they are being asked to do. A lack of people and skills also inhibits existing professionals' abilities to adapt to the changing technology needs of the organization and the evolving threat landscape outside it.

Both technical and nontechnical skills are in short supply. Few respondents selected just one issue within their team. Further underscoring that skills, rather than headcount, was the critical factor this year, nearly two-thirds (59%) cited critical or significant skills needs this year, up from 44% in 2024, while 95% of respondents have at least one or more skills needs, also up 5% on the previous year. More specifically, nearly a quarter (23%) are grappling with one or more critical skills needs, while a further 36% face significant skills shortages. Only 5% of respondents believe their teams do not have any current skills needs.

Skills Needs are a Problem for Cybersecurity Teams



AI was the most pressing skills need (41%) cited by respondents, followed by cloud security (36%), maintaining their position as the 2024 top two needs. Risk assessment (29%), application security (28%), as well as security engineering and governance, risk and compliance (GRC) (both at 27%), represent the other top skills needed by security teams.

Respondents reported some skills to be in lower demand compared to last year. Zero trust, for example, was highlighted by 27% as a needed skill in 2024, but by only 24% this year. Digital forensics and incident response declined 3% year-on-year to 22%. Both were in the top five last year and are now holding lower positions. Quantum computing came in at the bottom of the list at 17%, illustrating that it has yet to become a mainstream or accessible technology for many organizations outside large enterprises and academia, lowering the criticality of the skills need around it.

Key Skills for Cloud Security

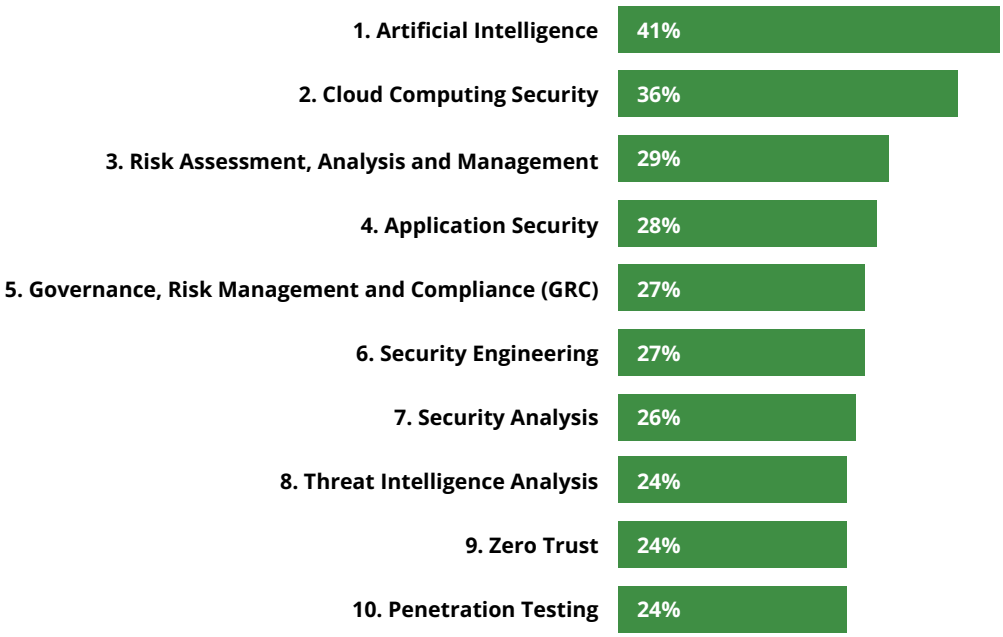
Cloud security has long existed as a major skills need for cybersecurity professionals and their employer organizations. The growing prominence of the cloud in the software supply chain has made cloud security an essential discipline within teams tasked with securing distributed assets, datasets and users.

Cloud architecture and secure design were called out by half of respondents focused on cloud skills (50%), underlining the critical role of design and implementation in successful and secure cloud deployments and operations. This was followed by cloud platform and infrastructure security (41%). Secure cloud deployment and configuration management (38%) is a highly topical response considering reports of several high-profile misconfiguration cloud issues in the last year that impacted both platform operators and their customers.

Identity and access management (IAM) is similarly a highly topical skills need (35%) in the face of several reported data breaches and network intrusions that came about due to lax access and authentication controls, especially further down the cloud supply chain.

Cloud data protection (34%) skills, particularly as they relate to encryption, obfuscation and tokenization, are seen as highly necessary given the volume of valuable and sensitive data residing outside core networks.

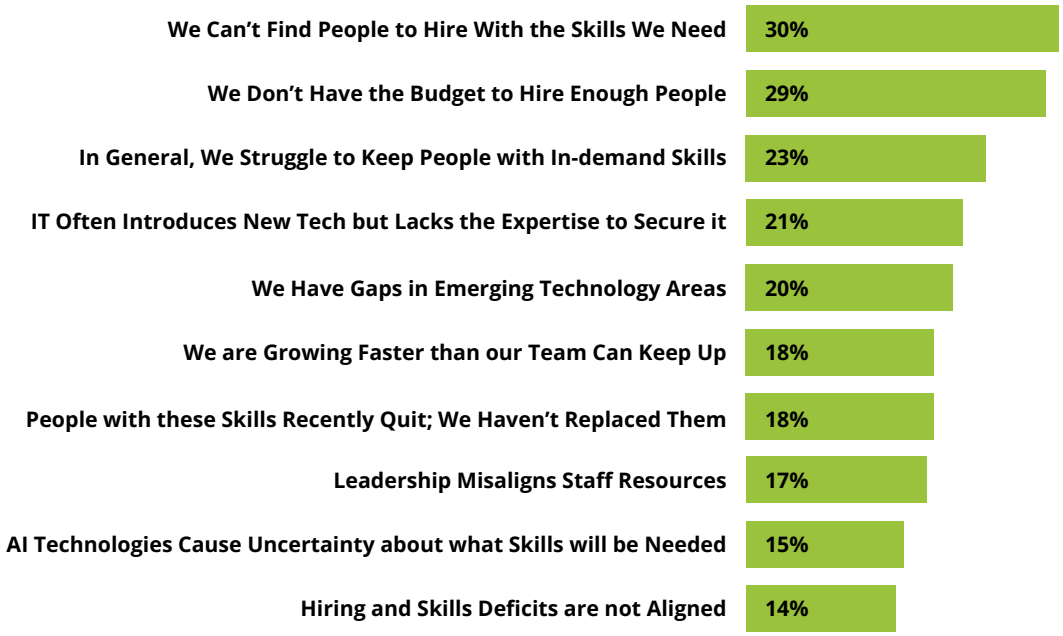
Top 10 Security Team Skills Needs



The primary drivers for skills shortages brought up two consistent themes: being unable to find people with the needed skills (30%) and not having the budget to hire enough people (29%). This was joined by 10% of respondents who noted their organizations can find the people with the skills they need, but they can't afford them. Budget pressures once again illustrate a direct impact on capability and readiness within cybersecurity teams.

Respondents also cite challenges retaining people with in-demand skills (23%) and IT driving the adoption of new technology before the organization can obtain the skills needed to fully secure it (21%).

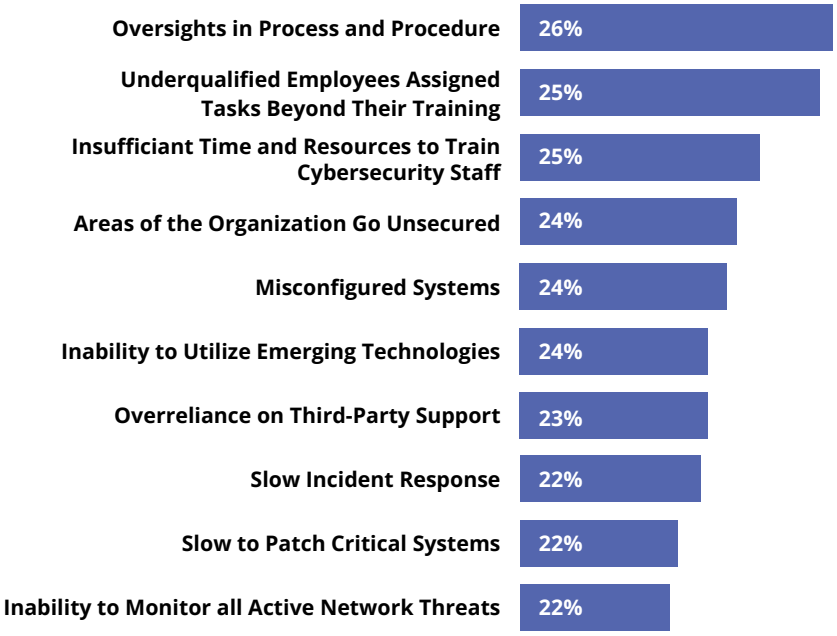
Top Causes of Skills Needs on Cybersecurity Teams



These skills shortages have had a range of consequences for respondents and their organizations. A little more than a quarter (26%) have experienced oversights in cybersecurity processes and procedures, while a quarter have also been forced to put underqualified or inexperienced people into roles to cover them. A quarter also noted that they did not have the time or resources to train cybersecurity staff. A similar number (24%) noted issues with misconfigured systems — a common and topical issue for organizations with several instances making global news in 2025. Another commonly cited (24%) outcome of skills shortages is that parts of the organization are left under-secured and staff are unable to take advantage of emerging cybersecurity technologies (24% each).

Overall, 88% of respondents have experienced at least one significant cybersecurity consequence because of a skills deficiency within the team or wider organization, with 69% experiencing more than one.

Consequences of Security Team Skills Needs



88%
Reported Experiencing at Least One Consequence Due to Skills Needs

18%
Reported Experiencing One of These Consequences

69%
Reported Experiencing More Than One of These Consequences

Key Skills for Zero Trust

While zero trust has dropped as a priority in 2025 compared to the findings from the 2024 study, it remains a clear focus area for respondents and interlinks with both cloud and AI in a number of shared discipline areas.

Designing zero trust architectures (59%) was by far the primary focus for respondents that are focused on zero trust skills, followed by least privilege access control implementation (33%) and identity-centric security (30%), both broadly in line with the IAM focus of those with cloud skills specialization in mind.

Zero trust governance (30%) also echoes the skills focus of AI specialists, with both recognizing the organizational importance of governance and policy competencies when delivering functional and secure system deployments.

Technical network management skills such as network isolation and segmentation techniques (28%), along with continuous authentication and authorization (26%), round out the most pressing skills concerns for those charged with delivering a viable zero trust architecture and environment for their organizations.

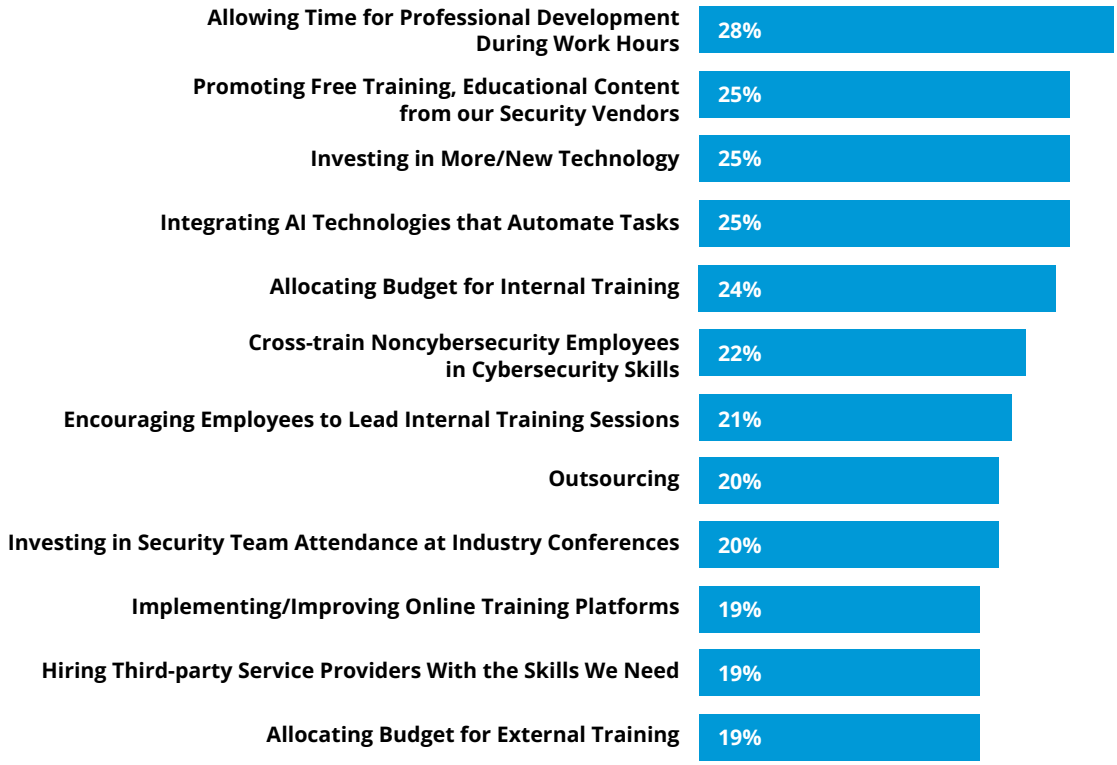
To upskill their workforce, respondents noted that their organizations are leveraging a variety of solutions and approaches to address or mitigate skills deficiencies:

- **Cybersecurity Team Development:** 28% of respondents said their organizations are allowing time for staff to undertake professional development during working hours. A quarter (25%) are encouraging the use of free training and educational content provided by security vendors, while 24% are allocating budget to deliver internal training and 21% are encouraging employees to host internal training sessions and knowledge sharing to educate and help others develop their skills.

- **Mitigation Measures:** 25% said they are investing in more and new technology, with 25% also turning to AI and automation, to mitigate the shortage of cybersecurity skills. More than a fifth (22%) reported that their organizations are cross-training employees from outside the established cybersecurity team to develop specific skills and competencies to offset shortages.

- **External Support:** Several external tactics are being used to offset skills shortages, including outsourcing work (20%), bringing in third-party service providers (19%) and hiring temporary contractors (17%) to fill the need.

How Organizations Address Cybersecurity Team Skills Needs



Skills Prioritization Highlights a Disconnect in the Workforce

While security teams align on skills needs, there is a disconnect between the skills cybersecurity managers are looking for when hiring and the skills that professionals view as in-demand. These differences surfaced in our 2024 research as well.

In terms of technical skills, hiring managers identified cloud security (29%), AI (27%), security engineering (24%), security analysis (23%) and risk assessment (23%) as the skills they are prioritizing when hiring. Professionals were aligned with hiring managers that AI (44%), cloud security (40%), and risk assessment (26%) are skills in high demand, but they also view GRC (30%) and zero trust implementation (27%) as priority skills areas. The technical areas seen as lacking this year are similar to those cited in 2024, suggesting that technical skills needs have not eased or improved year-on-year.

Technical Skills Valued by Hiring Managers vs. Cybersecurity Professionals

Skills:	Hiring Managers Are Looking For:	Professionals View As In Demand:
Cloud Computing Security	29%	40%
Artificial Intelligence/Machine Learning	27%	44%
Security Engineering	24%	20%
Risk Assessment, Analysis, and Mgmt.	23%	26%
Security Analysis	23%	17%
GRC	21%	30%
Application Security	20%	20%
Security Administration	19%	13%
Secops	18%	19%
Zero Trust Implementation	17%	27%
Identity and Access Management	16%	20%
Threat Intelligence Analysis	16%	18%
Network Monitoring	15%	10%
Operation Technology Security (ICS)	15%	10%

Hiring managers and professional participants are more aligned on the nontechnical skills needed in the workforce. Both identified problem-solving, teamwork/collaboration and communication skills as the top three skills needs. However, professionals view strong communication skills as the top in-demand skill (59%) whereas hiring managers ranked it third (48%) on their list of skills they are prioritizing when hiring.

Nontechnical Skills Valued by Hiring Managers vs. Cybersecurity Professionals

Skills:	Hiring Managers Are Looking For:	Professionals View As In Demand:
Strong Problem-Solving Skills	54%	55%
Teamwork and Collaboration Skills	51%	50%
Strong Communication Skills	48%	59%
Curiosity/Eager to Learn	40%	44%
Strong Strategic Thinking Skills	37%	39%
Time Mgmt and Organization	31%	29%
Strong Project Mgmt Skills	28%	28%
Emotional Intelligence	25%	25%
Leadership Abilities	24%	29%
Conflict Resolution Skills	20%	23%
Talent/Personnel Evaluation Skills	17%	11%

Cybersecurity professionals need strong technical skills to perform in their roles, but we have seen nontechnical skills becoming just as important over the past several years, even before AI-driven automation began impacting the profession. When looking at both technical and nontechnical skillsets together, hiring managers and professionals aligned in ranking some nontechnical skills higher than technical skills, but differences surfaced in technical skills prioritization.

The top five skills hiring managers are looking for were all nontechnical skills with problem solving (29%), collaboration (24%), communications (22%), willingness to learn (20%), and strategic thinking skills (16%). Professionals agreed that nontechnical skills such as strong problem-solving (28%) and communication (29%) are needed in the workforce, but they also recognize the value of practical technical skills, ranking AI and cloud security in the top four skills they view as in-demand. Results from our 2024 research were similar both in terms of hiring managers prioritizing nontechnical skills and professionals viewing AI and cloud security as equally important.

Nontechnical/Technical Skills Valued by Hiring Managers vs. Cybersecurity Professionals

Skills:	Hiring Managers Are Looking For:	Professionals View as In Demand:
Strong Problem-Solving Skills	29%	28%
Teamwork and Collaboration Skills	24%	20%
Strong Communication Skills	22%	29%
Curiosity/Eager to Learn	20%	19%
Strong Strategic Thinking Skills	16%	17%
AI/ML	15%	28%
Cloud Computing Security	15%	22%
Security Engineering	12%	8%
Time Management and Organization	11%	9%
Risk Assessment, Analysis And Mgmt	11%	13%
GRC	11%	15%
Strong Project Mgmt Skills	11%	11%
Security Analysis	10%	7%
Leadership Abilities	10%	12%
Emotional Intelligence	10%	8%

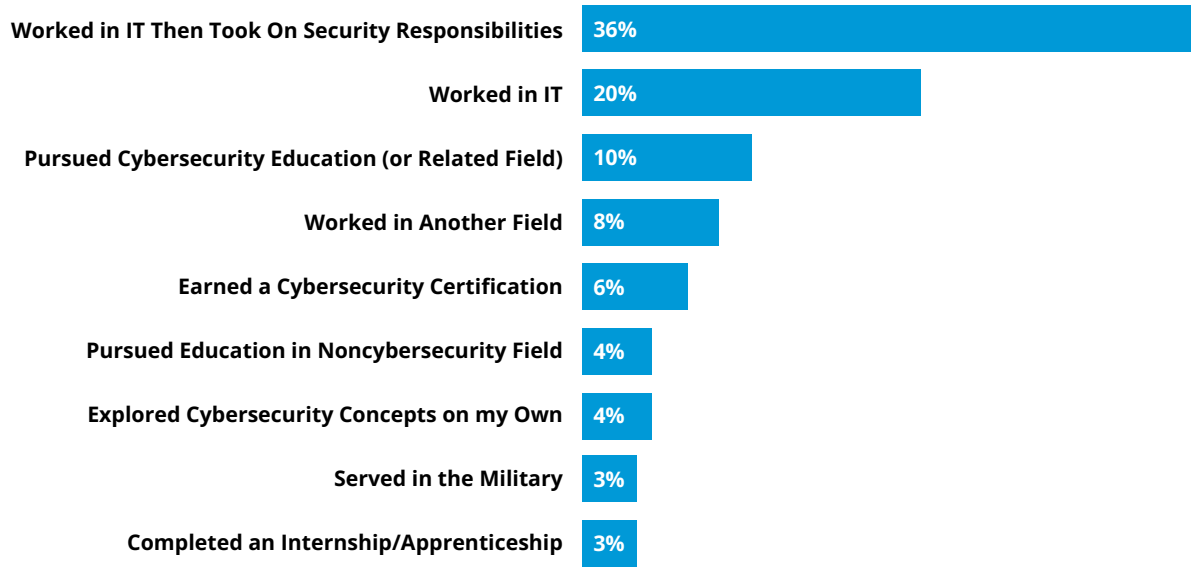
Many of the top skills valued by both cybersecurity hiring managers and professionals are nontechnical

Is Cybersecurity Still Closely Tied to IT?

As we've seen with previous iterations of this study, IT experience is still the primary pathway into a cybersecurity role, with 56% reporting this was their experience. There are nuances to how that transition happened, however, with 36% of respondents reporting that they took on cybersecurity responsibilities while in an IT role before moving into a cyber-focused role. Meanwhile, 20% moved directly from IT into cybersecurity without an interim step.

Education in cybersecurity is the third most frequently cited pathway as noted by 10% of participants — with the remainder entering through non-IT professional experience (8%), earning cybersecurity certifications (6%), exploring cybersecurity concepts on their own (4%), military backgrounds (3%) and internships or apprenticeships (3%).

Pathways Into Cybersecurity Careers



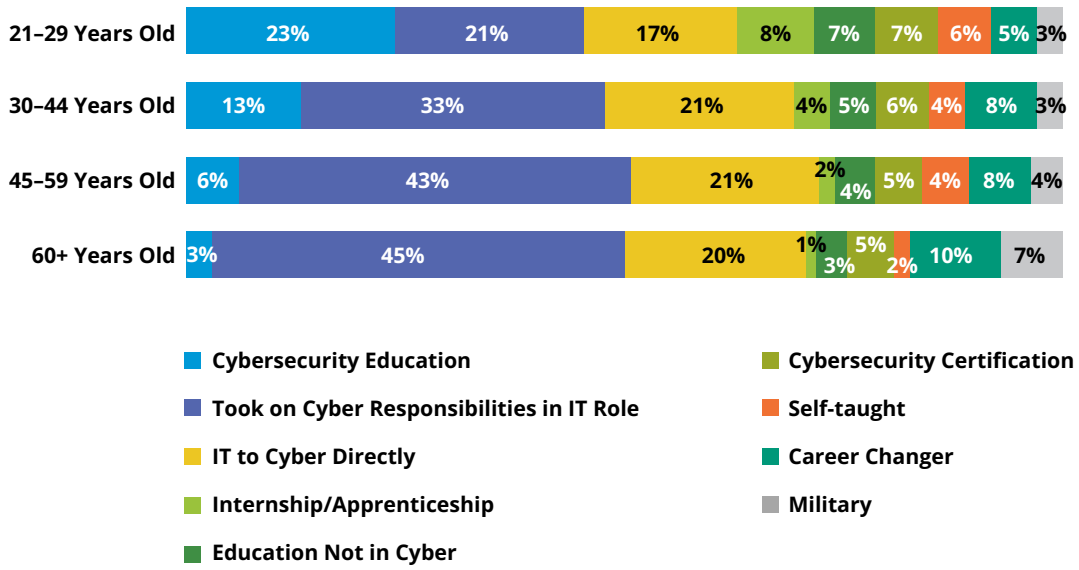
Where we see a shift in IT as the dominant pathway is among those under 30 years of age. While 38% of participants age 21–29 entered through an IT pathway, an equal percentage (38%) entered through means other than IT or cybersecurity education (e.g., career changers, certification, self-taught,

military, internship/apprenticeship, etc.), with 23% entering by completing a cybersecurity degree program. The highest career-changer figures were among those moving into the field from the legal, real estate, retail/wholesale and construction industries, but the proportion was less than 10% for each of them.

Within the 38% that entered through routes other than IT or cybersecurity education, the pathways are more diverse — they have higher rates of entrance through internship/apprenticeship programs (8%), degree programs outside cybersecurity (7%) and cybersecurity certifications (7%) compared to their older cohorts.

As participant age increases, so does the percentage of those entering through IT pathways — from 54% in the 30- to 44-year-old age category to around 65% of those over age 45 (64% for age 45–59, 65% for 60+).

Pathways Into Cybersecurity, by Age

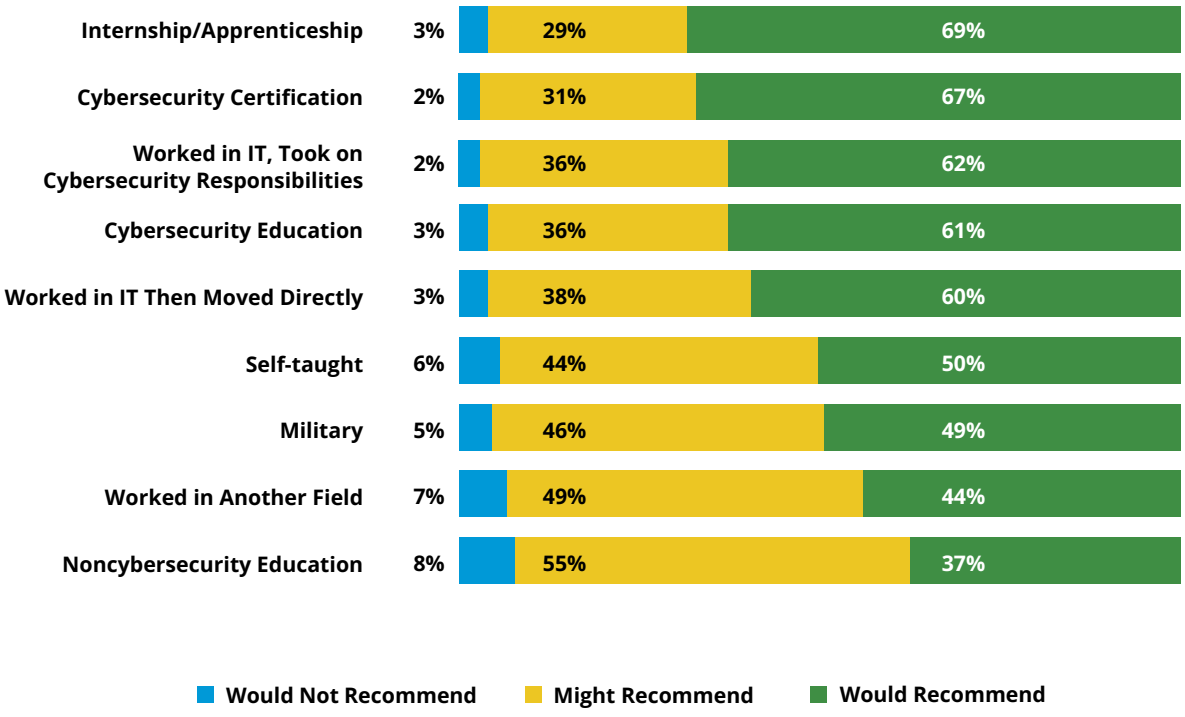


Most participants felt that their pathway into a cybersecurity role was the right one — 57% said they would recommend their pathway to others, while 39% said they may or may not; only 4% said they would not recommend their pathway. That high percentage of self-path IT recommendation is

potentially creating a feedback loop that is helping to maintain IT's high feed level into the cybersecurity field.

Not surprisingly, those who secured a cybersecurity role via an internship or apprenticeship (which only 3% of participants experienced) had the highest rate (69%) of recommending that pathway to others. Other highly recommended pathways were cybersecurity certifications (67%), IT (60–62%) and cybersecurity education (61%). Those with lower levels of practical experience (i.e., career changers or education in a field unrelated to cybersecurity) had the lowest likelihood to recommend their pathways to others.

Do Cybersecurity Professionals Recommend Their Career Pathway to Others?

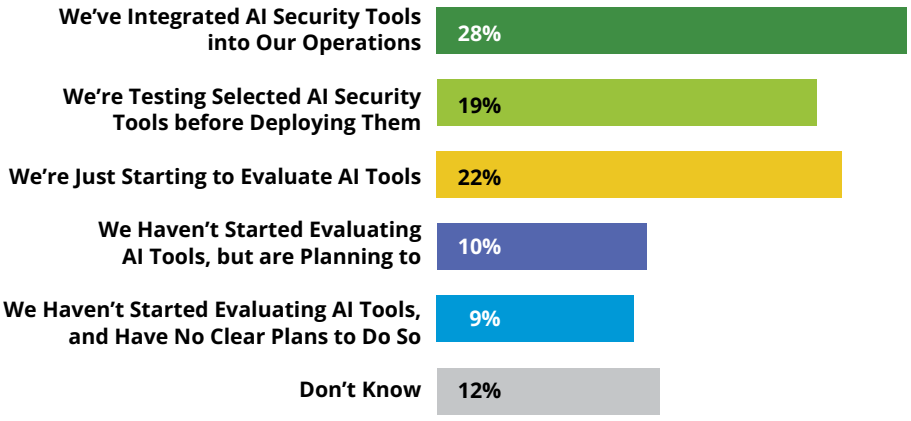


AI Is Creating Opportunities for Cybersecurity Professionals

Cybersecurity teams are frequently finding themselves stretched thin due to limited budgets and resources, making it harder to deal with rising volumes of alerts, logs and other high-volume, time-intensive monitoring and investigative activities. AI-driven tools offer the promise of alleviating this burden by automating repetitive tasks such as monitoring network traffic, identifying anomalies and flagging suspicious behavior. However, the adoption of AI tools carries implications for existing cybersecurity professionals, both those tasked to manage and use these systems and those who find their existing roles reshaped by their use.

Adoption is progressing, with 28% of respondents having already integrated AI tools into their operations, with a further 19% actively testing them and another 22% in the early evaluation phase. In total, more than two-thirds of respondents (69%) are on a path toward regular AI security tool use. The majority of cybersecurity teams that are currently working with AI security tools report positive

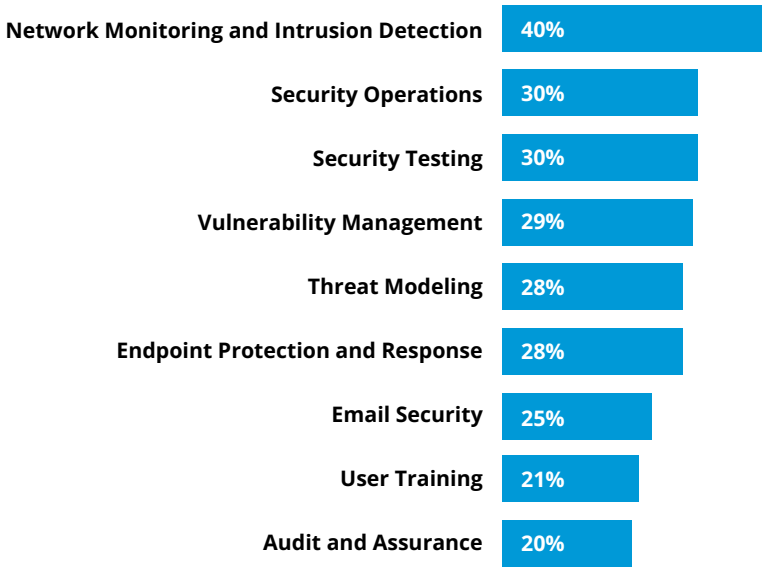
Cybersecurity Team AI Security Tools Adoption Rates



experiences, with 63% stating they are enjoying a significant boost to their productivity. In contrast, only 21% of active AI security tool users said the technology was not having a meaningful impact on their productivity, with 12% saying it was too early to call and just 3% saying it was having no impact at all.

In terms of where AI is expected to have the most impact on cybersecurity operations in the shortest amount of time, 40% pointed toward network monitoring for the highest positive impact, followed by security operations and security testing (both at 30%), vulnerability management (29%), threat modeling and endpoint protection (both at 28%). What's notable about all these areas is that they are time- and resource-intensive, generating large amounts of information that needs to be processed and examined. These areas are also ideal territory for automation.

Where AI Security Tools Will Improve Efficiencies the Fastest



Contrary to **some research reports**, AI is seen by respondents as a catalyst for career development opportunities rather than a threat. Far from reducing cybersecurity functions, participants believe AI will create the need for new types of roles, as 73% said AI will create more specialized cybersecurity

skills. Furthermore, 72% said that AI would create a need for more strategic cybersecurity mindsets. AI will generate a need for broader skillsets across the field, said 66% of respondents, while 66% agreed that technical roles will also be needed. More communications roles and skills will also appear, according to 65% of respondents, as AI adoption grows.

The use of AI tools and the perception that AI will be a career-booster within the cybersecurity field are prompting professionals to take proactive steps to develop and grow their knowledge and skills base to future-proof their careers.

In terms of AI-focused skills development, 48% of respondents are already working to gain more generalized AI knowledge and skills, while others are educating themselves on AI solutions risk to better understand vulnerabilities and exploits (35%) and how to audit the security and integrity of AI systems (22%). Some are considering a more strategic approach in their acquisition of AI skills by positioning themselves as early AI adopters within their organization (26%). Some are evaluating AI solutions that benefit their organizations by identifying and proposing new applications for AI to improve profitability or efficiency (25%) or improve their organizations' defense (24%). Some (17%) have already obtained AI-focused qualifications to demonstrate these skills, while many (53%) have plans to obtain them in the near future.

More than half (57%) of participants are also staying current by continually building their overall cybersecurity knowledge. Some (37%) are also trying to gain strategic skills to build upon their tactical skills. While AI is challenging some cybersecurity skills and roles, it is not causing many professionals (18%) to actively consider changing careers, but some are obtaining new degrees (16%).

AI-based attacks represent new threat vectors and risks that most cybersecurity professionals had not encountered in their careers until the last few years. Taking on an AI-centric professional mindset appears to be a necessary strategy in light of the growing threats AI poses. Both technical and human-based AI attacks have emerged in the past 12 months, with 40% of respondents experiencing AI-optimized social engineering attacks, 25% reporting data leakage, 23% seeing suspected AI-powered cyberattacks and another 23% experiencing AI-related data breaches. Data and AI infrastructure are also popular targets, with 11% of respondents encountering data poisoning and another 9% experiencing model theft attacks on their own AI architecture.

Key Skills for AI

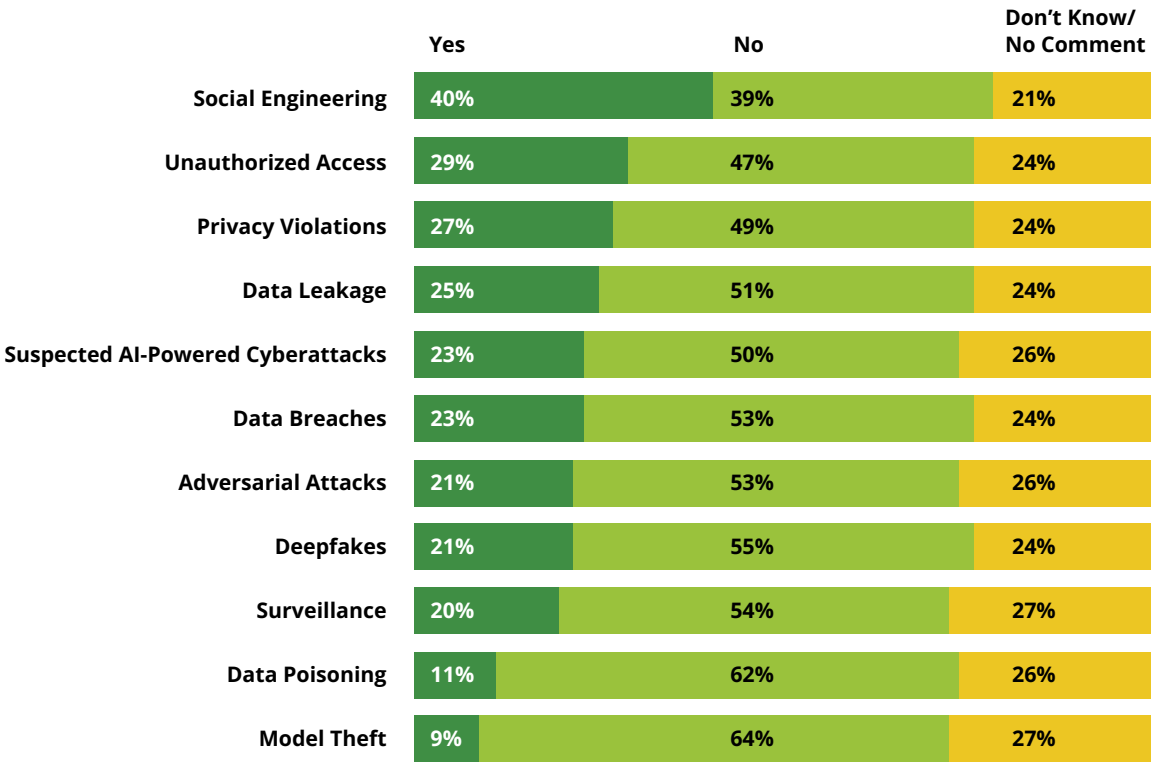
With AI considered to be an area of critical skills deficiency, respondents were asked to highlight the key AI/ML competencies they believe cybersecurity professionals need to advance.

The ability to use AI in threat detection and response was the most highly rated AI-specific skill, cited by 42% of respondents, followed by AI in threat modeling and risk assessment (39%).

Infrastructure and policy ranked very high, underlining the importance of defending the actual AI systems alongside using AI as part of a wider cybersecurity tool set. Defending AI models from attack was considered important by more than a third (35%), with securing AI integrations in cloud and edge deployments (31%) followed by AI governance and policy implementation (30%).

Data integrity and privacy in AI (30%) and AI regulatory compliance (29%) — itself a young and rapidly changing space — also ranked very highly with cybersecurity professionals focused on AI skills.

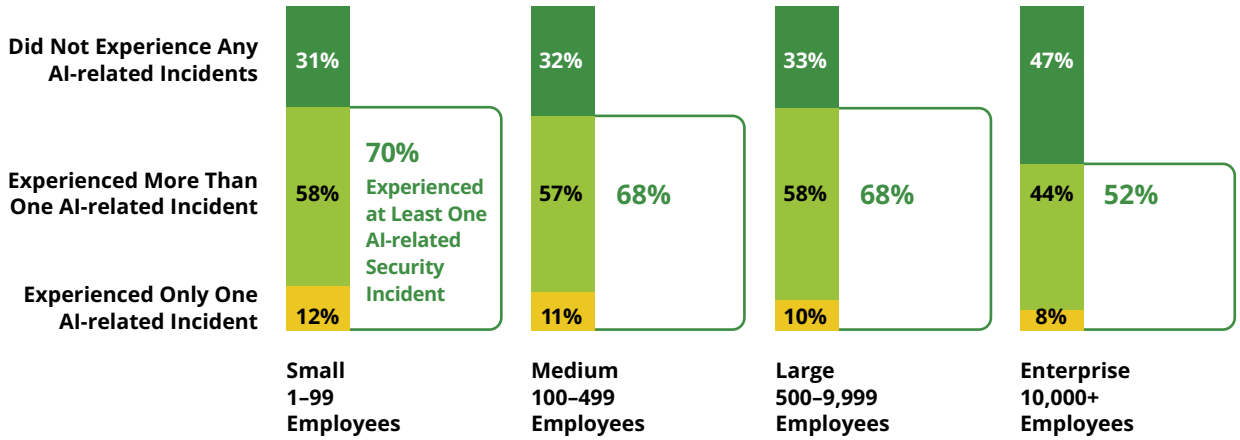
AI-related Security Events Experienced by Cybersecurity Professionals in the Past Year



Participants working at small organizations reported the highest rates of experiencing AI-related security events — with 70% having experienced at least one of the AI-related events included in the survey — and most (58%) have experienced more than one type of AI-driven security incident in the past year.

In contrast, 52% of those working at enterprise-size organizations reported experiencing at least one AI-related security event in their role, again with the majority of them (44%) reporting more than one incident.

Number of AI-related Security Incidents Experienced In the Past 12 Months by Organization Size

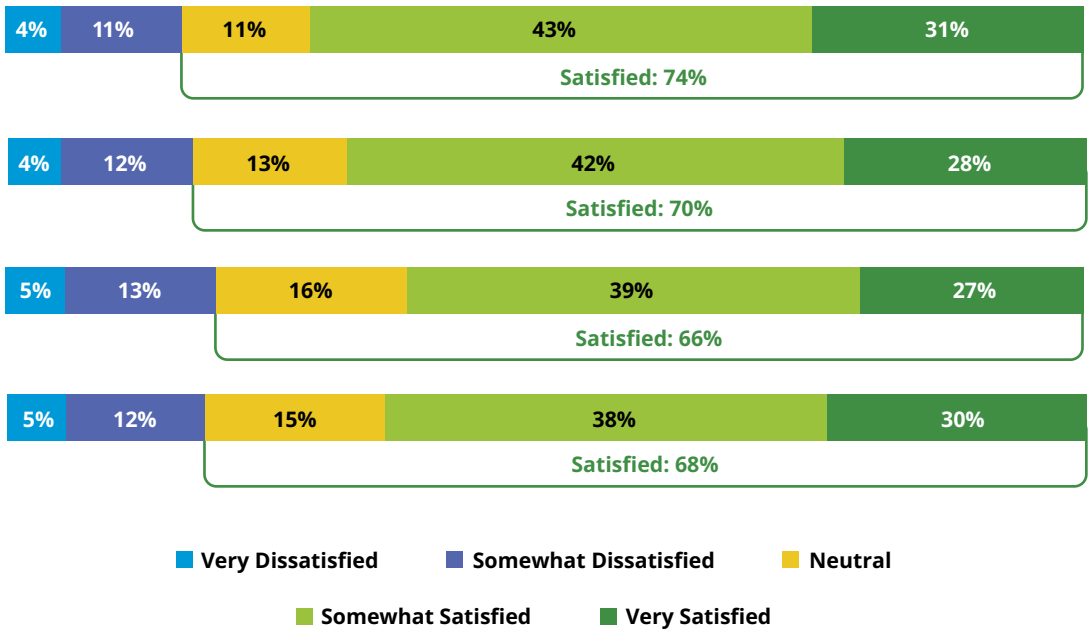


Job Satisfaction is Enduring Despite Significant Pressure

Economic challenges, wider AI adoption and a consequential shortage of essential skills and talent all have an impact on job satisfaction and wellbeing in the cybersecurity workforce. Even with the disruptive and challenging factors that have impacted cybersecurity professionals, they remain relatively positive and fulfilled in their career choice. However, there are some things employers should consider for long-term planning.

Overall, 68% of participants reported being satisfied in their current job, a 2% increase from 2024. This is a positive indicator as there was a significant 4% decline in overall job satisfaction from 2023 to 2024. Among those who are satisfied, there was also a 3% increase year-on-year in respondents who were "very satisfied" (from 27% in 2024 to 30% in 2025).

Overall Job Satisfaction Over the Years



Satisfaction varies by the layers of engagement in a position, with respondent satisfaction highest in relation to their teams (78% satisfied) and direct managers (73% satisfied). It declines when participants evaluate their satisfaction with their organization (71% satisfied) and further with the leadership of their organization (63% satisfied). Regardless of how participants feel about where they work, most (80%) reported that they feel passionate about the work they do, while 71% are satisfied with their day-to-day work experience.

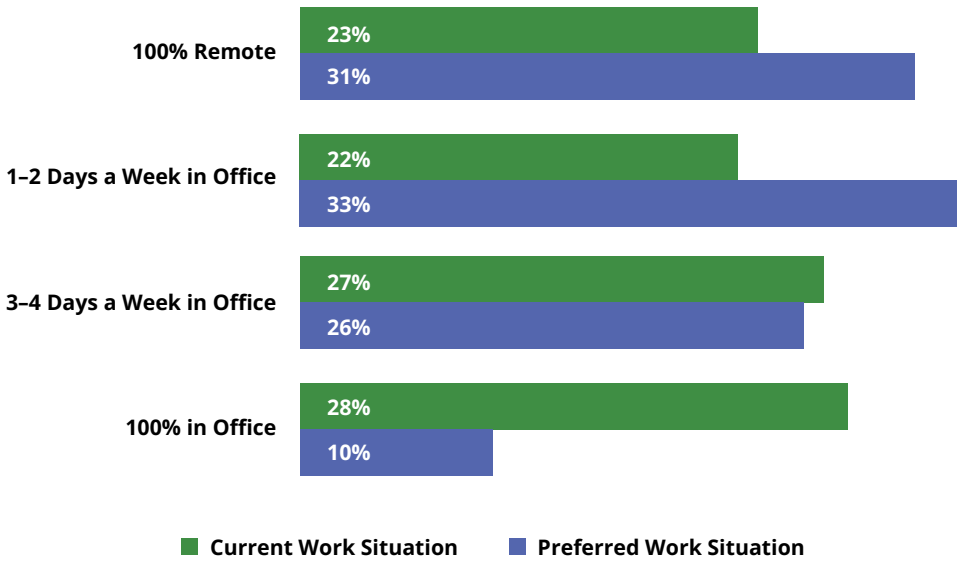
While there is room for organizational improvement, most (90%) participants reported that their organizations are doing things to address skills deficiencies and needs. Many of the efforts that participants value focus on upskilling. Allocating budget for professional development (35%) was the most common, followed by investing in organizationwide security awareness training (24%) and providing cross-training opportunities to learn new skills (24%). Only 32% said their organizations prioritized cybersecurity as a critical business function.

Many actions that drive engagement were focused on workplace culture and employee value, such as listening to and acting upon advice from employees (30%), celebrating individual and organizational successes (29%) and creating an inclusive environment (29%). Nearly a third (31%) of participants view opportunities for career growth, advancement and receiving unplanned financial or benefit rewards (e.g., spot bonus for performance, extra paid day off, etc.) as important drivers of their engagement. Lastly, the most valued offering is flexible working arrangements, which 42% of participants said their organizations offered.

Things Organizations Are Doing That Make Cybersecurity Professionals Feel Engaged

Knowing that many organizations have shifted from fully remote to either hybrid or full-time in office once the COVID-19 pandemic eased, respondents were asked how they are currently working and what their preferred work situation is. It revealed an obvious disconnect —with 23% working fully remote yet 31% preferring it. Meanwhile, 28% are working full-time in office while only 10% would choose to do this. The most common work environment is hybrid, with 22% reporting they work in an office 1–2 days a week and 27% working 3–4 days. In terms of hybrid preferences, 33% would prefer 1–2 days in office and 26% prefer 3–4 days.

Cybersecurity Professionals' Current vs. Preferred Work Situations



Unsurprisingly, those whose current and preferred work situations aligned reported higher levels of job satisfaction. Satisfaction was highest (75% satisfied) for those working full-time in office when full-time in office was their preferred situation. Results were similar when those working fully remote aligned (74% satisfied). Conversely, mismatches in preferences lead to greater job dissatisfaction, particularly among those working in office more than they would prefer to. Those currently working in office full-time yet preferring to be fully remote reported the lowest job satisfaction (43% satisfied).

Participants reported several other factors that cause them to be dissatisfied with their roles. Staffing and skills shortages, a recurring theme throughout this research, were behind some of the most frequently mentioned issues. Almost a third (32%) reported feeling overworked due to these shortages, and 20% said they were expected to work long hours. These shortages also impact organizational security — 28% reported they do not have enough time to stay current on security issues, 23% don't have adequate training opportunities and 22% even reported that they are expected to cover security responsibilities outside their area of expertise.

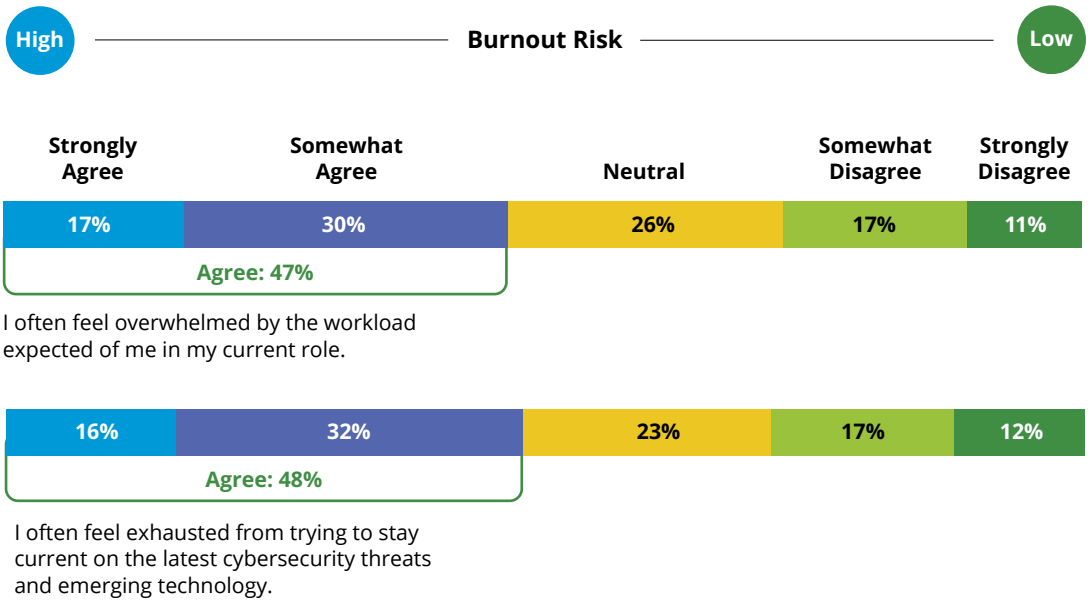
Other systemic factors such as a lack of opportunity for career growth and advancement, reported by 32% of respondents, along with insufficient pay (31%), were among the most frequently mentioned issues impacting their job satisfaction.

While cybersecurity jobs have been viewed as high-paying, 20% of participants said they received no salary increase over the past year, with the majority (57%) receiving a salary increase ranging from 1–9%. Only 20% experienced a pay increase of more than 10% from their previous year's salary. Organizational issues that lead to job dissatisfaction include leadership not prioritizing cybersecurity as a critical business function (23%) and a lack of flexible work arrangements (17%).

What Causes Job Dissatisfaction Amongst Cybersecurity Professionals?

Beyond these elements that impact job satisfaction, it's apparent that participants are experiencing job stress and burnout. Almost half (48%) reported feeling exhausted from trying to stay current on the latest cybersecurity threats and emerging technologies, and 47% said they often feel overwhelmed by the workload they're expected to bear.

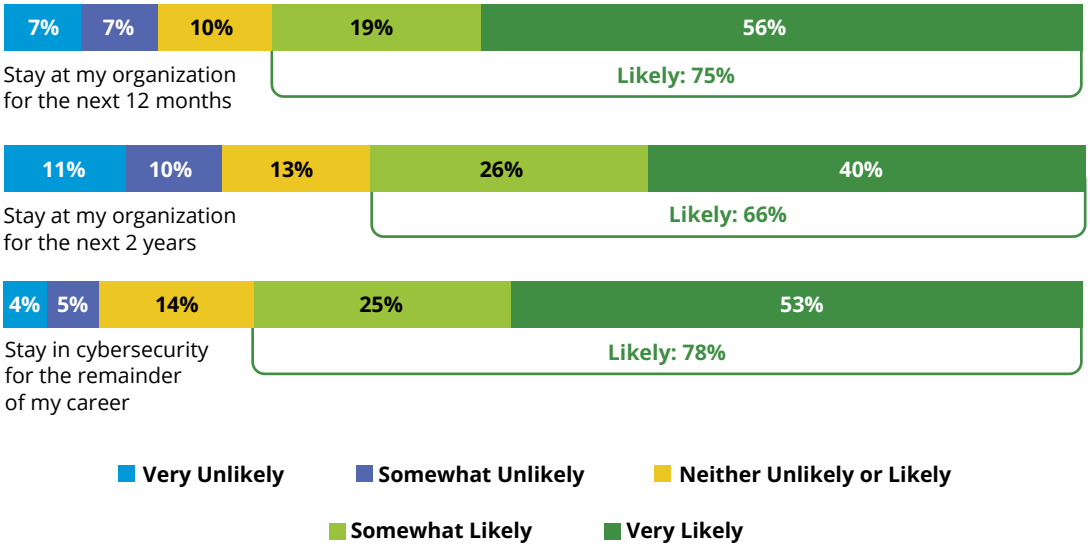
Burnout Risk Indicators: Workload and Cybersecurity Demands



There are some indicators that all these negative elements impact the outlook respondents have of their careers and the profession at large. Most still feel dedicated to the profession — 87% believe there will always be a need for cybersecurity professionals and 81% are confident the profession will remain strong.

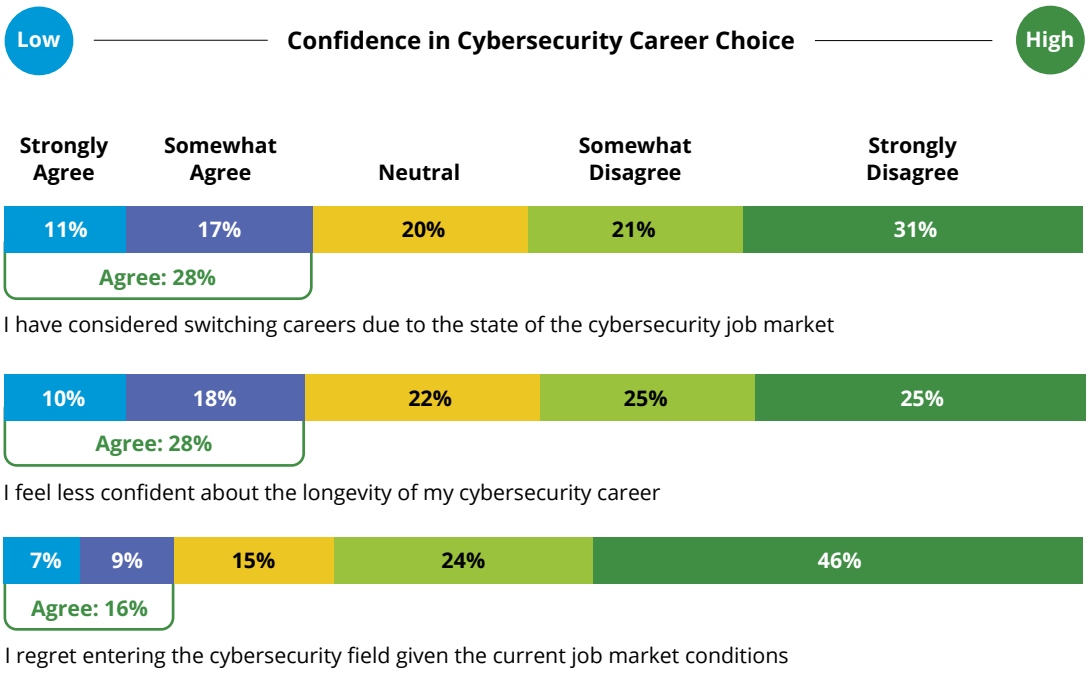
While 78% plan to stay in cybersecurity for the remainder of their careers, they feel less strongly about staying at their current organizations. Three-quarters (75%) reported they were likely to stay at their current organization for the next 12 months, but that percentage dropped to 66% when asked about their outlook over the next two years.

Projected Retention and Career Commitment



Some respondents do not seem to be as optimistic about their careers or cybersecurity as a profession. More than a quarter (28%) reported they feel less confident about the longevity of their career, and the same percentage have considered switching careers due to the state of the cybersecurity job market. While not a high percentage, 16% regret entering the cybersecurity field given current job market conditions. Yet, two-thirds (66%) would still recommend cybersecurity as a career to their children or other young people.

Some Express Doubts About Their Choice of a Career in Cybersecurity



The conflicting elements of job satisfaction serve as a signpost to cybersecurity and organization leaders that there is room for improvement. Strategies are required, based on these findings, to mitigate and address workplace pressures; otherwise, organizations may risk losing valuable skills and people. Listening to staff and aligning their priorities with the organizations' goals, as well as ensuring space within the company so they can learn and grow, will build loyalty and may help to ease burnout.

Conclusion

The findings of the 2025 ISC2 Cybersecurity Workforce Study highlight that cybersecurity teams are experiencing significant strain, brought about by economic pressure on budgets and staffing levels. Jobs and recruitment continue to be impacted, but it's the shortage of skills rather than just people that is the most pressing issue for a profession experiencing multiple disruptive factors. Despite these skills shortages and a rapidly evolving threat landscape, cybersecurity professionals remain positive about their career choices and prospects, even though some feel their current roles are not keeping them fully engaged. While AI introduces its own unique challenges, they remain optimistic about its overall impact too.

While the skills and knowledge needed to remain current may not be keeping pace, AI is seen as an opportunity among those using AI tools to enhance their job experience and ability to function, rather than being seen as a threat to their position. With AI set to drive significant changes to the tasks carried out by cybersecurity professionals, enabling training, development and knowledge sharing are critical to enable respondents to adapt to new needs and new ways of working.

Tackling these issues can be broken down into five critical recommendations for both cybersecurity leaders and hiring managers:

- **Keep Teams Motivated:** Find ways to invest in your cybersecurity personnel, even if budgetary constraints prevent you from promoting them or raising their salaries. Options cited as meaningful to cybersecurity professionals include providing flexible working opportunities, internal training, enabling cybersecurity professionals to be education leaders within the organization, providing allowances to visit technical conferences and benchmarking a budget for personal development such as certifications and courses. These are just a few cost-effective ways of motivating security teams to stay in their current roles or with their current organizations.

- **Invest in Your People and Their Skills:** Increasing skills competencies doesn't necessarily mean hiring more people. While increasing headcount may also be necessary, increasing the cybersecurity skills base within existing teams and across other members of the organization is an important and effective way of equipping the organization with skill sets to meet the needs of new and evolving technologies and working practices. Direct budget allocation for staff development is a key strategic action, with 35% of participants citing this as a way to keep them

engaged. Prioritizing professional development could be an effective way of upskilling your current workforce, rather than trying to hire one or more unicorn professionals with all the skills required.

- **The Future is AI:** The early signs remain positive that AI is enhancing the experience rather than being a downsizing tool. Employees see AI as a career opportunity to upskill and enhance their own professional growth, as 70% of study respondents have or are pursuing AI qualifications to remain relevant. Cybersecurity professionals are optimistic about the opportunities for career progression as a result of AI adoption, with 72% believing that AI will create the need for more strategic roles and skills in cybersecurity. Nearly two-thirds (65%) also suggest that AI use will require more communication roles and skills in cybersecurity, both opportunities for cybersecurity professionals to adapt their skills and knowledge in order to take on roles with increasing AI elements.

- **Have a Clear Leadership Strategy for Cybersecurity:** Recognize the value of cybersecurity professionals and ensure the organization is building or fostering a culture that emphasizes the importance of cybersecurity to all stakeholders, including the cybersecurity professionals themselves. While most cybersecurity professionals who participated in the study plan to stay in cybersecurity as their profession, they are far less committed to their current roles or for the longer term. Three-quarters (75%) said they were likely to stay where they are for the next 12 months, a figure that dropped to 66% when respondents considered the next two years. Leadership not prioritizing cybersecurity as a critical business function was identified as a driver of dissatisfaction in current roles. Prioritizing this is a clear way to bolster job satisfaction and retention.

- **Get Ready:** Only 55% agree their organizations have the resources to ensure preparedness in addressing security incidents in the next 2–3 years (with less than a quarter strongly agreeing with this sentiment). Ensure that any hiring freezes and restructuring of the cybersecurity team have not compromised their ability to protect and defend the organization and maintain operational resilience.

Ultimately, putting security employees' motivation and happiness at the center of companywide development will bring more staff loyalty and reliably secure employer organizations.

About the ISC2 Cybersecurity Workforce Study

ISC2 conducts in-depth research into the challenges and opportunities facing the cybersecurity profession. The ISC2 Cybersecurity Workforce Study is conducted annually to better understand the barriers facing the cybersecurity profession and uncover solutions that enable individuals to excel in their profession, achieve their career goals and better secure their organizations' critical assets.

Methodology

The 2025 ISC2 Cybersecurity Workforce Study is based on online survey data collected in May and June 2025 from 16,029 individuals responsible for cybersecurity at workplaces throughout North America; Latin America; the Asia-Pacific region; and Europe, the Middle East and Africa. Respondents in non-English-speaking countries completed a locally translated version of the survey.

Learn more at **www.isc2.org/research**.

Appendix: Participant Details

Industry

Industry	%
IT services	22%
Financial services	11%
Government	11%
Consulting	6%
Military	5%
Healthcare	5%
Manufacturing	4%
Telecommunications	4%
Security software/hardware development	3%
Education	3%
Retail/wholesale	3%
Energy/power/utilities	3%
Insurance	3%
Aerospace	2%
Engineering	2%
Automotive	2%
Transportation	2%
Entertainment/media/arts	1%
Construction	1%

Nonsecurity software/hardware development	1%
Food/beverage/hospitality/travel	1%
Hosted/cloud services	1%
Nonprofit	1%
Legal	1%
Real estate	1%
Agriculture	1%
Other	3%

Organization Size

Size (Number of employees)	**%**
1 (independent contractor/self-employed)	2%
2 to 4	1%
5 to 9	1%
10 to 19	2%
20 to 49	4%
50 to 99	5%
100 to 249	8%
250 to 499	9%
500 to 999	10%
1,000 to 2,499	11%
2,500 to 4,999	10%
5,000 to 9,999	9%

10,000 to 19,999	7%
20,000 or more	21%

Job Role

Role	%
Security Engineer	7%
IT Security Manager	6%
IT Manager	6%
Security Consultant/Advisor	6%
Security Analyst	5%
IT Director	5%
Security Architect	4%
CISO	4%
IT Security Director	4%
Security Specialist	3%
IT Specialist	3%
Information System Security Manager (ISSM)	3%
Project Manager	2%
Information System Security Officer (ISSO)	2%
Systems Engineer	2%
IT Auditor	2%
CIO	2%
Security/Compliance Officer	2%

CTO	2%
Software Developer/Engineer	2%
Network/System Administrator	1%
VP IT	1%
Network Engineer	1%
Systems Architect	1%

Type of Role

Type of Role	%
Internal security staff (I am primarily responsible for securing my organization's network as an employee or contractor)	62%
External security staff (I am primarily responsible for securing clients' networks; I work with an MSSP, service provider, external SOC, etc.)	12%
Security consultant (I advise clients on their security strategy)	19%
Other (specify)	7%

Respondent Level

Level	%
C-level executive	5%
Executive management	6%
Director/Middle manager	18%
Manager	22%
Nonmanagerial mid- or advanced-level staff	39%

Entry-junior-level staff	5%
Independent contractor/consultant	4%
Other (please specify)	1%

Hiring Authority

Hiring Authority	%
Yes, I make final decisions about hiring	20%
Yes, I am part of a team that makes hiring decisions	26%
I interview candidates and influence decisions but do not make final decisions	26%
No	28%

Employment Status

Employment Status	%
Employed/self-employed full-time	94%
Currently not working/Unemployed	3%
Employed/self-employed part-time	3%

Age

Age Group	%
24 or under	2%
25–29	6%
30–34	13%
35–39	16%

40-44	17%
45-49	15%
50-54	12%
55-59	7%
60-64	4%
65 or above	2%
Prefer not to say	6%

Gender

Gender	%
Female	16%
Male	78%
Nonbinary/gender nonconforming	0.4%
Prefer not to say	5%

Education

Education	%
High School Diploma (or equivalent)	4%
Two-year Associate Degree (or equivalent)	5%
Bachelor's Degree (or equivalent)	39%
Master's Degree (or equivalent)	42%
Doctorate (or equivalent)	6%
Other	1%
Prefer not to say	4%

Country

Country	%
United States (U.S.)	34%
Japan	8%
Canada	6%
United Kingdom (U.K.)	6%
China	4%
Australia	3%
Germany	3%
India	3%
Netherlands	3%
Singapore	3%
France	2%
Republic of Korea	2%
Spain	2%
Brazil	2%
Hong Kong	2%
Republic of Ireland	1%
Italy	1%
Mexico	1%
Nigeria	1%
Philippines	1%
Poland	1%
Saudi Arabia	1%

South Africa	1%
Switzerland	1%
Taiwan	1%
United Arab Emirates	1%

02/2026