ISACA

State of Cybersecurity 2025

Global Update on Workforce Efforts, Resources, and Cybersecurity Operations

Information Security

CONTENTS

4 **Executive Summary**

5 **Survey Methodology**

8 **Cybersecurity Workforce Challenges**
8 / Hiring and Open Roles
12 / Burnout and Retention
14 / Some Employer Benefits Decrease

17 **The Talent Pipeline**
17 / Future Workforce Concerns
18 / Skill Gaps

21 **Cybersecurity Operations**
21 / Budgets
21 / Boards and Cybersecurity Prioritization

24 **Cyberrisk and Cyberattacks**
27 / Cyberrisk Assessments

29 **AI and Cybersecurity**

31 **Conclusion: Preparing for an Uncertain Future**

32 **Acknowledgments**

ABSTRACT

State of Cybersecurity 2025: Global Update on Workforce Efforts, Resources, and Cybersecurity Operations reports the results of the annual ISACA® global *State of Cybersecurity Survey*, conducted in the second quarter of 2025. This survey report features trends in cybersecurity hiring, staffing, and budgets; cyberrisk and threats; cybersecurity operations; and the role of artificial intelligence (AI) in cybersecurity work. Although some findings are similar to previous years, some significant differences signal changes in cybersecurity operations and broader workforce trends.

Executive Summary

The eleventh annual ISACA® global *State of Cybersecurity Survey* explores challenges, trends, and opportunities within the cybersecurity field. This year's survey report presents insights on cybersecurity skills, hiring, and budgets; cyberrisk; and the role of artificial intelligence (AI) in cybersecurity.

Certain findings are consistent with last year's survey report; other survey findings indicate changes in the way that cybersecurity professionals work. Like in 2024, respondents to this year's survey have concerns about cybersecurity budgets, which are likely a reflection of broader market uncertainty.

Key findings include:

- Adaptability is the most important factor in determining a cybersecurity applicant's qualifications. Sixty-one percent of respondents indicate that adaptability is very important. Prior hands-on experience drops from first place last year to second place, with 60% of respondents indicating that prior cybersecurity work experience is very important. The importance of this factor is a considerable decline from last year, when 73% of respondents said it was very important.
- Last year, for the first time in the history of this survey, the percentage of respondents between the ages of 45 and 54 overtook the percentage of respondents in the 35 to 44 age group, and this trend continues this year. The aging cybersecurity workforce has expanded slightly among survey respondents. The largest percentage of survey respondents are between the ages of 45 and 54 (35%, which is one point higher than last year). This survey finding, when combined with a slight decline (one point) in the percentage of respondents who are ages 34 and below, is cause for concern. Further evidence of an aging workforce is the survey finding that less than half of respondents manage staff with less than three years of work experience. As these experienced cybersecurity workers approach retirement age, enough cybersecurity talent with managerial experience might not be available to replace retiring managers. Enterprises should begin to consider succession planning now to anticipate and address potential hiring challenges.
- Optimism about cybersecurity budgets growing is somewhat less compared to last year. Only 41% of respondents believe that their cybersecurity budgets will increase in the next 12 months, compared to last year, when 47% of respondents believed that budgets would increase. Eighteen percent of survey respondents believe that their cybersecurity budgets will decrease in the next 12 months, compared to 13% last year.
- Cybersecurity roles remain stressful. Sixty-six percent of respondents indicate that their roles are significantly or slightly more stressful now than five years ago. Survey respondents say that the main reason for this stress is the increasingly complex threat landscape. Although the complexity of the threat landscape was also the top stressor last year, fewer respondents identify it as a challenge this year (63% in 2025 compared to 81% in 2024).

Cybersecurity roles remain stressful. Sixty-six percent of respondents indicate that their roles are significantly or slightly more stressful now than five years ago.

- Soft skills are the largest skill gap among cybersecurity professionals, increasing from 51% in 2024 to 59% in 2025. Survey respondents report that critical thinking (57%); communication, which includes listening, speaking, and conflict resolution (56%); and problem solving (47%) are the top-three most important soft skills that security professionals need today.

- Half of the respondent enterprises have challenges retaining qualified cybersecurity professionals—the lowest percentage of retention challenges since 2020. High work-stress levels, limited promotion and development opportunities, and recruitment by other enterprises are the top reasons cybersecurity professionals are leaving their current roles.
- This year, the top employer-provided benefit shifts to professional development training. Employer-paid employee certification fees drop to the second most common benefit. Only 54% of respondents say that it is an employer benefit, a decrease from 65% in 2024. Professional development training is the most common employer benefit at 60%, three percentage points higher than last year.
- Enterprise efforts to address technical cybersecurity skill gaps drop considerably this year. Last year, 41% of respondent enterprises provided training to allow nonsecurity staff to move into security roles; this year, that percentage drops to just 29%. The top method to address technical skill gaps is increasing usage of contract employees or outside consultants. But even this is a decline from last year: 30% of respondents indicate their enterprise has increased reliance on contractors or consultants this year, compared to 36% last year.

Enterprise efforts to address technical cybersecurity skill gaps drop considerably this year. The top method to address technical skill gaps is increasing usage of contract employees or outside consultants.

- The use of AI has increased for a variety of security-related operations, including automating threat detection/response, endpoint security, and automating routine security tasks. Security professionals are not only increasing their use of AI tools, but also are more likely to be involved with shaping how their enterprise uses AI. Compared to 2024, more security professionals are involved in the development, onboarding, or implementation of AI solutions and the development of a policy governing the use of AI technology.

Survey Methodology

In the second quarter of 2025, ISACA sent online survey invitations to a global population of cybersecurity professionals who hold the ISACA Certified Information Security Manager® (CISM®) certification or have registered job titles in the information security field and are ISACA members.

The survey contains questions across the following areas:

- Staffing and skills
- Artificial intelligence
- Cybersecurity budgets
- Cyberthreats
- Cyberrisk
- Organizational structure/boards of directors

A total of 3,812 respondents completed the survey in its entirety, and their responses are included in this survey report. The survey has a margin of error of +/- 2 points at a 95% confidence level. Survey data was collected anonymously, and response rates vary by question.

Forty-six percent of the 3,812 respondents indicate that cybersecurity is their primary professional area of responsibility. **Figure 1** shows demographic information about the respondents. **Figure 2** features the industries that are represented by survey respondents.

FIGURE 1: Respondent Demographics

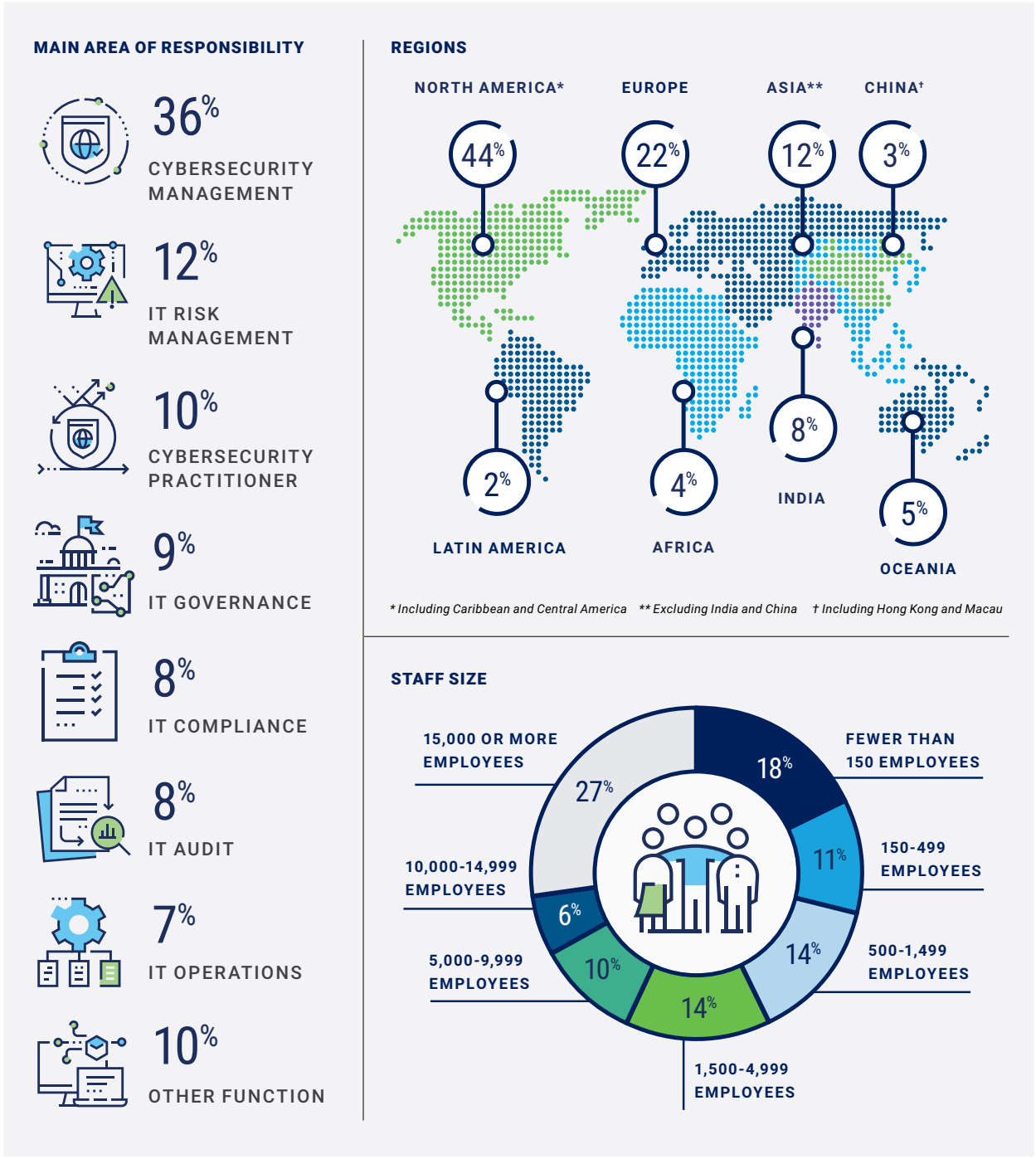
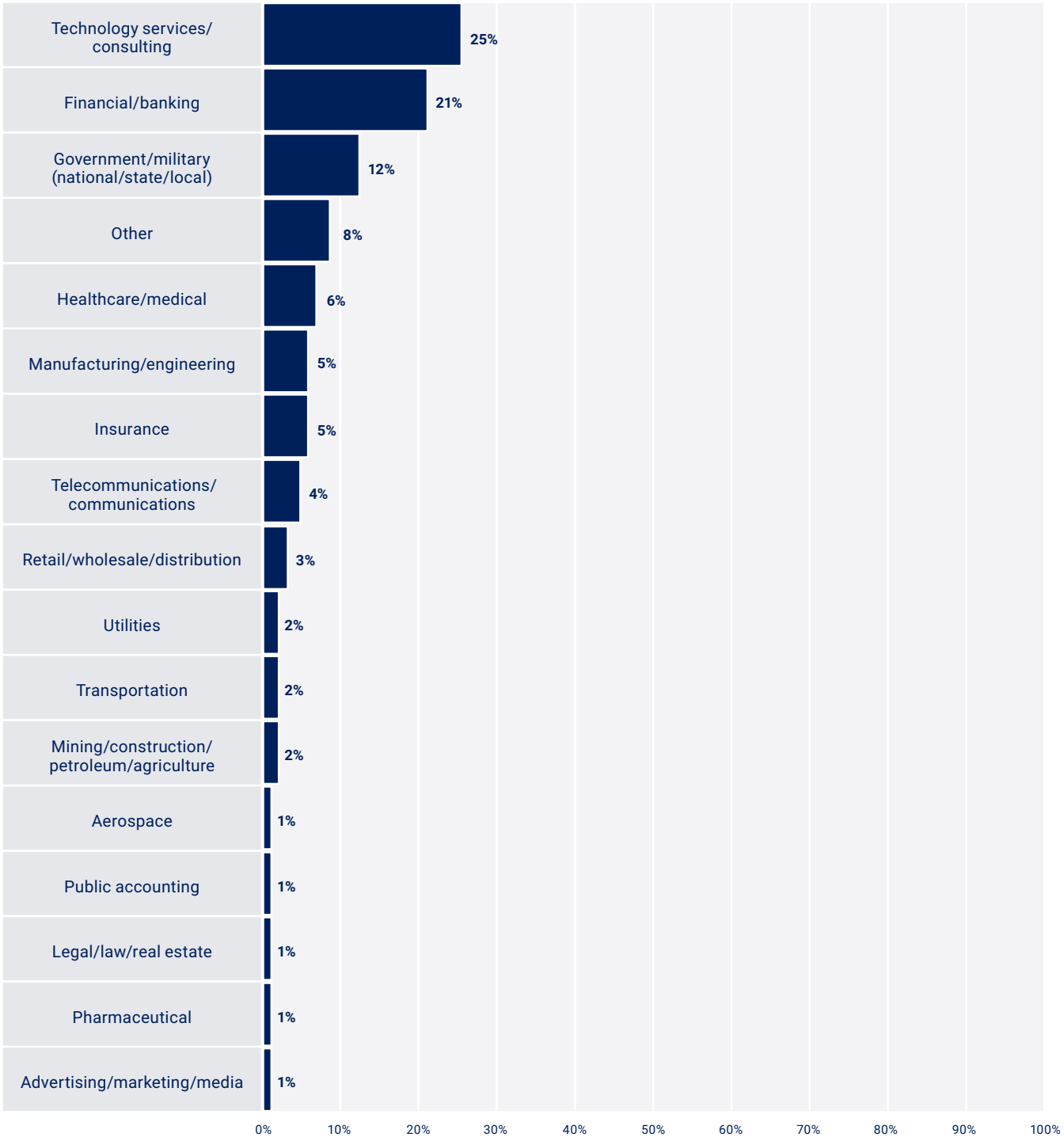


FIGURE 2: Industries Represented

Please indicate your organization's primary industry.



Cybersecurity Workforce Considerations

Like in previous years, many respondents believe that cybersecurity staffing is a challenge. The majority of survey respondents (55%) believe that their cybersecurity team is understaffed—this is a slight improvement from last year, when 57% of respondents believed that their cybersecurity team was understaffed. Respondents at enterprises with 500 to 4,999 employees are more likely to say that their cybersecurity team is understaffed, with 62% of these respondents indicating that their cybersecurity team is significantly or somewhat understaffed.

The percentages of respondents who believe that their cybersecurity team is appropriately staffed or overstaffed are similar to last year. The median security staff size remains the same as last year, at eight employees.

Hiring and Open Roles

The survey results show that many enterprises continue to have open cybersecurity positions, and not much of the data related to open roles changes compared to last year. **Figure 3** shows the percentage of respondent enterprises with open cybersecurity roles and the levels of those roles. The percentage of respondent enterprises with open entry-level positions remains the same as last year, at 18%, and the percentage of respondents with open non-entry-level positions (47%) is one point higher than in 2024.

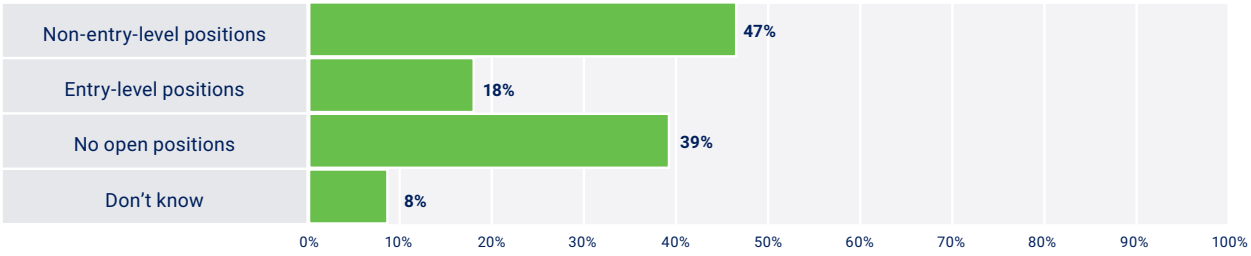
Finding the best, most qualified person for a cybersecurity role can take a significant amount of time, regardless of the level of the position. Thirty-eight percent of respondents say that the time to fill entry-level cybersecurity roles with a qualified candidate is three to six months on average, and 13% say that the time to fill these positions is more than six months on average.

Unsurprisingly, the time to fill non-entry-level roles is slightly longer, with 39% of respondents indicating that it takes three to six months to fill these roles and 25% of respondents reporting more than six months on average. The survey results reveal regional differences—31% of respondents in Asia[1] and 30% of respondents in Africa and Europe say that filling non-entry-level cybersecurity roles takes more than six months, whereas only 14% of respondents in Oceania report that filling these roles takes more than six months.

Twenty-one percent of respondents believe that the time to fill open cybersecurity positions has increased, 43% say it stayed the same, and 17% say it decreased.

FIGURE 3: Open Roles

Does your organization have unfilled (open) cybersecurity positions? Select all that apply.



1 Excluding China and India.

These results are similar to last year, when 24% said the time to fill positions increased, 42% said it stayed the same, and 16% said it decreased. **Figure 4** shows the position levels where respondent enterprises have most or all their unfilled cybersecurity positions.

Many enterprises struggle to find the best, most qualified talent for open roles. Only 31% of survey respondents say that a majority of cybersecurity applicants are well qualified for the positions to which they are applying. Twenty-three percent of respondents say that 25% or fewer applicants are well qualified.

Figure 5 shows the factors that today's cybersecurity professionals consider to be very important in determining a candidate's qualifications. A noteworthy finding is that adaptability—a new option provided in this year's survey—is now the most important factor in determining a candidate's qualifications. Given the rapid pace at which cyberincidents can occur and the fast-changing technology landscape, enterprises want to hire cybersecurity professionals who are able to adapt to a wide variety of environments and situations. These factors, coupled with shifting enterprise priorities, may explain why adaptability has the highest value.

The importance of prior work experience in cybersecurity drops considerably compared to last year, falling from the first to the second most sought-after factor in determining candidate qualification. The top-three most desired factors have a considerable lead over the remaining factors, indicating that adaptability, previous work experience, and organizational fit are better indicators of qualification than some other factors.

Many enterprises struggle to find the best, most qualified talent for open roles.

The anticipated demand for cybersecurity positions varies based on seniority level. **Figure 6** shows that the position that is most likely to increase in demand is the individual technical cybersecurity professional. Considering that enterprises may employ multiple individual cybersecurity contributors but only one cybersecurity executive and senior manager, it makes sense that the demand for senior-level positions is not expected to be as high as the demand for individual contributors. Overall, the anticipated demand for all positions is similar to last year's survey findings, but the demand for all positions levels is dropping more than last year.

FIGURE 4: Open Cybersecurity Position Levels

How many of your unfilled (open) cybersecurity positions are at the following levels? Percentages indicate respondents selecting "all" and "most."

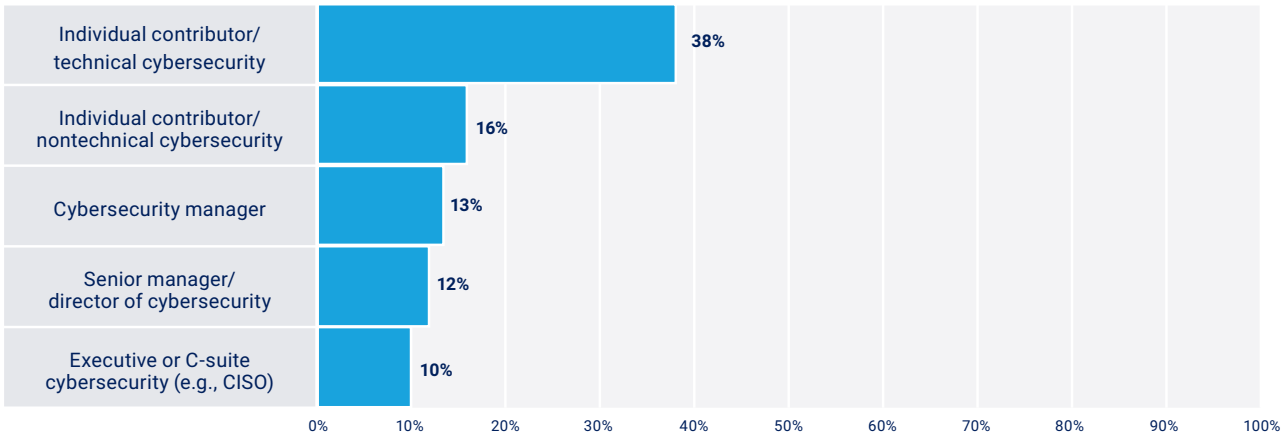
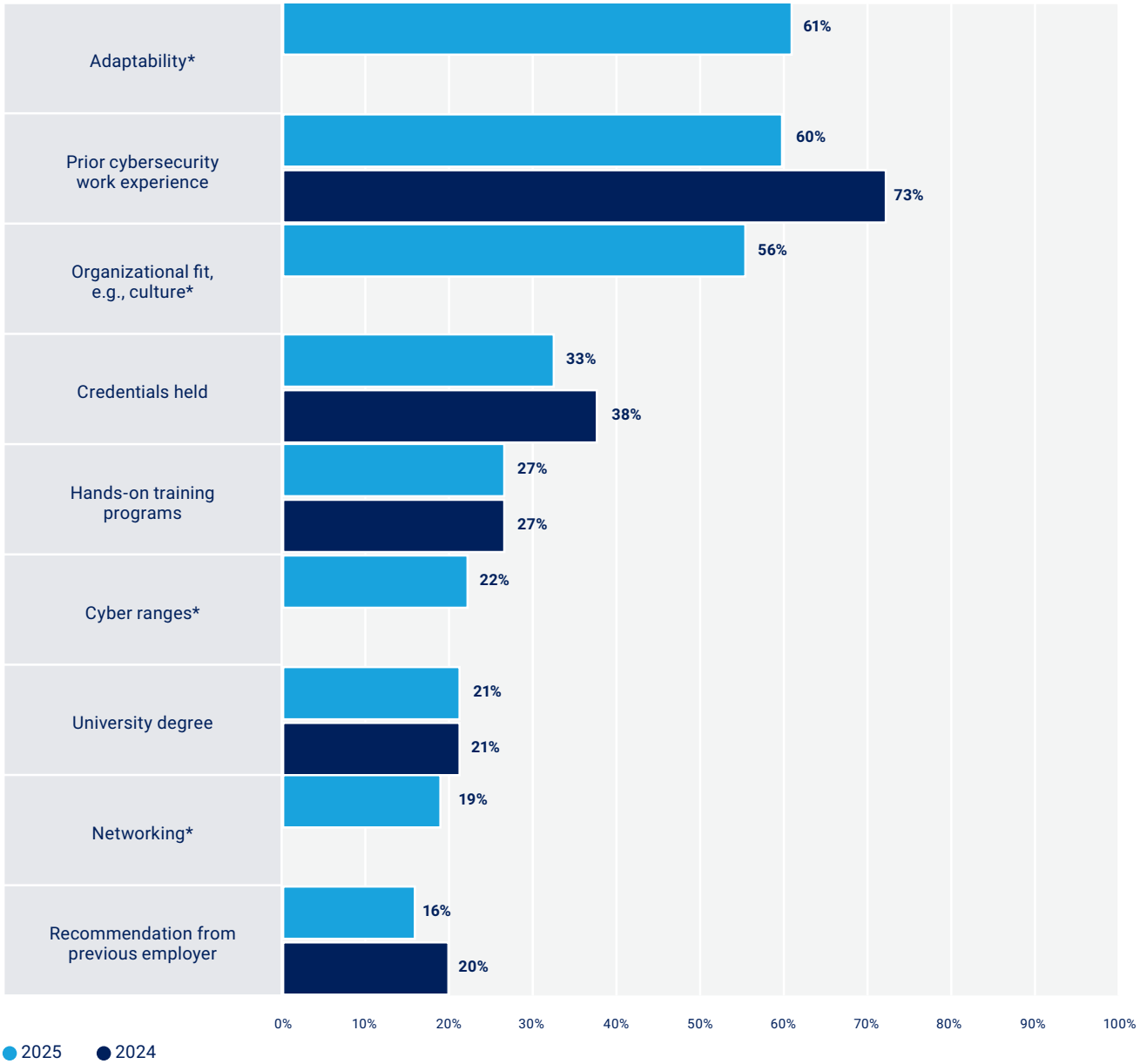


FIGURE 5: Factors Indicating Candidate Qualification

How important are each of the following factors in determining if a cybersecurity candidate is qualified? Percentages represent respondents indicating these factors as "very important."

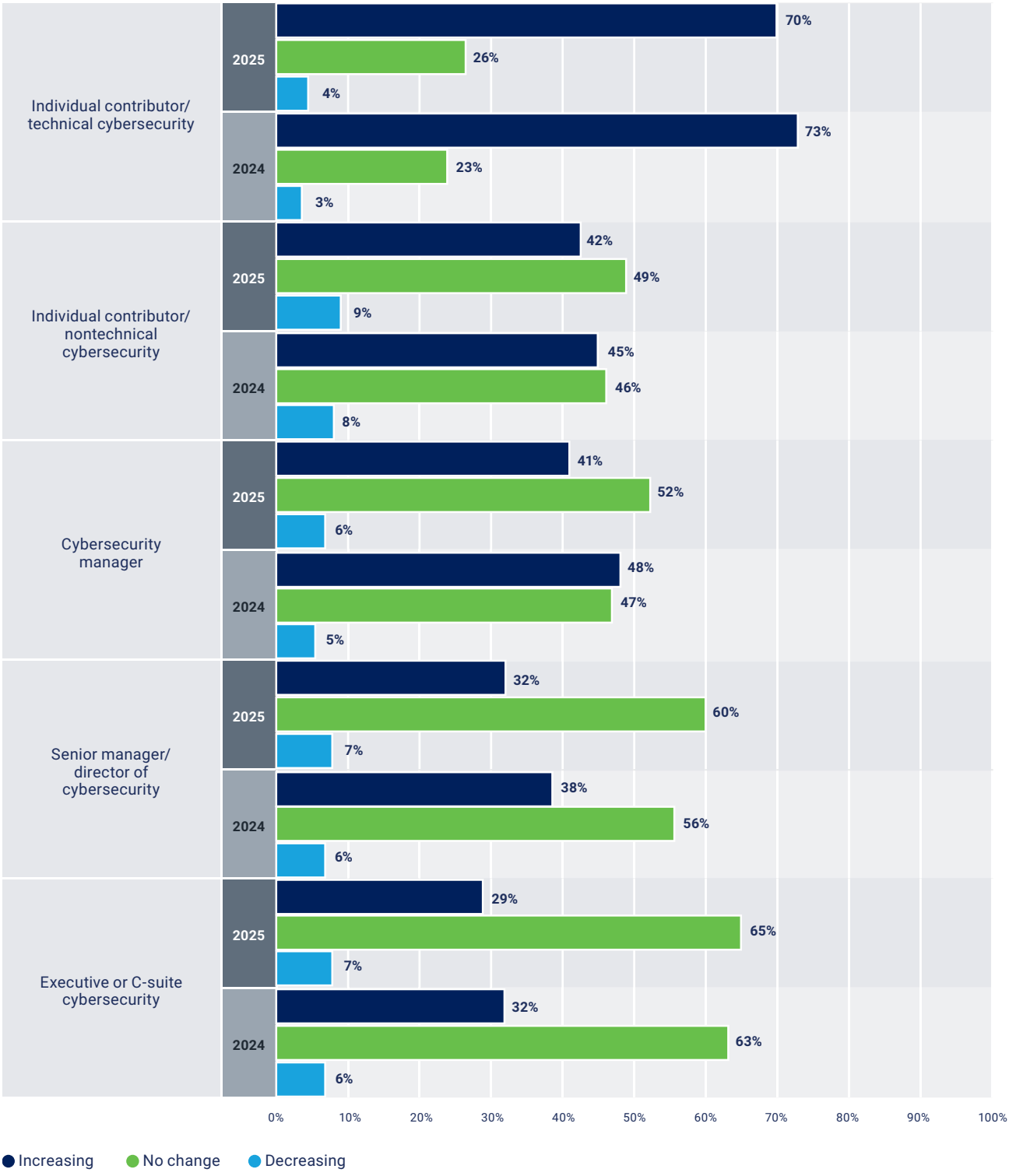


**New factor in 2025 survey*

The importance of prior work experience in cybersecurity drops considerably compared to last year, falling from the first to the second most sought-after factor in determining candidate qualification.

FIGURE 6: Anticipated Demand for Cybersecurity Positions[2]

In the next year, do you see the demand for the following cybersecurity position levels increasing, decreasing, or remaining the same?



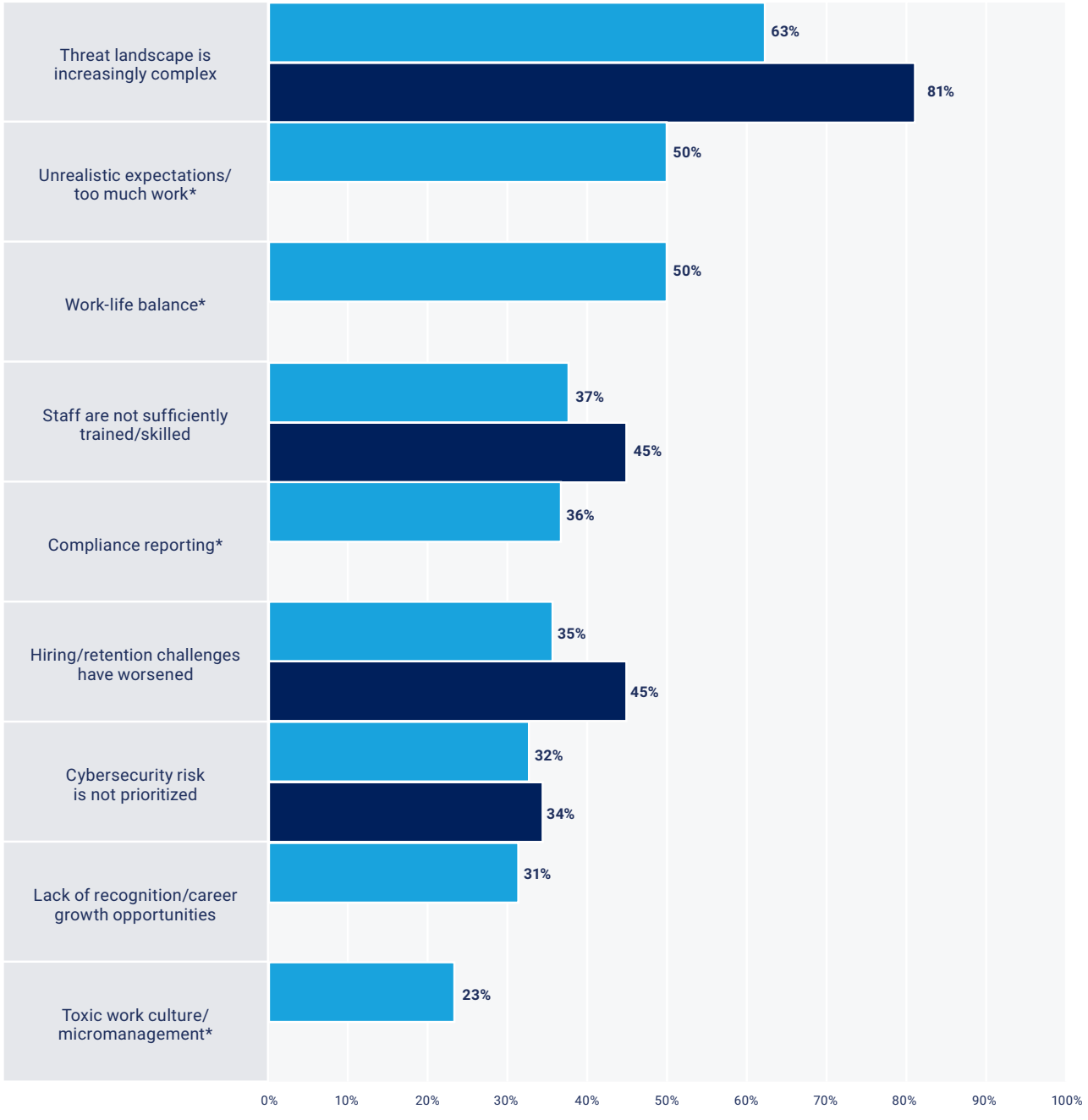
2 This figure excludes "Don't know" responses.

Burnout and Retention

Consistent with last year's survey findings, the majority of respondents indicate that their roles are more stressful now than they were five years ago. This year, 37% of respondents say that their role is significantly more stressful now than it was five years ago, compared to 35% last year. **Figure 7** shows the reasons why cybersecurity jobs feel more stressful now than they did five years ago.

FIGURE 7: Sources of Job Stress

Please tell us why your role is more stressful today than it was 5 years ago.



**New option in 2025 survey*

One of the most notable differences from 2024 is that almost 20% fewer respondents indicate that a complex threat landscape is a reason why their roles feel more stressful. This finding may indicate that survey respondents have a better understanding of the threat landscape, which is supported by the slight increase in respondents who say that their enterprise provides professional development training (**figure 11**).[3] Enterprise leadership may see the value of cybersecurity professionals with threat landscape expertise and support further professional development related to its understanding, which may explain the decrease in respondents indicating that a complex threat landscape is a source of stress. Many cybersecurity organizations are expected to do more with fewer resources, which can impact work-life balance. These stressors, coupled with decreasing employer benefits and pessimistic budget forecasts, could account for why cybersecurity jobs feel more stressful now than in the past.

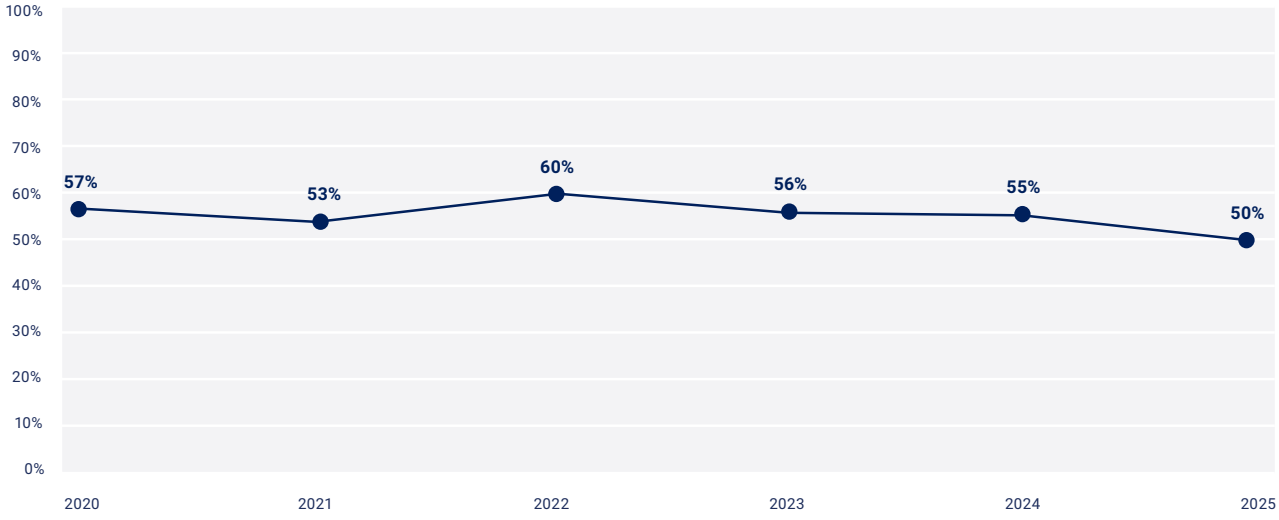
Because many cybersecurity professionals find their roles more stressful than they did five years ago, employee burnout is a serious concern for many enterprises. Burnout can impact employee productivity, increase turnover, and cause staff to be more likely to make mistakes.[4] It is concerning that one-quarter of respondents say that their enterprises are not taking steps to mitigate burnout. The most common methods that respondent enterprises that do address employee burnout use are flexibility and time away from work. Mitigation strategies include:

- Flexible work schedules (53%)
- Encouraging breaks and vacation time (46%)
- Rebalancing workloads (30%)
- Job rotations (15%)
- Sabbaticals/mandatory time off (12%)

Despite the prevalence of burnout and high levels of stress among cybersecurity staff, only half of respondents indicate difficulty in retaining qualified cybersecurity professionals—the lowest result since ISACA began reporting this metric in 2020 (**figure 8**).

FIGURE 8: Retention Difficulties (2020-2025)[5]

Has your organization experienced difficulties retaining qualified cybersecurity professionals?



3 Note that the 2025 survey contains more possible responses for figure 7 than last year's survey, which may dilute the absolute percentages.

4 American Psychological Association, "Employers need to focus on workplace burnout: Here's why," 12 May 2023, www.apa.org/topics/healthy-workplaces/workplace-burnout

5 The figure depicts "Yes" responses for the years 2020-2025.

Given that job markets can vary globally, there are some regional differences in retention difficulties based on region (**figure 9**). North America has the fewest challenges with retention, while retention is a considerable obstacle for respondents in Latin America and Africa.

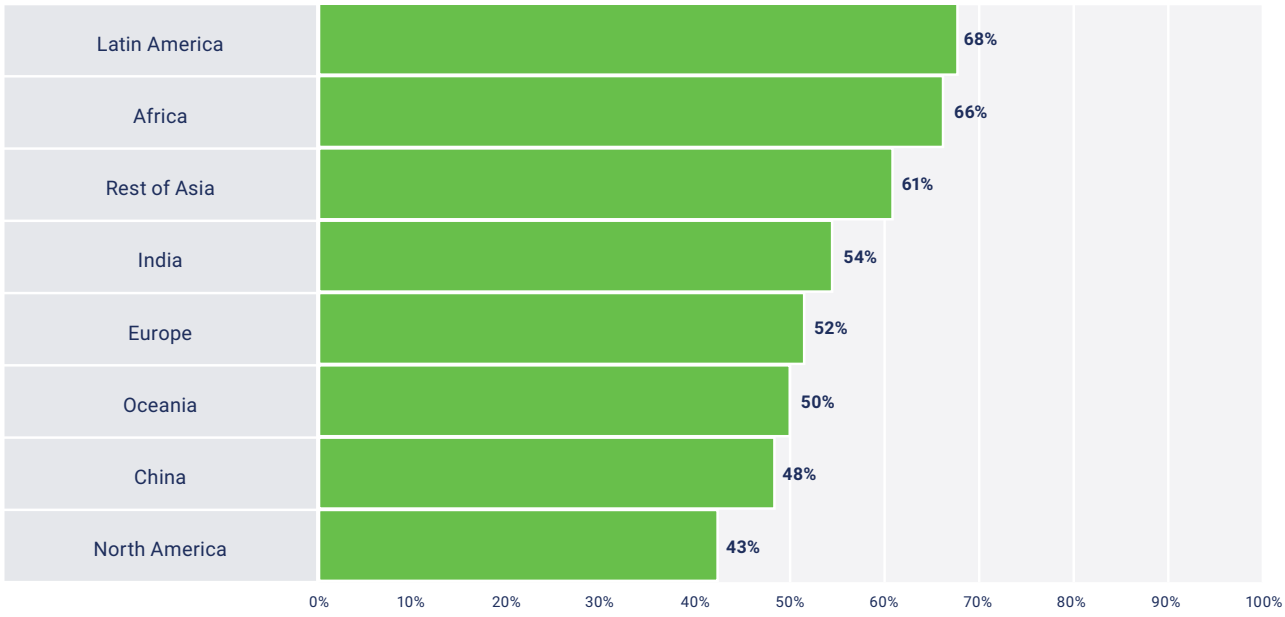
Burnout and other sources of job dissatisfaction may lead cybersecurity professionals to find new jobs. **Figure 10** shows the reasons why cybersecurity professionals leave their jobs. It supports the prevalence of the Big Stay—the trend of workers staying in their jobs rather than seeking new employment.[6] Recruitment by other enterprises is down 5% compared to last year. Dissatisfaction with financial incentives also decreases considerably (six percentage points) compared to 2024.

Some Employer Benefits Decrease

The findings in **figure 10** also indicate that employers have dominance in the cybersecurity labor market at this time—increased retention and a steady number of open positions favor employers rather than employees. This employer dominance is supported by the overall decrease in employer benefits compared to 2024 (**figure 11**).

FIGURE 9: Retention Difficulty by Region[7]

Has your organization experienced difficulties retaining qualified cybersecurity professionals?



6 Lewis, G.; Zurbano, A.; "The 'Big Stay' Is Still Here—But May Not Stay That Way for Long," LinkedIn, 16 May 2024, www.linkedin.com/business/talent/blog/talent-acquisition/big-stay-is-still-here

7 The figure depicts "Yes" responses to the question by reporting region.

FIGURE 10: Reasons for Leaving Current Job

Which, if any, of the following reasons do you feel are causing cybersecurity professionals to leave their current job?

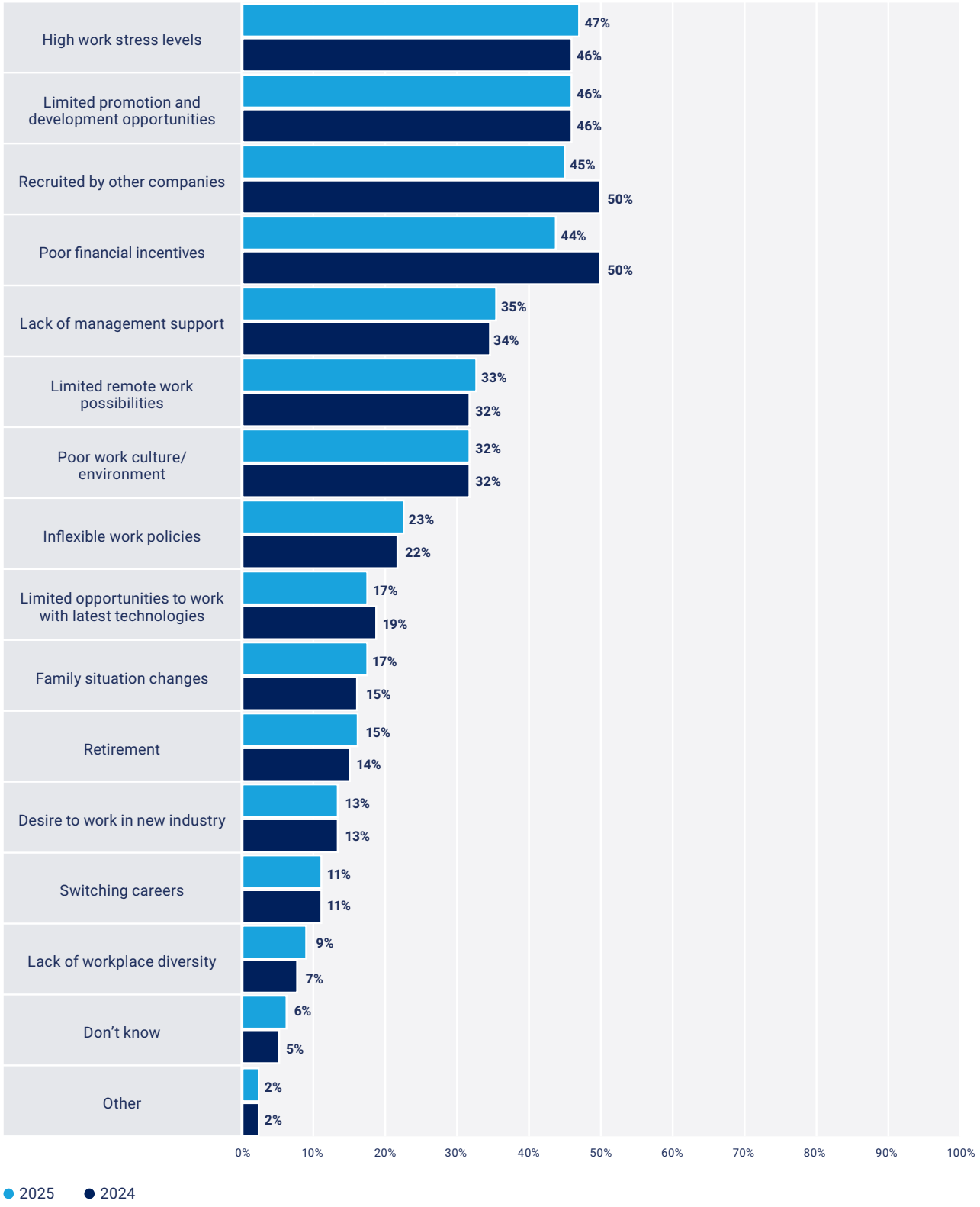
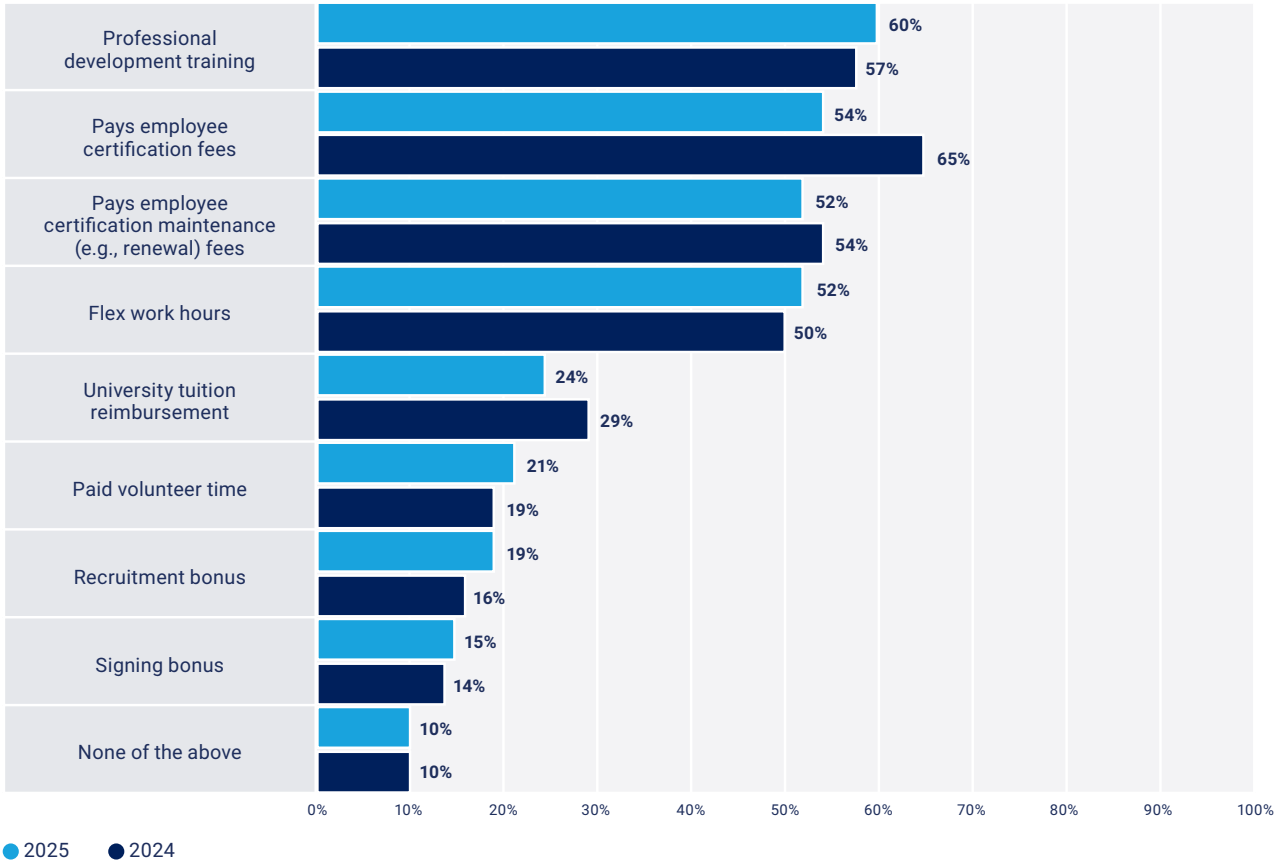


FIGURE 11: Employer Benefits

Which of the following benefits does your employer offer? Select all that apply.



Particularly concerning is the 11-point drop in the percentage of respondents indicating that their employers pay certification fees. A five-point drop in tuition reimbursement is also a concern—just less than one-quarter of respondents report that their employers offer tuition reimbursement.

High work stress is one of the primary reasons that cybersecurity professionals are leaving their jobs, so it is surprising that employers are not doing more to remedy this stress. Only 30% of respondents say that their enterprises rebalance workloads, and just over half (53%) of respondent enterprises offer employees flexible work hours. The top benefits are related to professional development and certifications. Although these are valuable and sought-after perks, they likely do not address work-related stress.

Upskilling, whether through professional development training or certification, remains a primary benefit offered to cybersecurity professionals, although the employer-paid certification fees benefit drops 11 points this year. According to survey respondents, upskilling is funded through:

- Operational budget (34%)
- Both operational and human resources (HR) budgets, depending on the circumstances (25%)
- HR budget (12%)

Five percent of respondents report that their enterprises do not fund employee upskilling, and 24% of respondents say that they do not know how their enterprise funds upskilling.

The Talent Pipeline

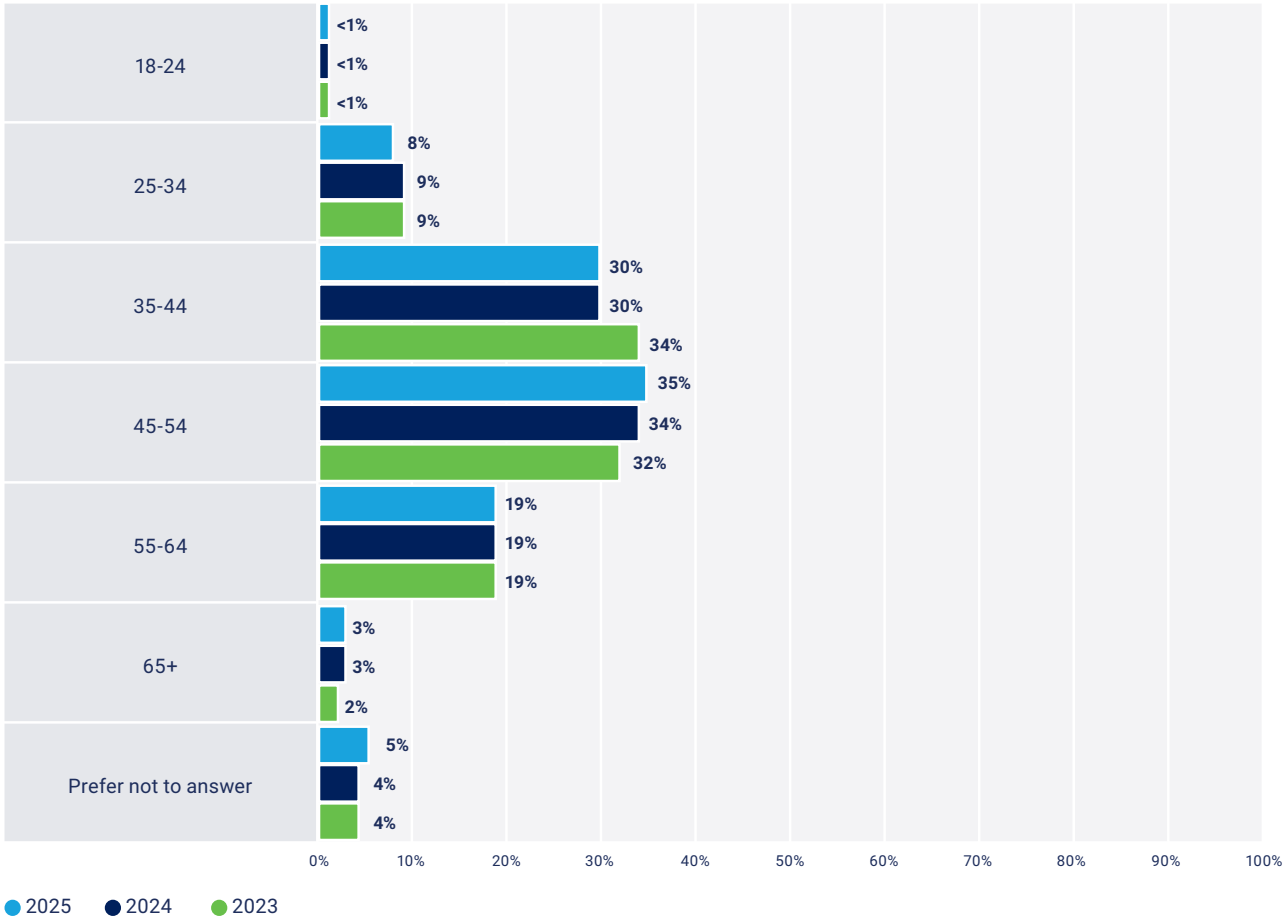
Because many pathways can lead to a career in cybersecurity, not everyone who is currently working in a cybersecurity role began their careers in cybersecurity. Forty percent of respondents say that half or more of their cybersecurity staff started their careers in cybersecurity, and 46% say that half or more of their cybersecurity staff started their careers in different fields and transitioned into cybersecurity roles.

Future Workforce Concerns

The 2023 and 2024 ISACA *State of Cybersecurity* surveys established that the cybersecurity workforce is aging slightly (**figure 12**).

FIGURE 12: Workforce Age

Please select your age.



Although ISACA surveys are conducted only among ISACA members and may not necessarily represent the broader cybersecurity workforce, other industry research corroborates these findings. The ISC2 *2024 ISC2 Cybersecurity Workforce Study* found an increase in workers entering the cybersecurity profession who are in the 39 to 49 age group (35%) and found that only 12% of entrants into the field are under the age of 30.[8]

This year's survey results show that the percentage of respondents under the age of 35 slightly drops, and the percentage of respondents who are ages 45 to 54 remains higher than those ages 35 to 44. This trend is worth watching, because nearly one-fifth of respondents are a decade or a little longer from considering retirement, and it does not appear that there are enough younger cybersecurity professionals to fill the roles left by seasoned cybersecurity professionals who will retire.

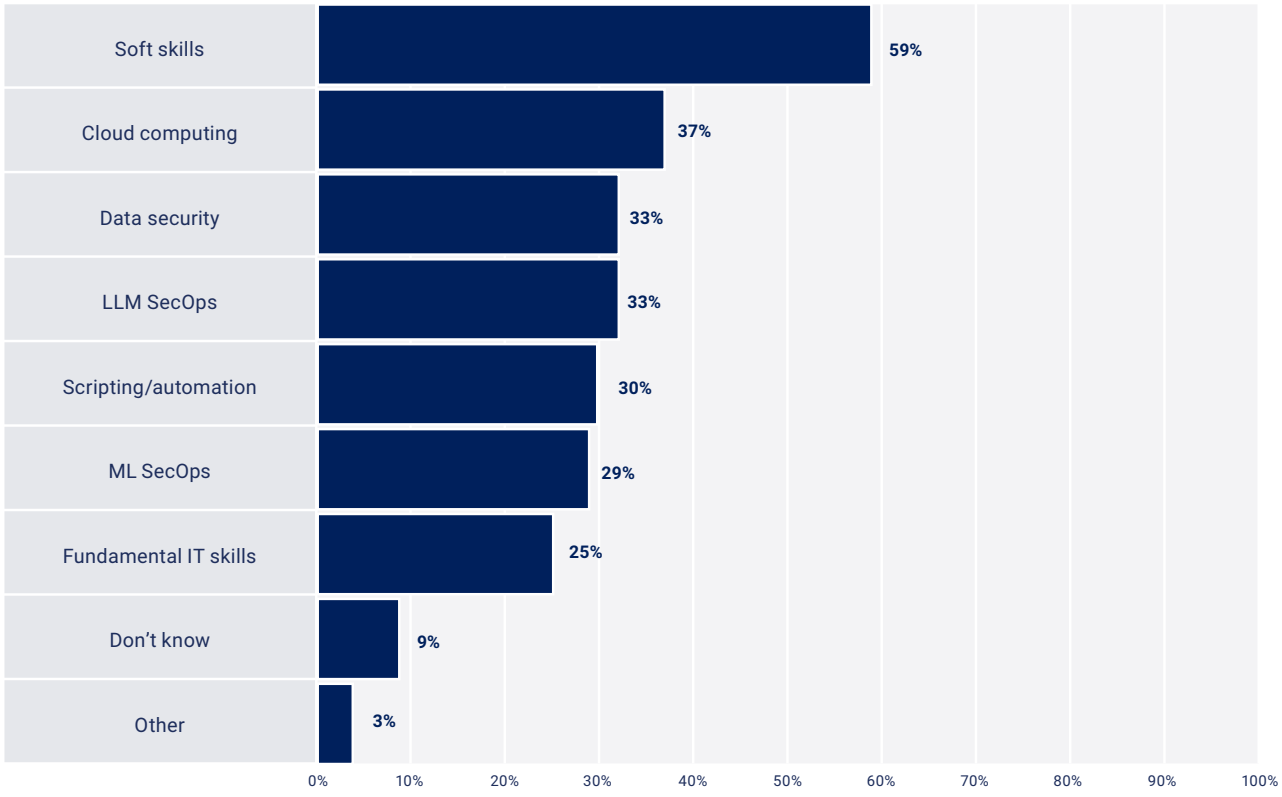
Note that the workforce is not aging this way in all regions. In India, 15% of respondents are ages 25 to 34, and 51% are ages 35 to 44. In China, 14% of respondents are ages 25 to 34, and 34% are ages 35 to 44.

Skill Gaps

Attracting new talent to the cybersecurity industry and creating pathways to allow people to move into cybersecurity careers can help mitigate challenges associated with succession planning. But this talent must have the requisite skills to excel in their roles. An even greater percentage of respondents than last year believe that soft skills are a significant skill gap. Fifty-nine percent of respondents identify it as a skill gap among cybersecurity professionals, which is eight points higher than last year. Cloud computing remains the second biggest skill gap (37%). **Figure 13** shows the skill gaps identified by survey respondents.

FIGURE 13: Skill Gaps in Today's Cybersecurity Professionals

What are the biggest skill gaps you see in today's cybersecurity professionals?



8 ISC2, *2024 ISC2 Cybersecurity Workforce Study: Global Cybersecurity Workforce Prepares for an AI-Driven World*, 31 October 2024, www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

Soft skills are highly valued among security professionals. Survey respondents say that the top-five most important soft skills security professionals need are:

- Critical thinking (57%)
- Communication (includes listening, speaking, and conflict resolution) (56%)
- Problem solving (47%)
- Teamwork (includes collaboration and cooperation) (45%)
- Adaptability/flexibility (40%)

To remedy the skill gaps associated with nontechnical skills, enterprises are leveraging online learning websites, mentoring, corporate training events, and academic tuition reimbursement.

These are the same top soft skills that were identified in 2024, with the same rankings, except that communication and critical thinking switched spots. Other important soft skills include:

- Self-motivation (32%)
- Leadership (31%)
- Work ethic (30%)
- Integrity/honesty (29%)
- Attitude (29%)
- Organization (27%)
- Writing skills (21%)
- Empathy (15%)

To remedy the skill gaps associated with these nontechnical skills, enterprises are leveraging online learning websites (51%), mentoring (41%), corporate training events (34%), and academic tuition reimbursement (19%).

Although soft skills are important, successful cybersecurity professionals must also possess technical skills. Survey respondents identify the following top-five most important security skills:

- Data security (54%)
- Vulnerability management (50%)
- Threat detection and response technologies (49%)
- Cloud computing (47%)
- Identity and access management (47%)

Other important security skills include:

- Incident response (46%)
- Vulnerability discovery (27%)
- Scripting/automation (25%)
- LLM SecOps (24%)
- ML SecOps (19%)
- Application programming interfaces (15%)
- Microsegmentation (12%)
- Virtualization (11%)

Last year, the top tactic to mitigate technical cybersecurity skill gaps was providing training to interested nonsecurity professionals to enable them to move into security roles (41%). This mitigation investment decreases greatly this year to 29%, and using contract employees takes the lead at 30% (down six percentage points from 2024). Other methods to address technical security gaps include:

- Relying on AI or automation (23%)
- Increasing use of reskilling programs (21%)
- Increasing the use of performance-based training to attest to actual skill mastery (20%)
- Leveraging apprenticeships/internships (19%)
- Increasingly relying on credentials to attest to actual subject matter expertise (18%)

A majority of global respondents (56%) typically require entry-level cybersecurity professionals to have a university degree. However, global variance on university degree requirements is considerable (**figure 14**).

Although many enterprises require cybersecurity professionals to have a university degree, having a degree does not mean that a candidate has all the necessary skills, knowledge, and expertise to excel in a cybersecurity role. Perceptions about the preparedness of university graduates for working in cybersecurity vary. **Figure 15** shows respondent evaluations of recent university graduates' preparedness for cybersecurity challenges.

FIGURE 14: Global University Degree Requirements[9]

Does your organization typically require a university degree to fill your entry-level cybersecurity positions?

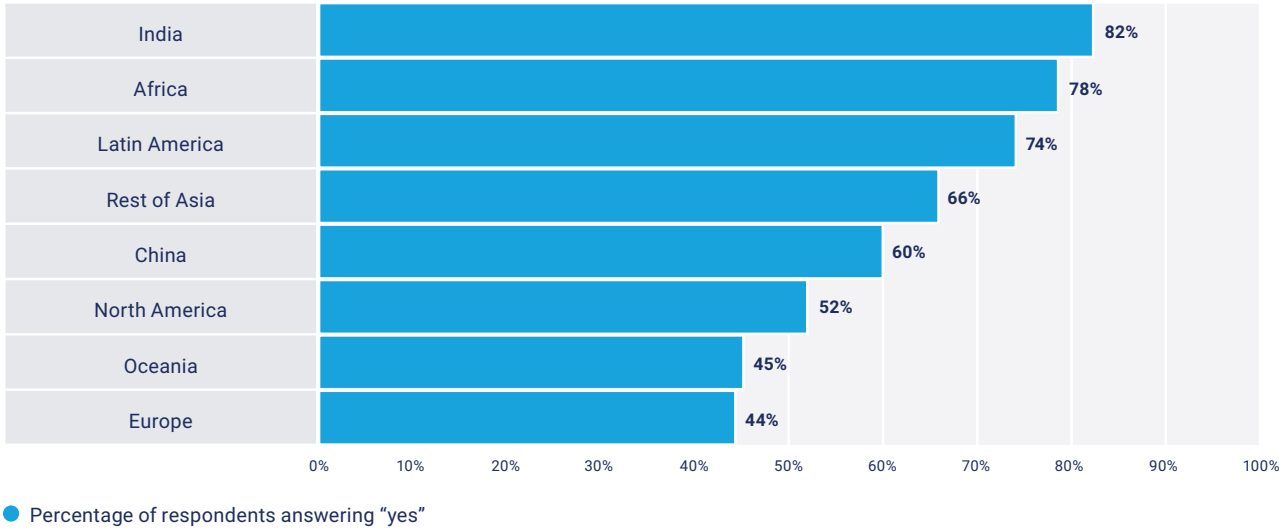
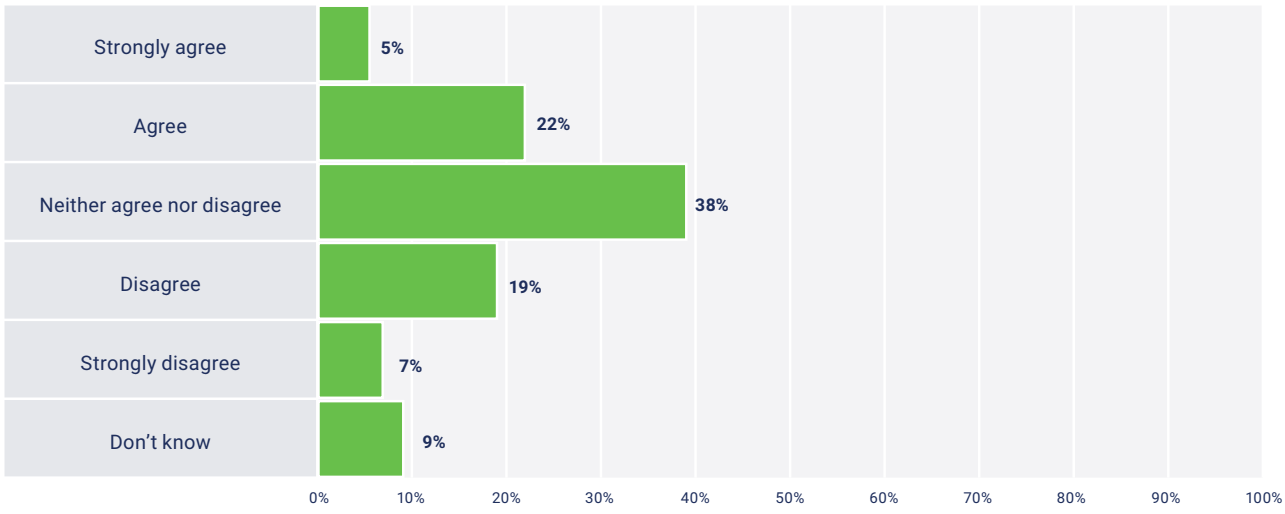


FIGURE 15: Career Preparedness

To what extent do you agree or disagree that recent university graduates in cybersecurity are well prepared for the cybersecurity challenges in your organization?



9 Percentages represent respondents who answer "Yes."

Survey respondents identify the following common skill gaps among recent university graduates:

- Incident response (43%)
- Data security (39%)
- Threat detection and response technologies (39%)
- Identity and access management (39%)
- Vulnerability management (37%)
- Cloud computing (32%)
- Vulnerability discovery (29%)
- Scripting/automation (27%)
- LLM SecOps (26%)
- ML SecOps (24%)
- Application programming interfaces (20%)
- Microsegmentation (20%)
- Virtualization (15%)

Just under half (45%) of survey respondents manage security staff who have less than three years of work experience. Survey respondents identify the following top areas in which staff with less than three years of work experience most need professional development and training:

- Data security (48%)
- Incident response (47%)
- Threat detection and response technologies (42%)
- Vulnerability management (41%)
- Cloud computing (40%)
- Identity and access management (40%)

Cybersecurity Operations

Depending on enterprise size, sector, and region, the structure of the cybersecurity organization can vary. Three-quarters of respondent cybersecurity organizations have a chief information security officer (CISO). **Figure 16** shows to whom CISOs report.

If an enterprise does not have a CISO, the security team reports to another leader. The most common roles to which security teams report at enterprises that do not have CISOs are the chief information officer (26%), chief technology officer (17%), and chief executive officer (14%).

Budgets

Just over half of respondents (53%) believe that their cybersecurity budget is somewhat or significantly underfunded. This is an improvement from 2024, when 59% reported that their cybersecurity budget was underfunded (**figure 17**). Despite this change, pessimism about anticipated cybersecurity budget cuts has grown and is almost equivalent with 2021, when 20% of respondents forecasted decreasing cybersecurity budgets in the following 12 months (**figure 18**). This pessimism may be caused by economic uncertainty. With the exception of Africa, respondents in most global regions share concerns about these budget cuts.

Boards and Cybersecurity Prioritization

The same percentage of respondents (56%) as last year say that their boards of directors adequately prioritize cybersecurity. Also identical to last year is the percentage of respondents who say that their enterprise cybersecurity strategy is aligned with enterprise objectives (74%). Unsurprisingly, among those whose boards adequately prioritize cybersecurity, this percentage jumps to 95%.

FIGURE 16: CISO Reporting

To whom does the CISO report in your organization?

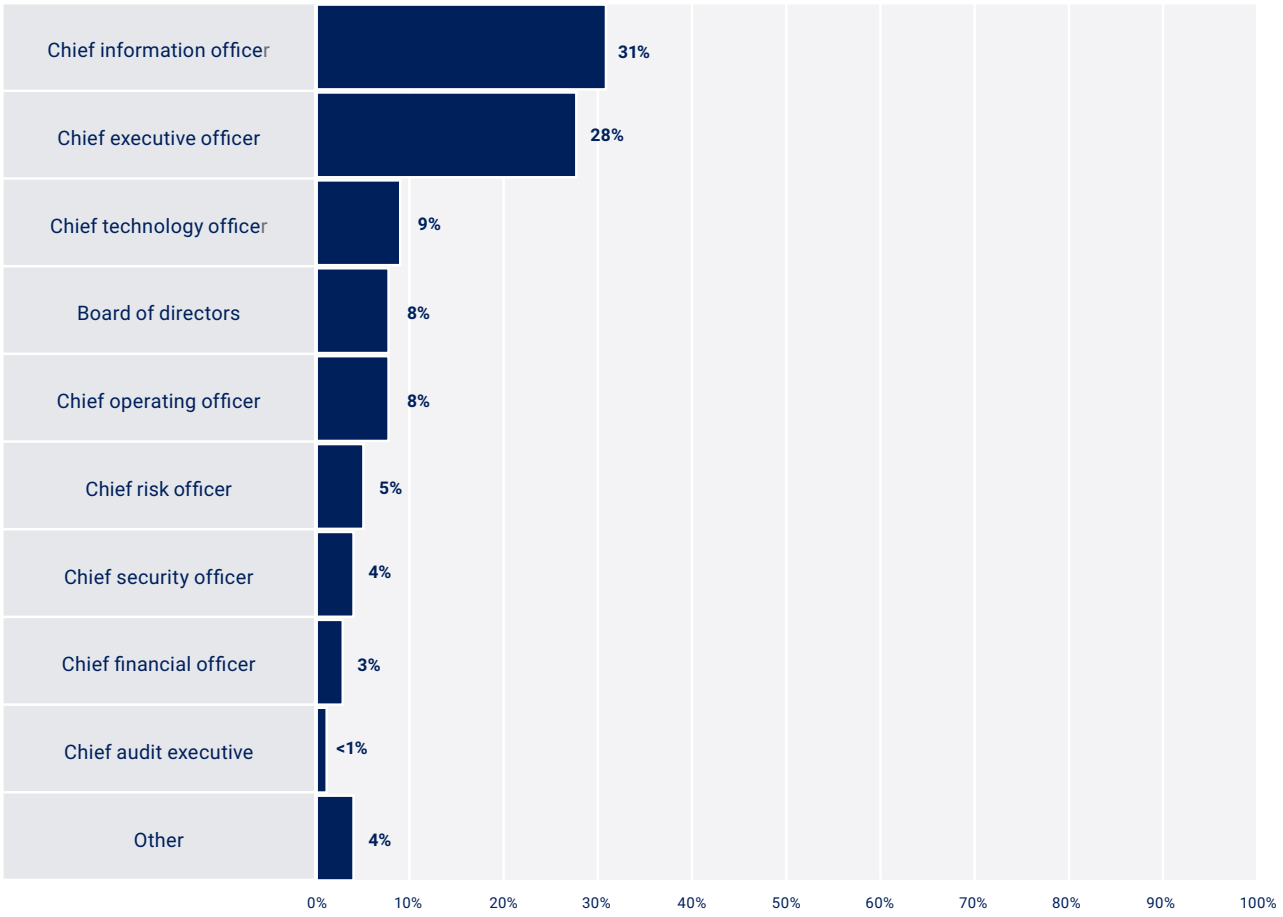


FIGURE 17: Cybersecurity Budget Funding

Do you feel that your organization's cybersecurity budget is currently:

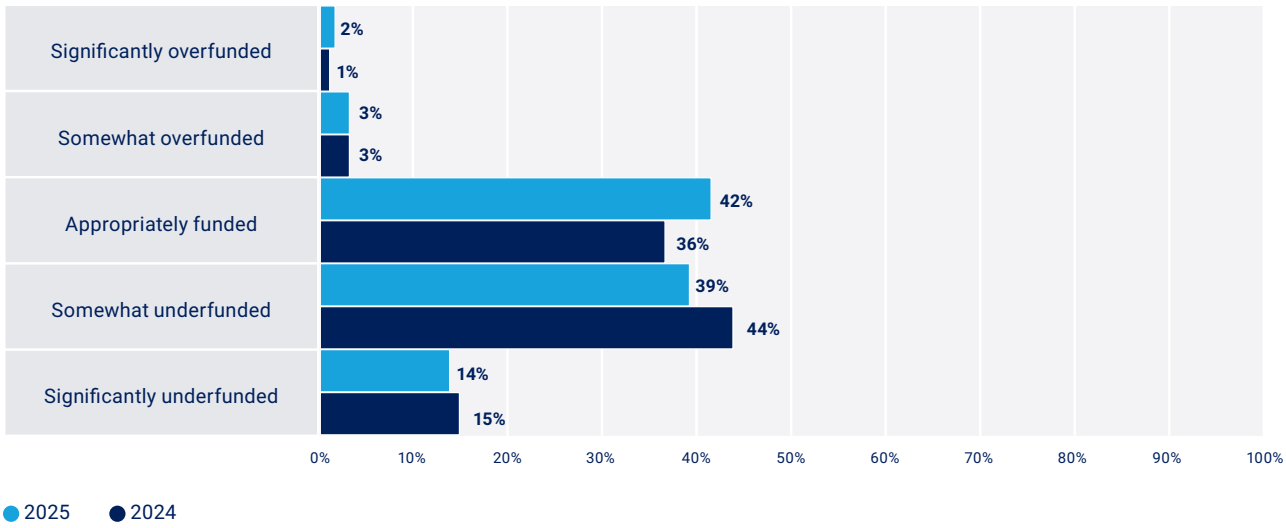
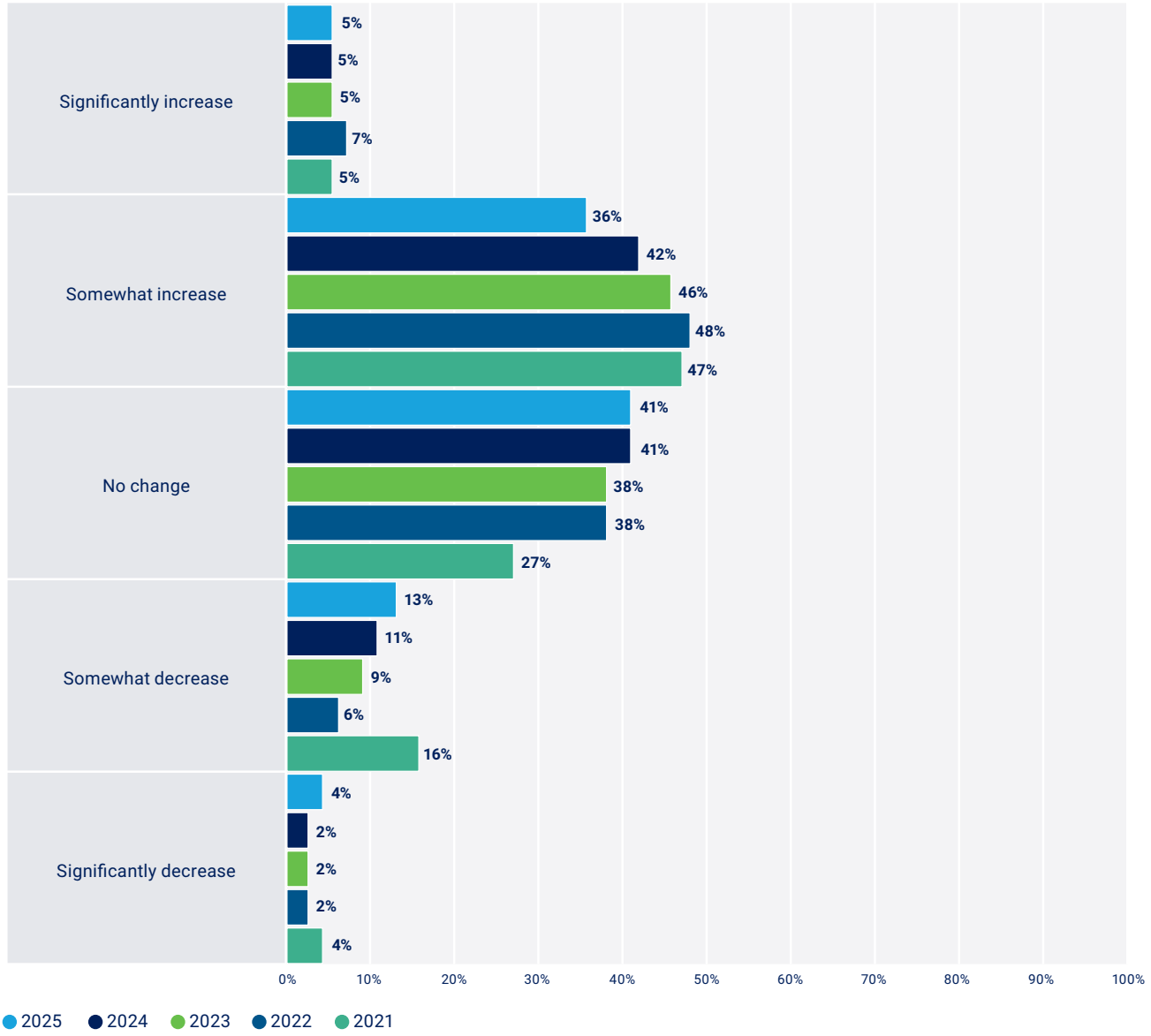


FIGURE 18: Cybersecurity Budget Forecasts

How, if any, will your organization's cybersecurity budget change in the next 12 months?



Other trends emerge when comparing the enterprises whose boards adequately prioritize cybersecurity with those who do not. Board prioritization can ensure that cybersecurity teams have the resources they need and that they feel more confident in their cybersecurity abilities:

- 56% of respondents feel completely confident or very confident in their enterprise cybersecurity team's ability to detect and respond to cyberthreats (compared to just 21% for respondents whose boards do not adequately prioritize cybersecurity).
- 35% of respondents feel that their cybersecurity budget is underfunded (compared to 74% of respondents whose boards do not adequately prioritize cybersecurity).
- Respondent enterprises whose boards prioritize cybersecurity are much more likely to offer competitive benefits (e.g., professional development training, paying employee certification fees).
- Only 48% of respondents have challenges retaining qualified cybersecurity staff (compared to 64% of respondents whose boards do not prioritize cybersecurity).

Cyberrisk and Cyberattacks

More than one-third of survey respondents say that their enterprises are experiencing an increase in cyberattacks compared to a year ago (**figure 19**), although this result is down three percentage points from last year.

Figure 20 lists the threat actors responsible for attacks, and the findings are overall similar to last year's survey results.

FIGURE 19: Cyberattack Trends

Is your organization experiencing an increase or decrease in cybersecurity attacks as compared to a year ago?

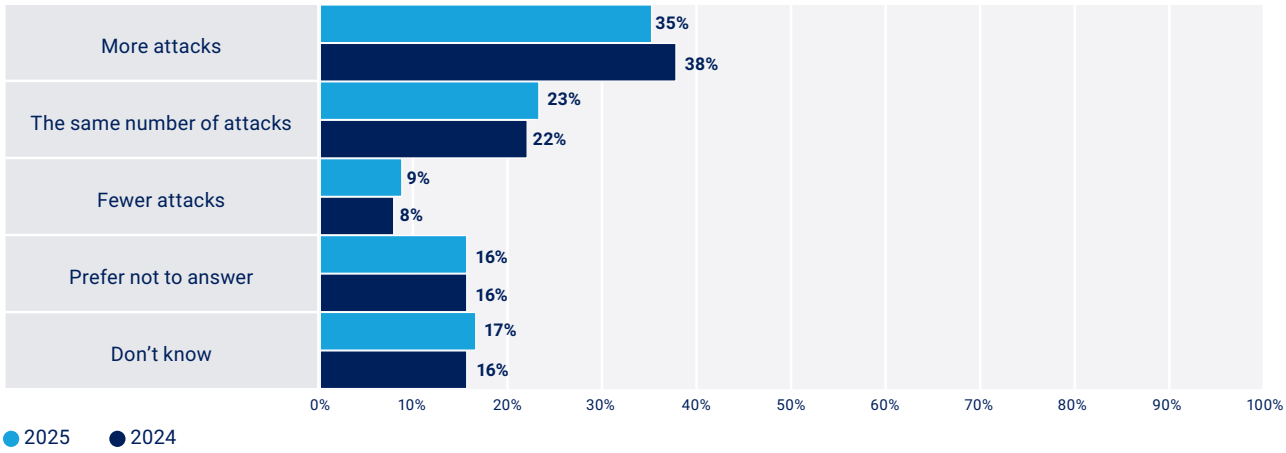
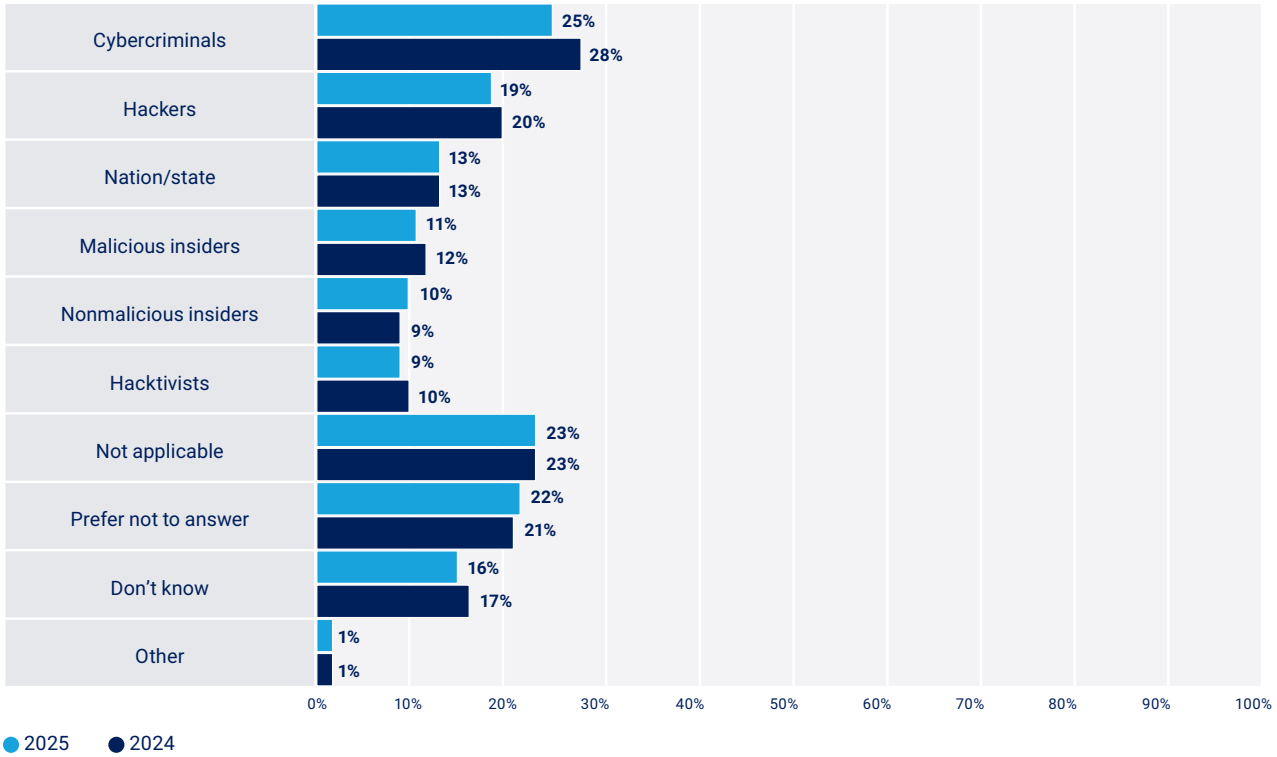


FIGURE 20: Threat Actors

If your organization was exploited this year, which of the following threat actors were to blame?



Only 10% of respondents say that their enterprises have been compromised since June 2024. Sixty-five percent said that their enterprises were not compromised within this time frame, and 26% do not know. **Figure 21** shows the attack vectors used when these enterprises were compromised.

AI can be used by bad actors to craft well-written phishing emails or malicious code; therefore, it is surprising that only 19% of respondents say that cyberattacks were confirmed or believed to be AI driven. Almost one-third (31%) of respondents do not know if cyberattacks were AI driven, indicating that it may not always be possible to determine if AI played a role in an attack.

Many respondents believe it is possible their enterprise will experience a cyberattack in the next year (43%) (**figure 22**), but this is a slight decrease from last year (47%).

FIGURE 21: Attack Vectors Used

Which of the following attack vectors were used when your organization was compromised?

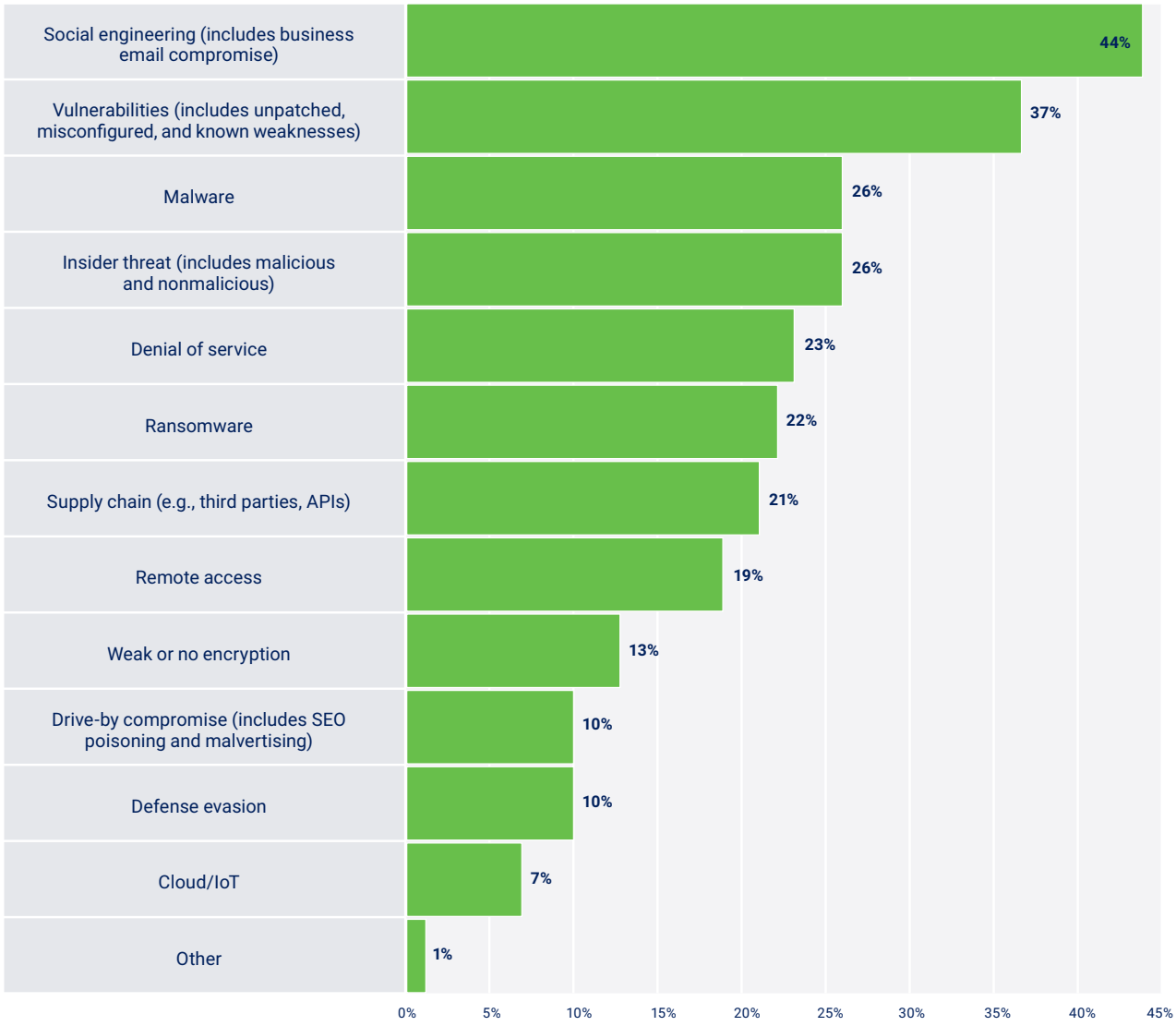
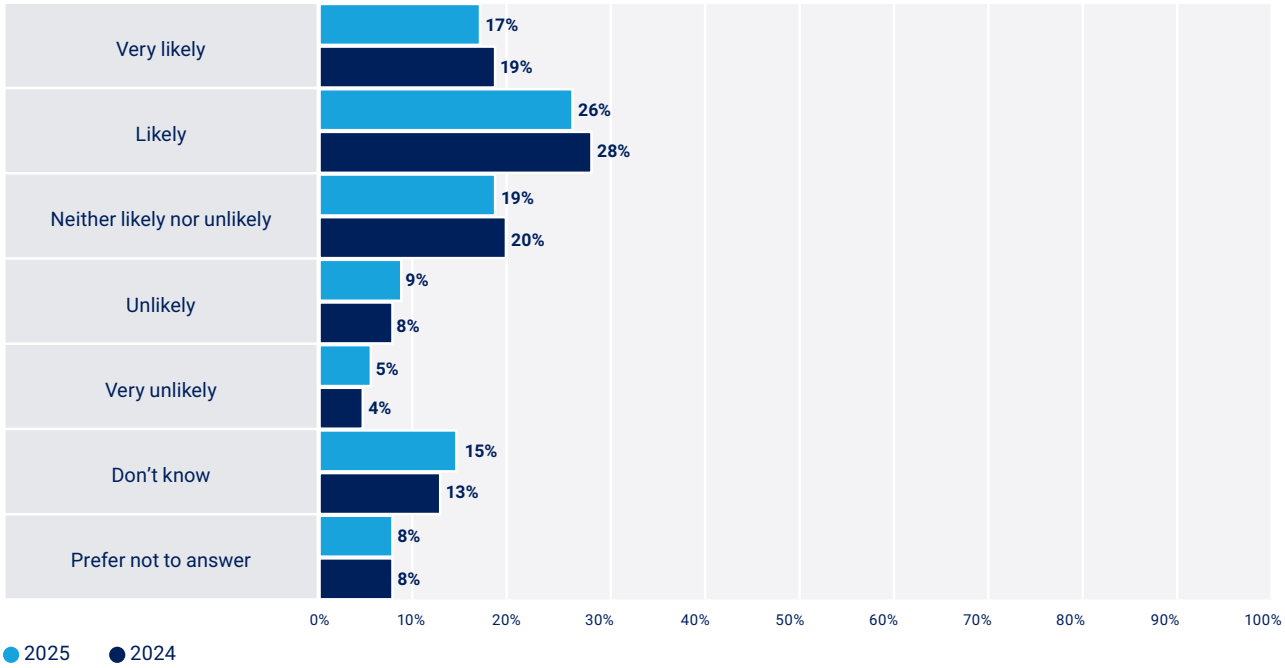


FIGURE 22: Likelihood of a Cyberattack

How likely is it that your organization will experience a cyberattack next year?

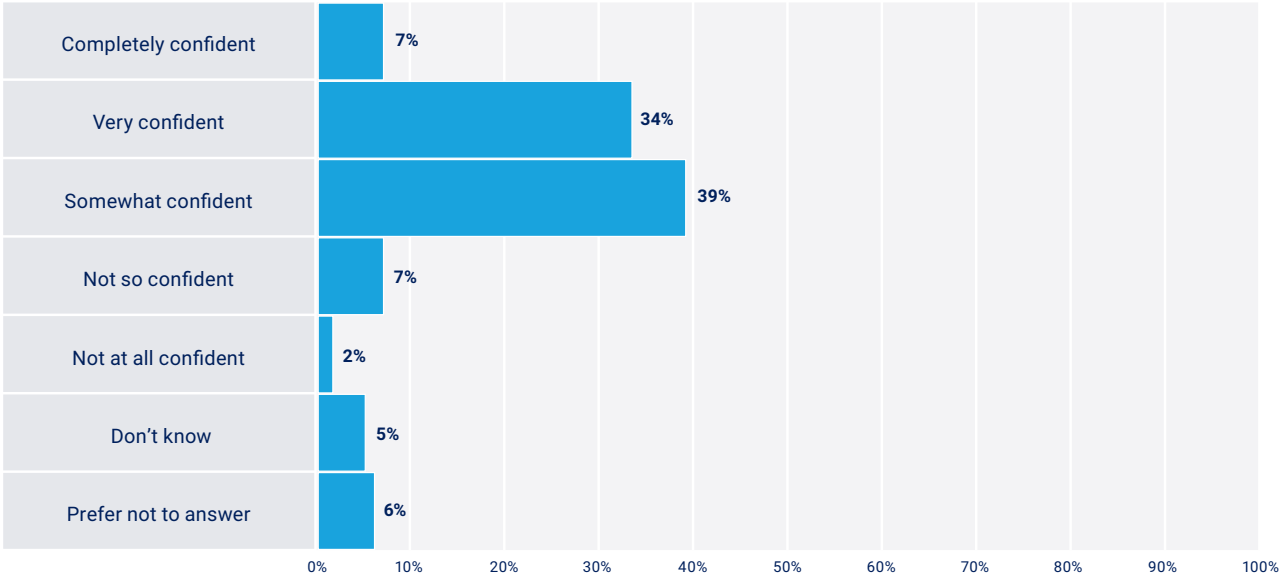


Despite the many respondents who think a cyberattack is likely in the next year, it is concerning that only 41% of respondents are completely or very confident in their cybersecurity team's ability to detect and respond to cyberthreats (**figure 23**). Note that respondents at enterprises with more resources tend to feel more confident—52% of respondents whose cybersecurity budgets are overfunded and 53% of respondents whose budgets are adequately funded are completely or very confident in their cybersecurity team's ability to detect and respond to threats. Fifty-three percent of respondents who believe that their cybersecurity teams are appropriately staffed are completely or very confident in their ability to detect and respond to cyberthreats. Fifty percent of respondents in enterprises with more than 10,000 employees are completely or very confident in their cybersecurity team's ability to detect and respond to cyberthreats.

A majority of respondents feel that cybercrime is underreported. Thirty-nine percent say that most enterprises underreport cybercrime even if they are required to report it, and 17% say that enterprises underreport cybercrime even if they are not required to report it. Just under one-quarter of respondents (23%) believe that cybercrime is accurately reported. These findings help with understanding why 29% of respondents say that integrity/honesty is an important soft skill for security professionals—not reporting cybercrime, especially when required, raises questions about ethics and integrity.

FIGURE 23: Confidence in Detecting and Responding to Cyberthreats

How confident are you overall in your organization's cybersecurity team's ability to detect and respond to cyberthreats?



Many enterprises have cyberinsurance in the event of a cybersecurity incident, but many respondents report that their enterprise has never used its cyberinsurance policy (**figure 24**). The percentage of respondents who say that they have used their cyberinsurance policy is two points lower than last year. Other industry research also supports a slight decline in the percentage of cyberinsurance claims.[10]

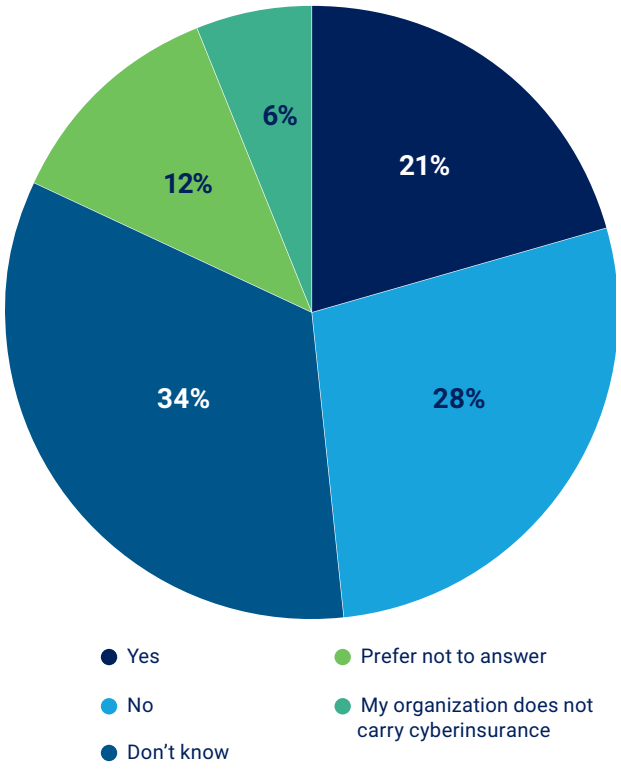
Cyberrisk Assessments

The percentage of survey respondents who perform cyberrisk assessments monthly increases from 8% in 2024 to 11% in 2025 (**figure 25**).

Nine percent of respondents who are not so confident or not at all confident in their enterprise cybersecurity team's ability to detect and respond to cyberthreats never perform cyberrisk assessments. Not performing cyberrisk assessments can explain why confidence in responding to threats is low in these enterprises.

FIGURE 24: Use of Cyberinsurance Policy

Has your organization ever used its cyberinsurance policy?



10 Araullo, K.; "Ransomware still costly, but cyber claims down – Coalition," Insurance Business, 8 May 2025, www.insurancebusinessmag.com/us/news/cyber/ransomware-still-costly-but-cyber-claims-down--coalition-534994.aspx

Among respondents whose enterprise cybersecurity strategy is not aligned with enterprise objectives, the percentage of respondents who never perform cybersecurity risk assessments jumps to 10%, indicating a correlation between cybersecurity posture and alignment with other enterprise priorities.

Figure 26 lists the obstacles that enterprises face in conducting cyberrisk assessments. Time commitment and not having enough personnel remain the top two obstacles but are slightly down from last year, when they were 41% and 37%, respectively.

FIGURE 25: Frequency of Cyberrisk Assessments

How often is a cyberrisk assessment performed on your organization?

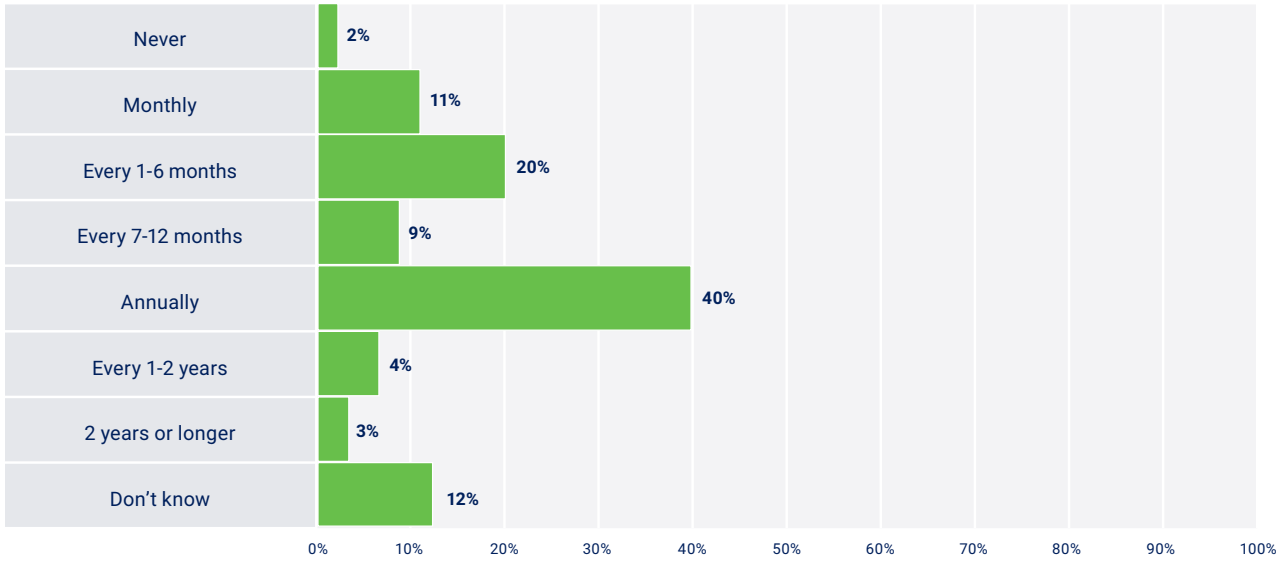
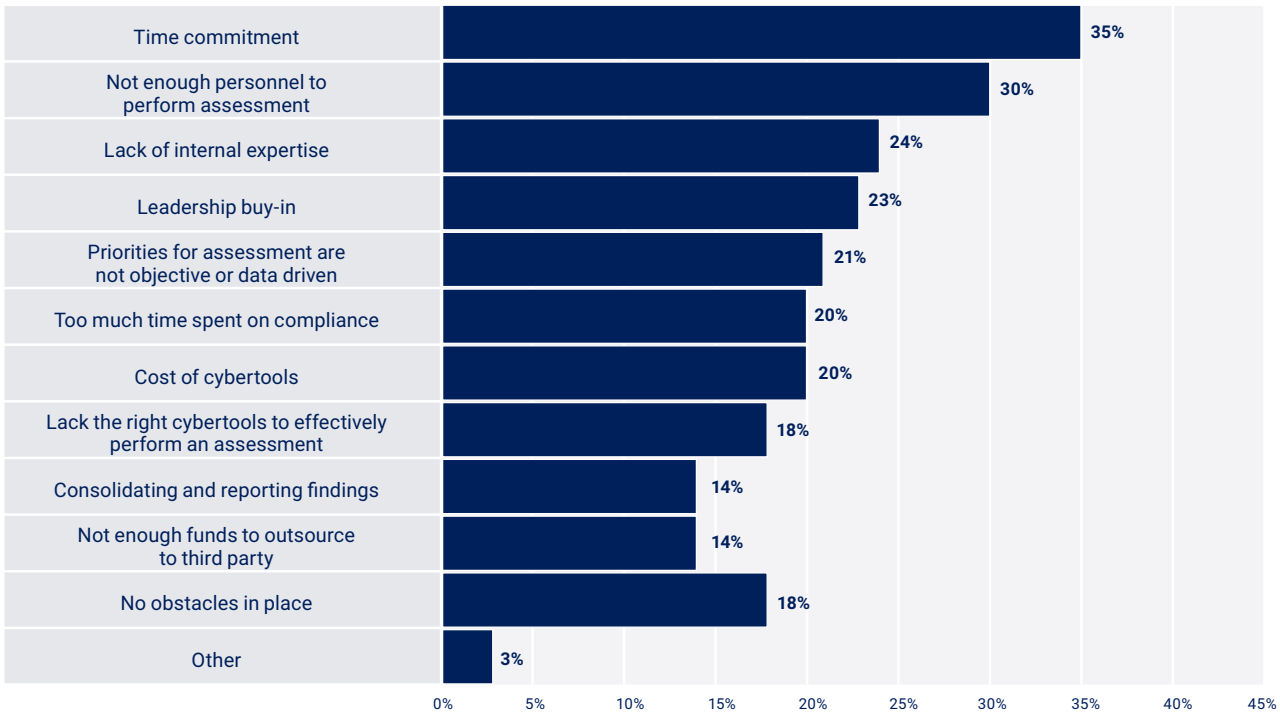


FIGURE 26: Obstacles to Conducting Cyberrisk Assessments

Which, if any, obstacles does your organization face in conducting a cyberrisk assessment?



AI and Cybersecurity

The use of AI tools for security operations has increased from last year (**figure 27**).

Forty percent of respondents indicate that they, or someone from their team, was involved in the development, onboarding, or implementation of AI solutions, which is considerably higher than last year (29%) (**figure 28**).

Almost half of respondents also say that they (or their team) were involved in the development of a policy that governs the use of AI in their enterprise, which is significantly higher than in 2024 (**figure 29**). This upward trend is reason for cautious optimism—enterprises seem to understand the value and importance of having cybersecurity input on AI, hinting at more secure and responsible AI implementation in the future.

The adoption of AI tools may correlate with cybersecurity maturity. Among respondents whose enterprises never conduct cyberrisk assessments, 44% say that they do not use AI for any of the tasks that are listed in the survey. This finding suggests that enterprises understand the possible risk associated with using AI, and if they do not have the bandwidth for cyberrisk assessments, they do not want to take on the risk associated with AI tools used for cybersecurity purposes.

FIGURE 27: Use of AI for Security Operations

Does your organization use artificial intelligence (AI) in any of the following security operations?

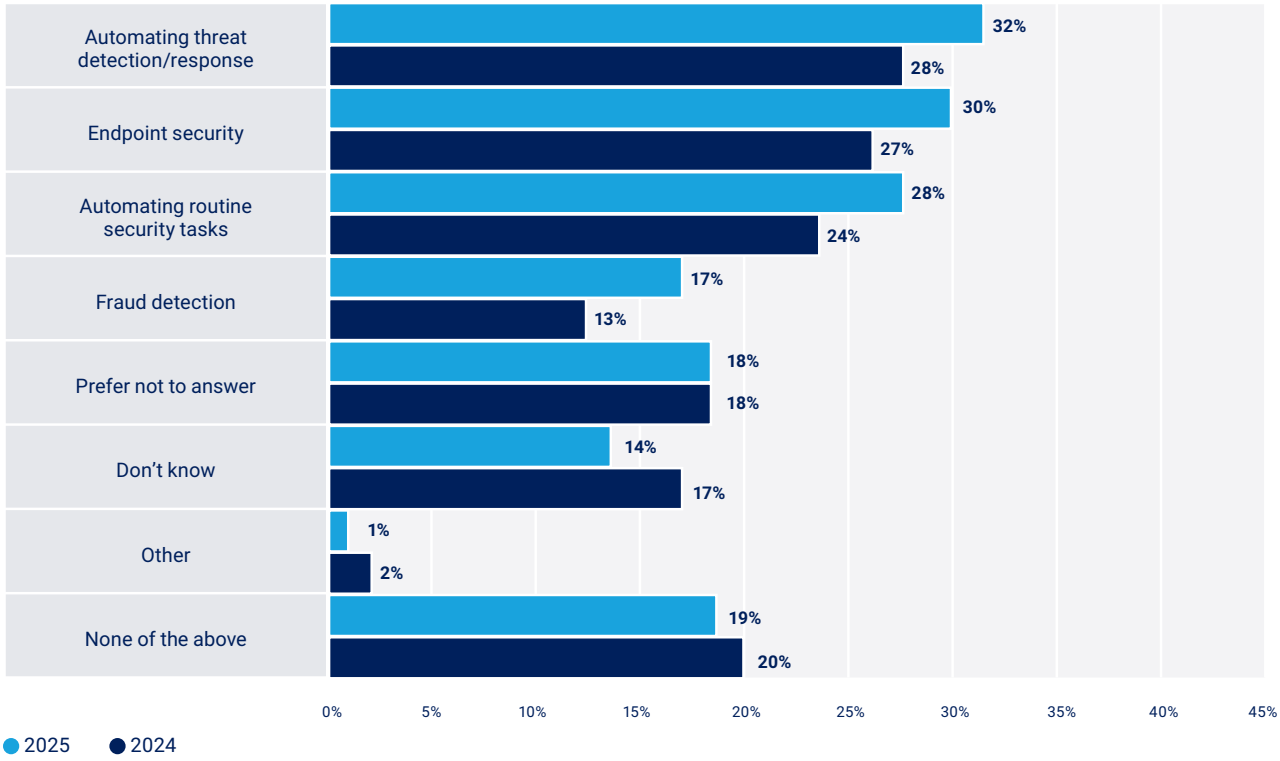


FIGURE 28: Involvement in AI Life Cycle

Were you, or anyone on your team, involved in the development, onboarding, or implementation of AI solutions?

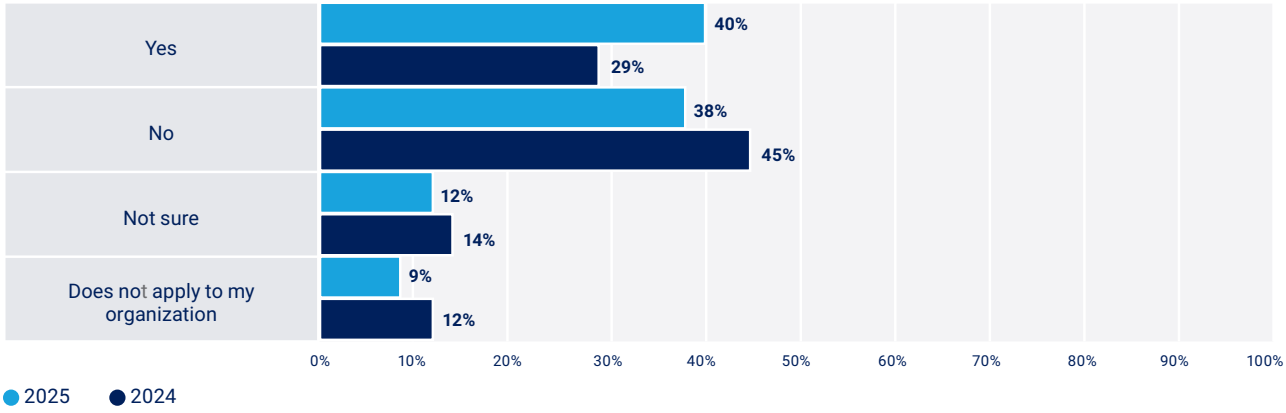
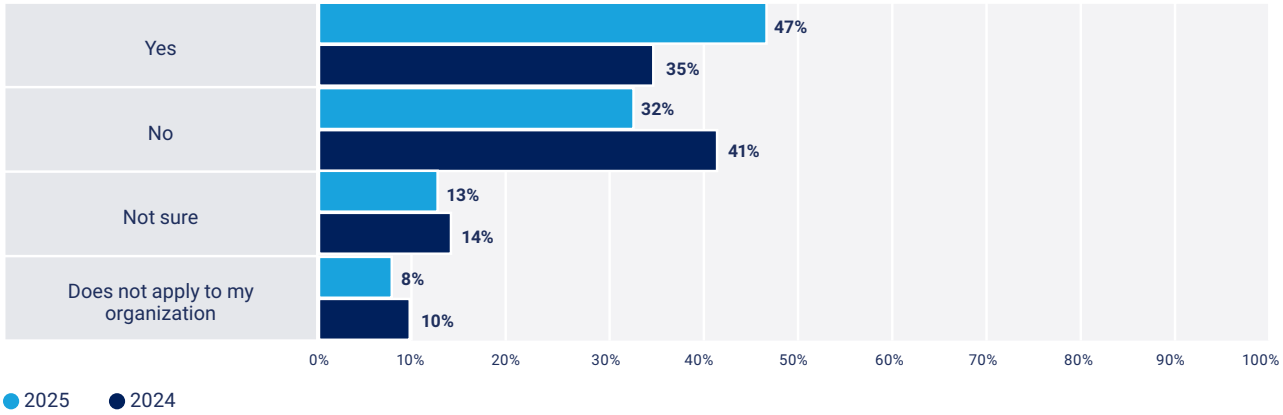


FIGURE 29: Involvement in Developing AI Policy

Were you, or anyone on your team, involved in the development of a policy governing the use of AI technology in your organization?



Almost half of respondents say that they (or their team) were involved in the development of a policy that governs the use of AI in their enterprise, which is significantly higher than in 2024. This upward trend is reason for cautious optimism—enterprises seem to understand the value and importance of having cybersecurity input on AI, hinting at more secure and responsible AI implementation in the future.

Conclusion: Preparing for an Uncertain Future

Although many findings from this year's *State of Cybersecurity Survey* are similar to those reported last year, some findings have potentially troubling implications for the future of the cybersecurity workforce. Burnout remains a considerable challenge, so it is concerning that almost one-quarter of respondents say their enterprises have not taken any action to mitigate burnout. Despite many respondents reporting that their jobs are more stressful now than in previous years, the job market and broader economic uncertainty has helped enterprises with retention.

Although talent shortages are not a significant problem now, an aging cybersecurity workforce paints a troubling picture—many experienced cybersecurity professionals are approaching retirement age, and there may not be enough younger professionals to compensate for this potential talent exodus. Enterprises should consider succession planning now to avoid business continuity issues in the future.

Despite technical cybersecurity professionals being in high demand, enterprises are doing less, compared to past year, to address technical cybersecurity skill gaps. Fewer enterprises are allowing noncybersecurity professionals to move into cybersecurity roles. Using outside contractors or consultants is now the primary method for combatting technical skill gaps, but even the percentage of enterprises using that method is down from 2024. These changes may be indicative of the Big Stay—the continuing trend of technical cybersecurity staff staying in their roles longer, reducing the need for addressing technical skill gaps. This reasoning is supported by the slight decline in respondents who say that the demand for individual technical cybersecurity professionals will increase.

The use of AI may help to alleviate some of the stress cybersecurity teams are experiencing, but broader enterprise use of AI has also created additional work for cybersecurity staff. They are increasingly expected to be involved with implementing AI solutions and AI-related policy development. The involvement of cybersecurity staff with this technology will, ideally, help to ensure that AI solutions are implemented safely, securely, and responsibly.

Board support remains a key driver of cybersecurity team success. Board support of cybersecurity is correlated with more resources, better staffing, and fewer retention challenges. It is vital that cybersecurity professionals know how to communicate the importance of their work to those who may not have technical knowledge. Survey findings show that soft skills, especially communication, are lacking among many cybersecurity professionals; therefore, it is understandable that boards may not understand the value of providing resources to cybersecurity departments. Cybersecurity leaders who can advocate for the important work of their teams may be able to garner board support, potentially resulting in more resources and better talent retention.

Acknowledgments

Lead Developer

An ISACA Staff Publication

About ISACA

ISACA® (www.isaca.org) champions the global workforce advancing trust in technology. For more than 55 years, ISACA has empowered its community of 185,000+ members with the knowledge, credentials, training and network they need to thrive in fields like information security, governance, assurance, risk management, data privacy and emerging tech. With a presence in more than 190 countries and with nearly 230 chapters worldwide, ISACA offers resources tailored to every stage of members' careers—helping them to thrive in a rapidly changing digital landscape, drive trusted innovation and ensure a more secure digital world. Through the ISACA Foundation, ISACA also expands IT and education career pathways, fostering opportunities to grow the next generation of technology professionals.

DISCLAIMER

ISACA has designed and created *State of Cybersecurity 2025: Global Update on Workforce Efforts, Resources, and Cybersecurity Operations* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome.
The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA
1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

X: www.x.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/