ISACA

TeamMate® by Wolters Kluwer

State of Cybersecurity 2026

Global Update on Workforce Efforts, Resources, and Cybersecurity Operations

Security

CONTENTS

ABSTRACT

State of Cybersecurity 2026: 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 2026. 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 consistent from year to year, other survey findings reveal significant changes in cybersecurity operations and broader workforce trends.

Executive Summary

The twelfth 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. Respondents to this year's survey have concerns about cybersecurity impacts from AI and the increasing skill gaps among cybersecurity professionals.

Key findings include:

- Stress in the cybersecurity workforce remains elevated. Sixty-eight percent of survey respondents report that their roles have become more stressful over the past five years. This is a slight increase from 66% in 2024 and 2025. The primary driver is the increasingly complex threat landscape. The percentage of respondents identifying this driver increases from 63% in 2025 to 71% in 2026. This is a change from the 18 percentage-point drop for this stress driver from 2024 (81%) to 2025 (63%).
- Soft skills remain the most significant skill gap in cybersecurity professionals, although the percentage of enterprises reporting this gap deceases this year (59% in 2025, and 57% in 2026). Survey respondents report LLM SecOps as the second largest skill gap (45%), up sharply from 33% in 2025.
- The top five most important security skills have shifted this year. Data security retains its top spot, but cloud computing is replaced by incident response in the top five. Priority technical skills focus on core risk reduction—data security (56%), threat detection and response (54%), vulnerability management (53%), identity and access management (51%), and incident response (49%).
- Respondents indicate the same most important soft skills needed by security professionals as last year, but the percent indicating the need for these skills has increased. The top five soft skills are critical thinking (59%), communication (57%), problem-solving (53%), teamwork (47%), and adaptability/flexibility (43%).
- AI adoption in security operations is accelerating, but the maturity of AI governance and incident response activities remain at a much lower level. Leading use cases for AI in security operations include automating threat detection and response (41%), automating routine security tasks (40%), and endpoint security (33%). Thirteen percent of enterprises do not yet use AI in security operations.
- AI-related preparedness is not keeping pace with adoption. Only 8% of enterprises conduct AI-related incident response exercises on a regular basis, creating a readiness gap as AI becomes normalized within security operations and adversarial tactics.

Survey Methodology

In the second quarter of 2026, ISACA sent online survey invitations to a global population of cybersecurity professionals who hold the ISACA Certified Information Security Manager® (CISM®) certification or who have registered job titles in the information security field and are ISACA members.

The survey contains questions across the following areas:

- Staffing and skills
- Security operations
- AI
- Cybersecurity budgets
- Cyberattacks and cyberthreats
- Cyberrisk and obstacles

A total of 1,888 respondents completed the survey in its entirety, and their responses are included in this 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.

Fifty-six percent of all respondents indicate that cybersecurity is their primary professional area of responsibility.

Figure 1 shows the demographic information of survey respondents, and **figure 2** features the industries represented.

FIGURE 1: Respondent Demographics

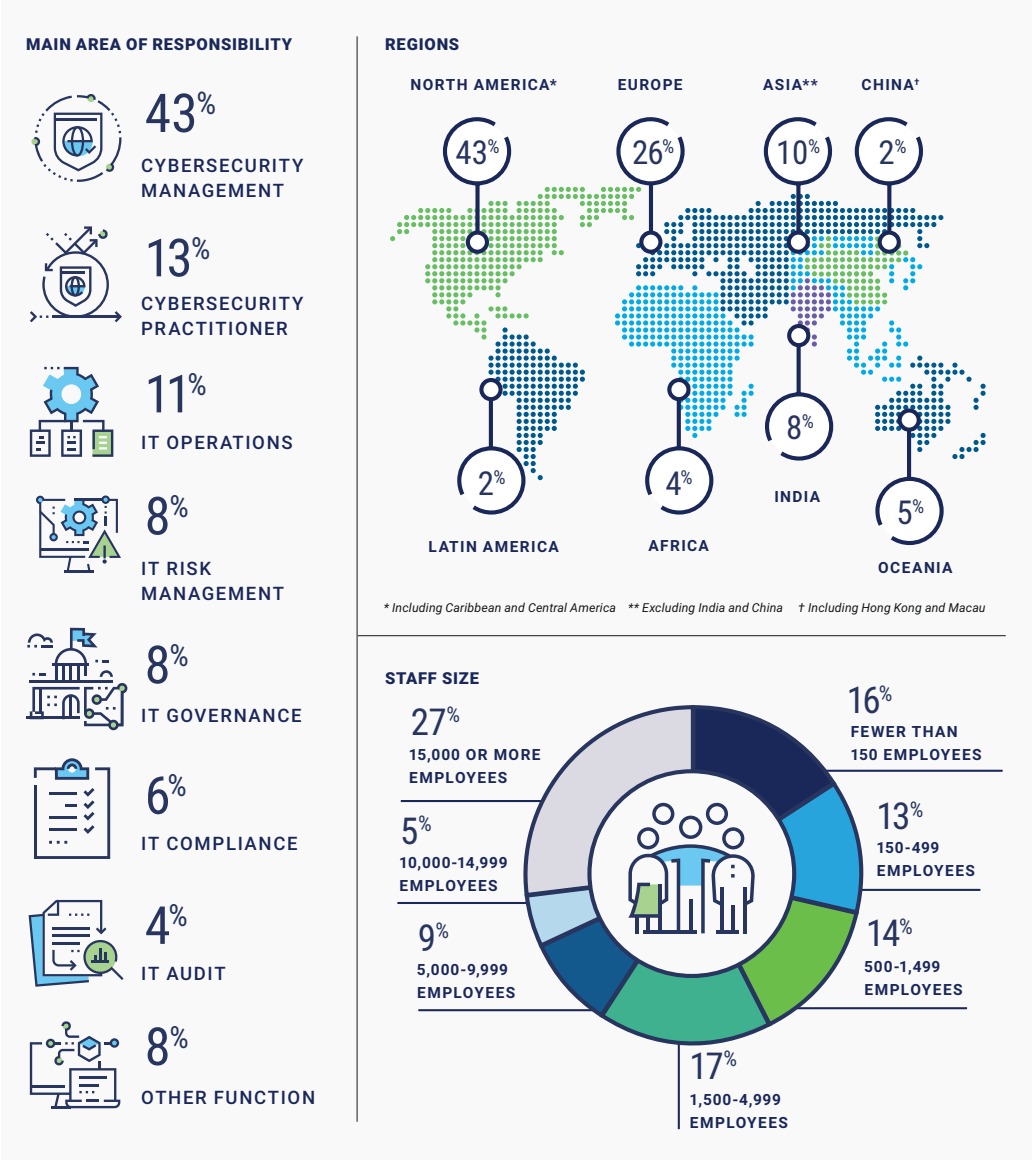
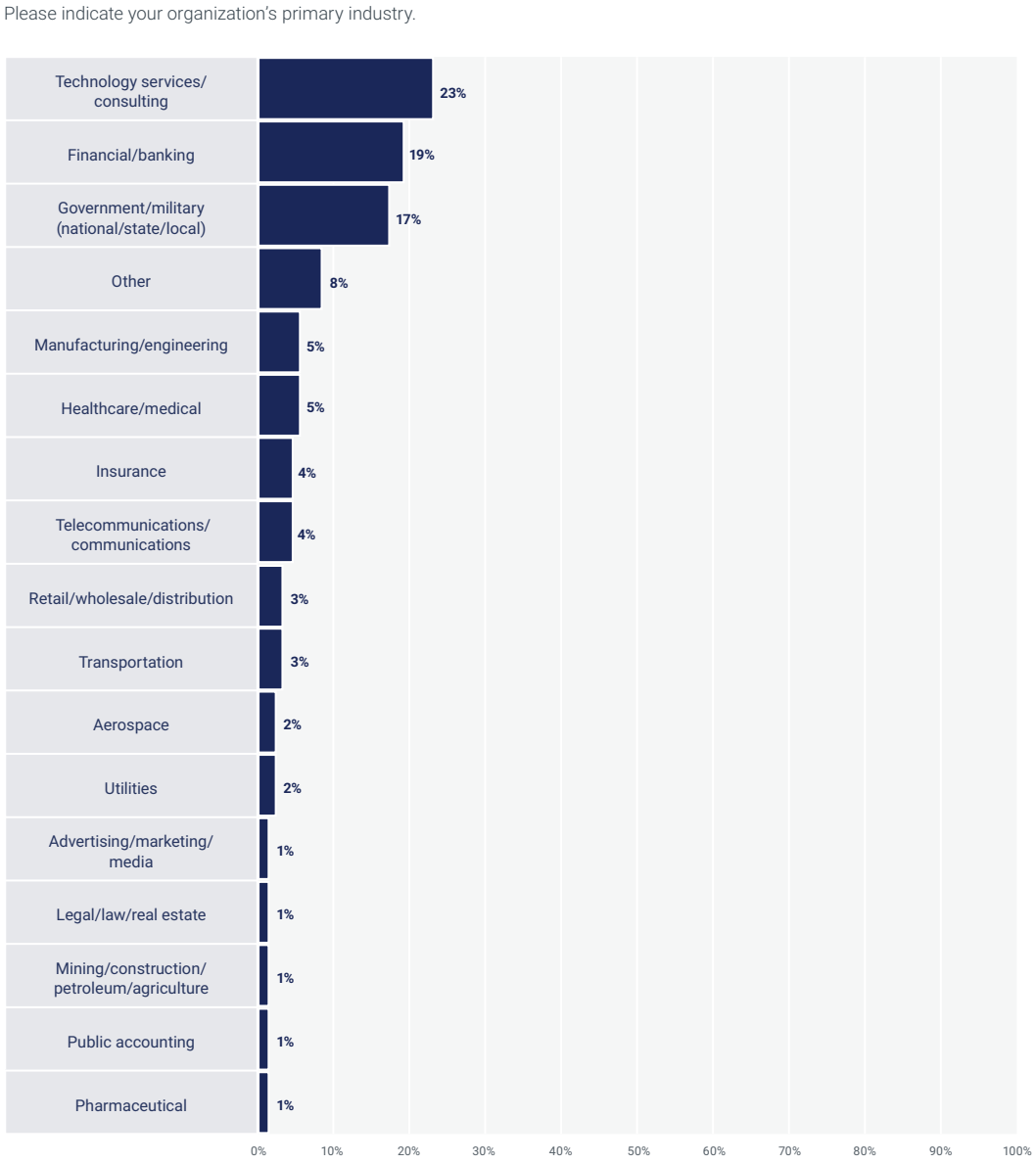


FIGURE 2: Industries Represented



Cybersecurity Workforce Considerations

As in prior years, cybersecurity staffing is a concern for an increasing majority of respondents. Fifty-eight percent reported that their cybersecurity team is understaffed—a slight increase from 55% last year.

Respondents at enterprises with 500 to 10,000 employees were more likely to report cybersecurity staffing shortages, with 60% saying their cybersecurity team is significantly or somewhat understaffed.

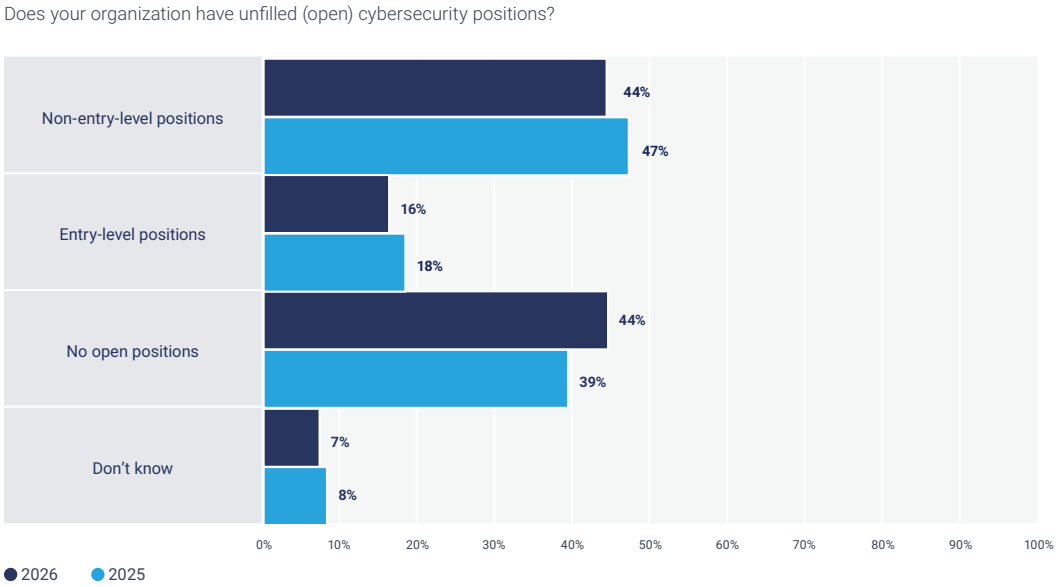
The share of respondents who believe their cybersecurity team is appropriately staffed or overstaffed is similar to the last two years. The median security staff size remains unchanged at eight employees.

Hiring and Open Roles

Just under half (49%) of respondents reported that their enterprises had unfilled cybersecurity positions. It is notable that enterprises reporting no openings rose 5% from last year. **Figure 3** shows the percentage of enterprises with open cybersecurity roles and the levels of those roles. The percentage of enterprises with open entry-level positions dropped 2 percentage-points from 2025, and open non-entry-level positions dropped 3 percentage-points.

Finding the most qualified candidate for a cybersecurity role continues to take a significant amount of time, regardless of the position level. For entry-level roles, 38% of respondents said it typically takes three to six months to hire a qualified candidate, while 12% said the process takes more than six months on average.

FIGURE 3: Open Roles



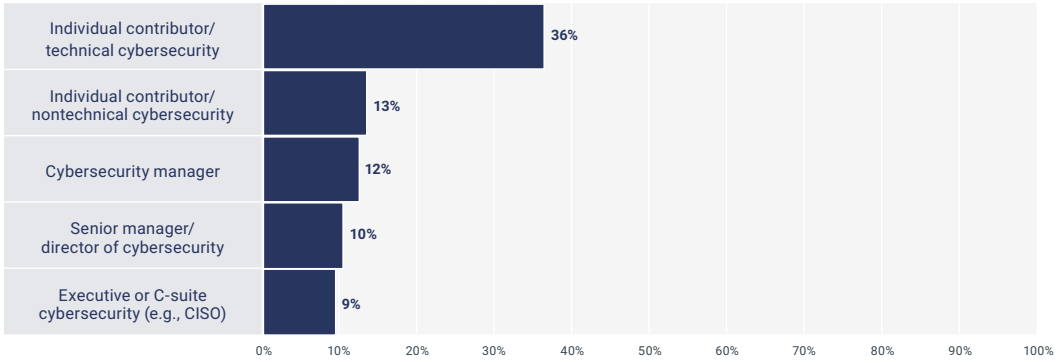
The hiring timeline is slightly longer for non-entry-level roles. Among respondents, 40% reported that the time to fill these positions with a qualified candidate is three to six months, and 24% said that it takes more than six months. Regional differences emerged in the survey results: 28% of respondents in Asia and 30% in Europe reported that filling non-entry-level roles takes longer than 6 months.

Regarding overall hiring timelines for open cybersecurity positions, 22% of respondents said the time to fill roles has increased, 44% said it has remained the same, and 17% said it has decreased. These results changed slightly compared to last year, when 21% reported an increase, 43% said that the timeline stayed the same, and 17% said it decreased.

Figure 4 shows the levels at which respondents reported having most or all unfilled cybersecurity positions.

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."



Attracting applicants with the required cybersecurity expertise remains difficult for many enterprises. Only 31% of survey respondents said that most cybersecurity applicants are well qualified for the roles they seek, and 23% of respondents reported that 25% or fewer applicants meet their standard.

Figure 5 shows the factors that cybersecurity professionals consider to be very important in determining a candidate's qualifications. Survey respondents said that candidates need to be adaptable (67%), have prior cybersecurity work experience (62%), and fit in with the organization (61%). The next highest factor for qualified candidates was holding credentials (34%).

The power of networking is also evident in the results. Eighteen percent of respondents said that a referral from someone other than a previous employer is very important to them when determining if a candidate is qualified for an open role—slightly more important than a recommendation from a previous employer. A networking referral is especially important because AI screening of candidates has increased rapidly, and studies reveal that some screening practices appear to be biased and, in some cases, prohibitive to candidate advancement.[1]

A networking referral is especially important because AI screening of candidates has increased rapidly, and studies reveal that some screening practices appear to be biased and, in some cases, prohibitive to candidate advancement.

There is a considerable gap between the top three most desired factors and the remaining factors, indicating that adaptability, previous cybersecurity work experience, and organizational fit are better indicators of qualification than some other factors.

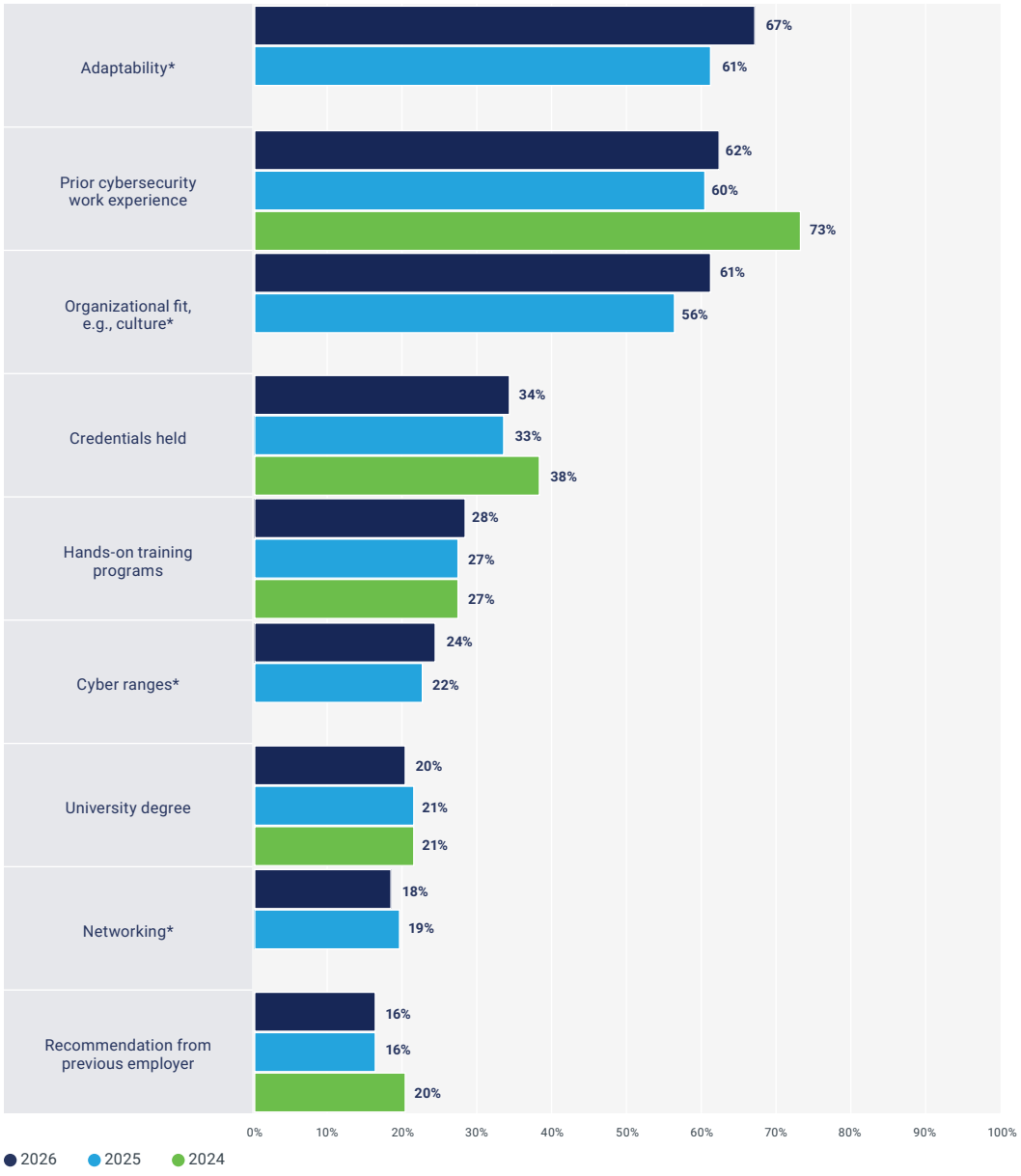
The anticipated demand for cybersecurity positions varies based on seniority level. As shown in **figure 6**, the demand for individual technical cybersecurity professionals is most likely to increase.

Adjustments to nontechnical practitioners and management levels can be attributed to AI use, human oversight of AI implementations in security operations, and the need for more technical contributors to engineer and maintain pace with enhanced adversary activity.[2]

1 Bommasani, R.; Bana, S.; et al.; "Algorithmic Monocultures in Hiring," *Proceedings of the 2026 ACM Conference on Fairness, Accountability, and Transparency*, 2026, https://digitaleconomy.stanford.edu/publication/algorithmic-monocultures-in-hiring/
2 Salvi, V.; "How AI Could Open up Cybersecurity to a Wider Workforce," World Economic Forum, 5 May 2026, www.weforum.org/stories/cybersecurity/how-ai-could-open-up-cybersecurity-to-a-wider-workforce/

FIGURE 5: Factors Indicating Candidate Qualification

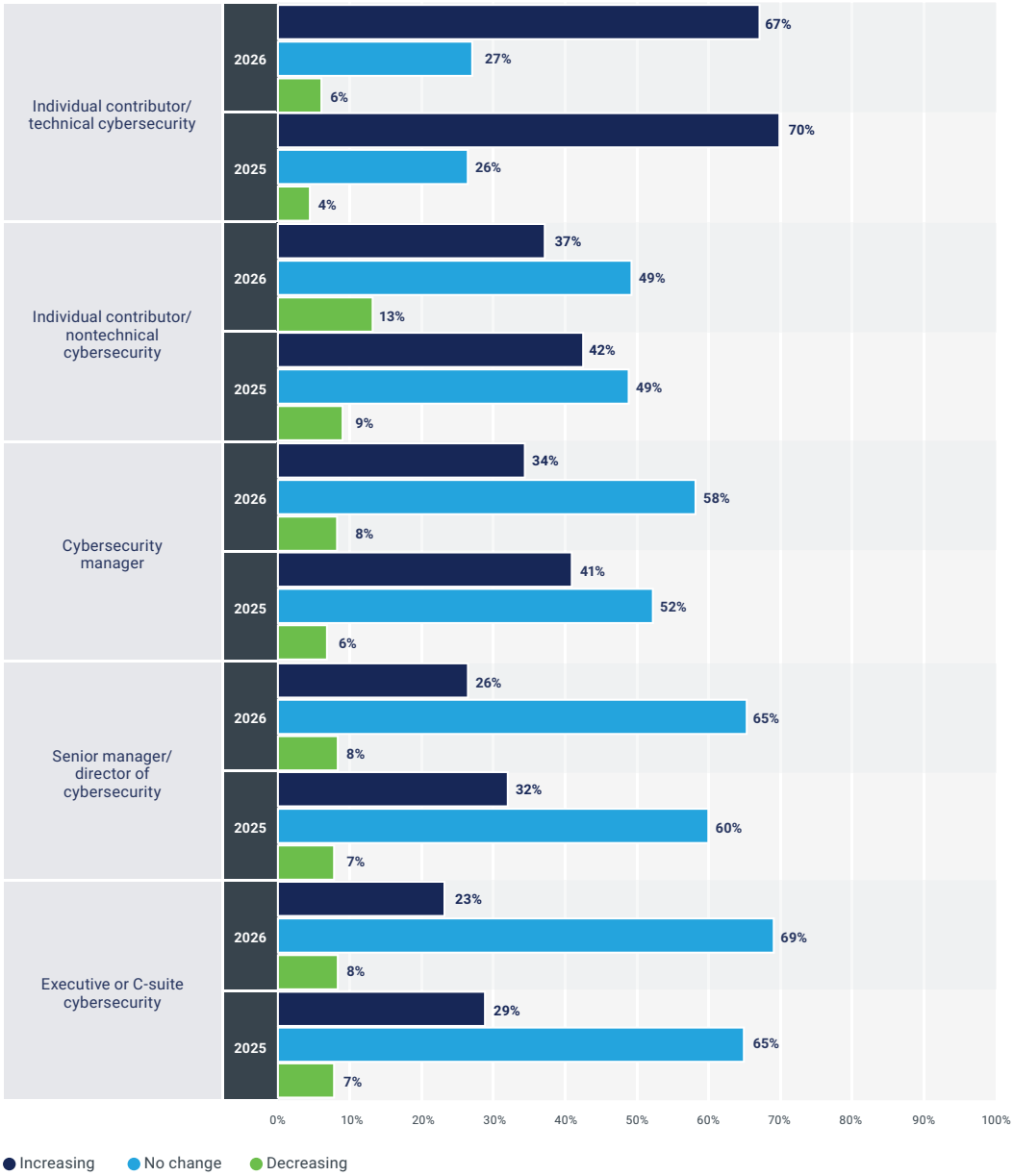
How important are each of the following factors in determining if a cybersecurity candidate is qualified? Percentages represent respondents indicating these factors as "very important."



*New factor in 2025 survey

FIGURE 6: Anticipated Demand for Cybersecurity Positions

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

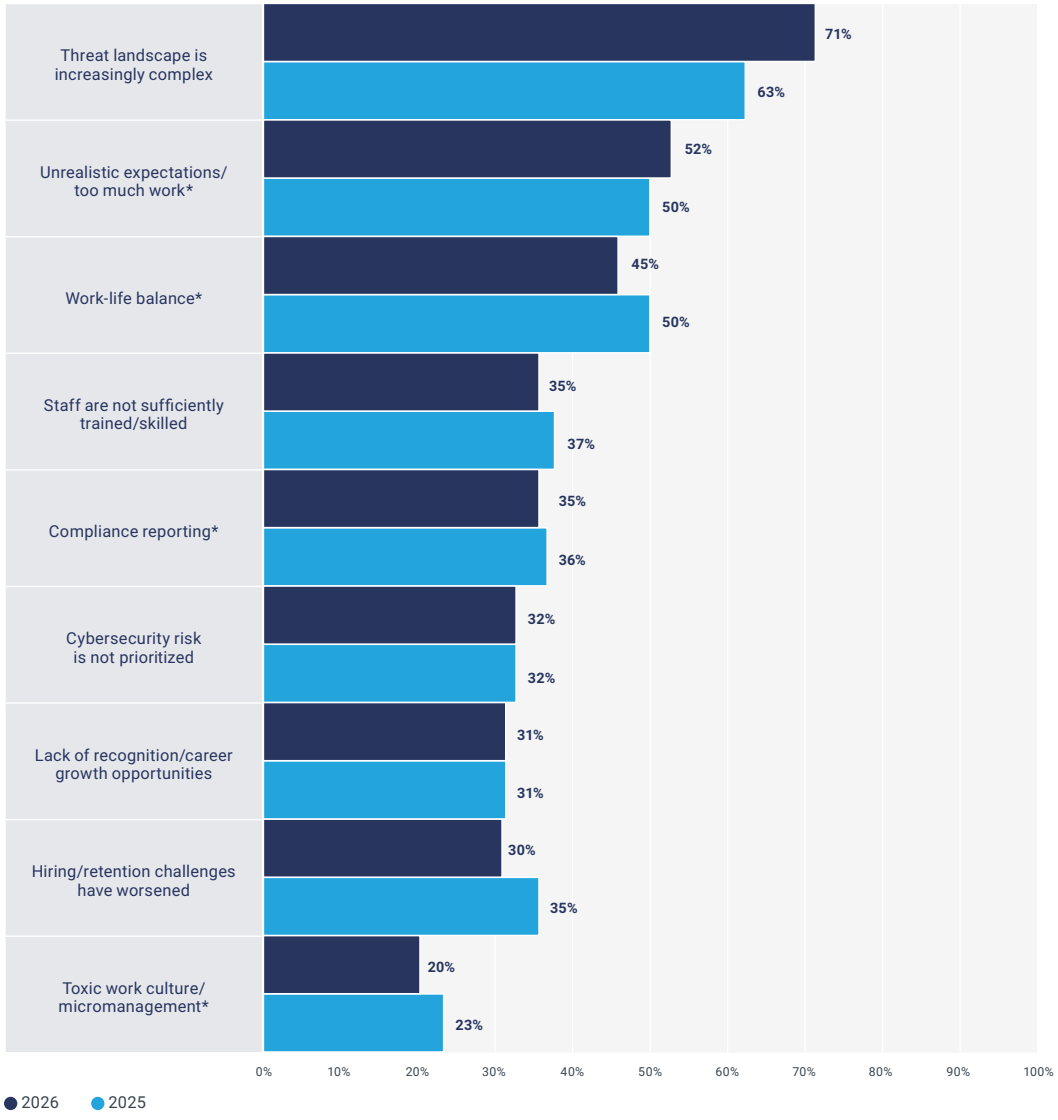


Burnout and Retention

Most survey respondents indicate that their roles are more stressful now than they were five years ago, which is consistent with last year's findings. Forty percent of respondents said that their role is "significantly more stressful" now than it was five years ago, compared to 37% last year. **Figure 7** outlines the reasons why cybersecurity jobs feel more stressful today.

FIGURE 7: Sources of Job Stress

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



*New option in 2025 survey

An increasingly complex threat landscape remains the prominent stress factor (71%), and its impact is escalating again after dropping in 2025.

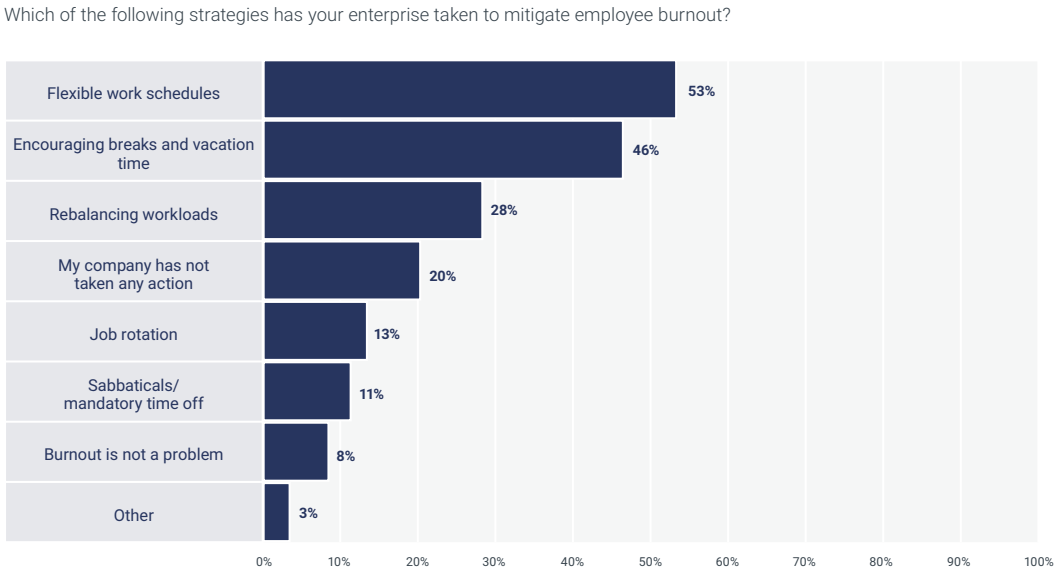
Work-life balance as a stress factor was 5% lower this year, which could indicate employers are helping employees better balance their time. Hiring and retention challenges (30%) continue to trend favorably, showing a five percentage-point improvement over 2025 and a 15 percentage-point drop from 2024.

Employee burnout due to high stress levels is a concern for many enterprises.

Employee burnout due to high stress levels is a concern for many enterprises.

Survey respondents reported that their employers primarily address workplace stress in two ways—flexible work schedules (53%) and encouraging breaks and vacation time (46%) (**figure 8**). Although health studies[3] often recommend increased rest and vacations to reduce stress and refocus efforts, the time allotted for this solution varies across geographic regions.[4]

FIGURE 8: Employee Burnout Mitigation



The percentage of respondents reporting difficulty in retaining qualified cybersecurity professionals increased to 55% (**figure 9**). This result shows a change in the trend of steadily dropping retention difficulty reported from 2022 (60%) through 2025 (50%). Given that job markets can vary globally, there are some regional differences in retention difficulties (**figure 10**). North America has the fewest challenges with retention, while it is a considerable obstacle for respondents in Africa, Latin America, and Asia.

3 Giridharan, S.; Pandiyan, B.; "Maximizing Recovery: The Superiority of Frequent Vacations for Well-Being and Performance," *Cureus*, vol. 17, iss. 7, 2025, www.cureus.com/articles/385949-maximizing-recovery-the-superiority-of-frequent-vacations-for-well-being-and-performance

4 Equal Futures, "Paid Annual Leave and a Weekly Day of Rest," Foundations for an Equal Future Brief Series, June 2026, https://www.equalfutures.org/sites/default/files/2026-06/EqualFutures_RightToPaidTimeOff_30Jun26.pdf

FIGURE 9: Retention Difficulties (2020-2026)

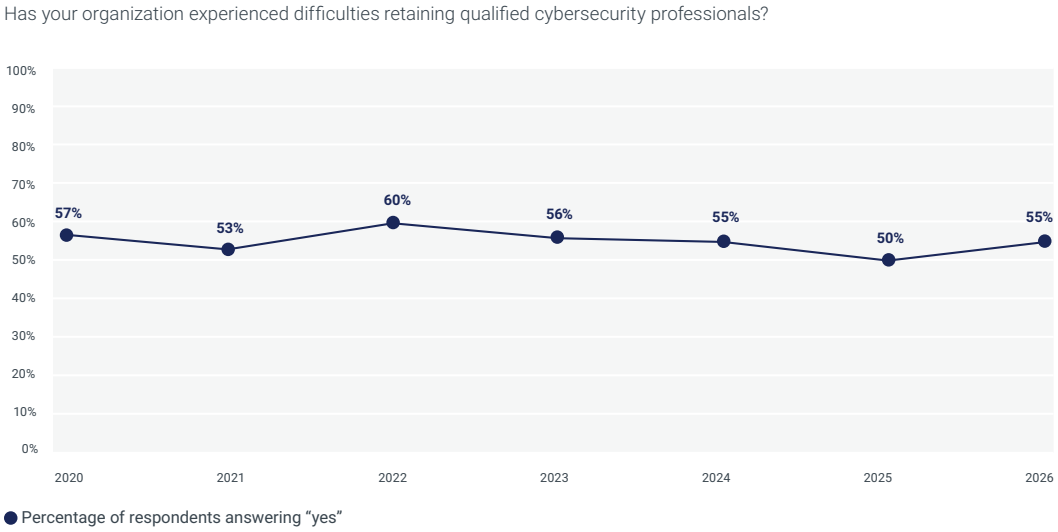
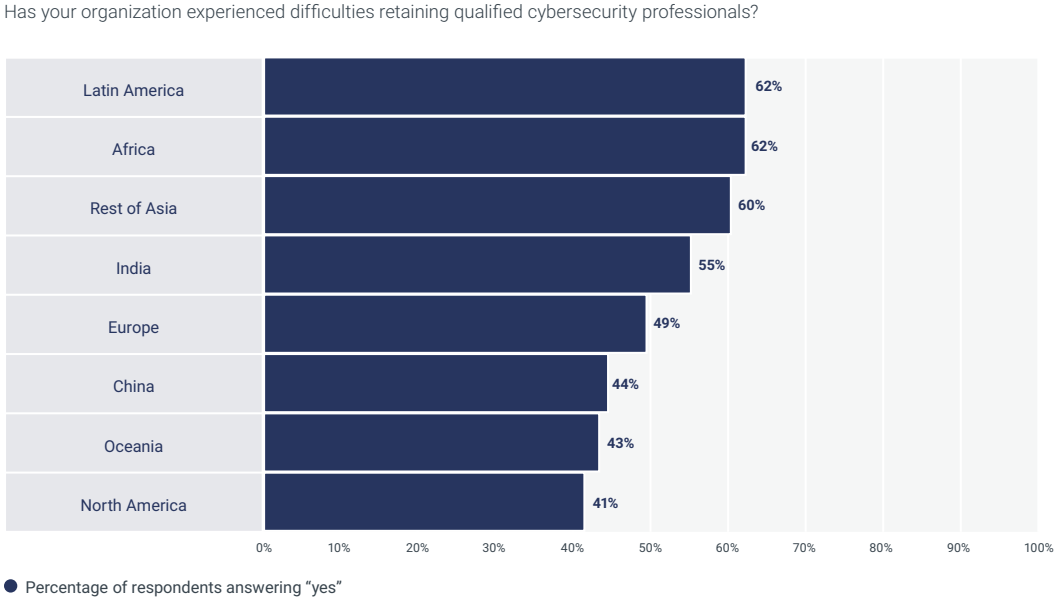


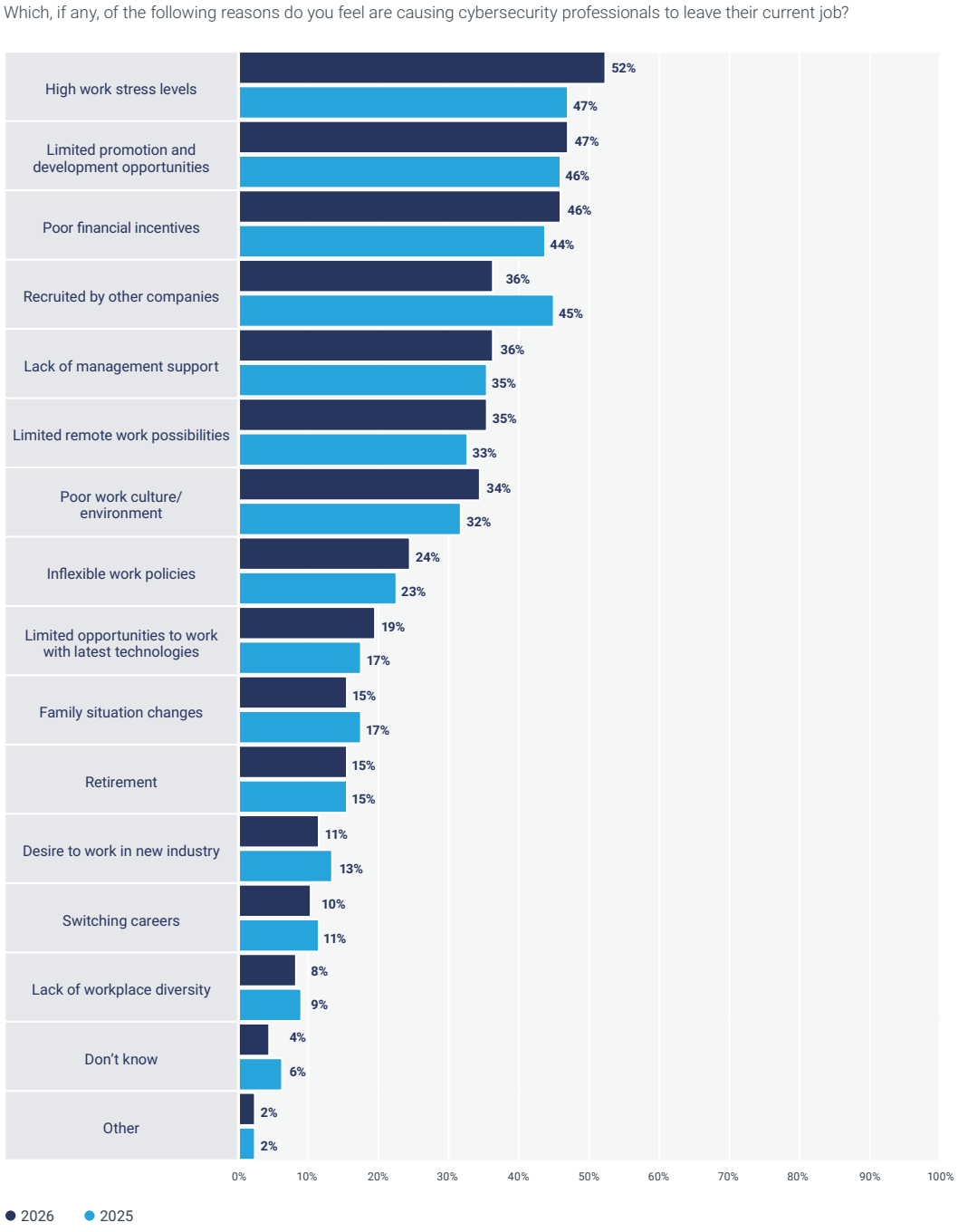
FIGURE 10: Retention Difficulty by Region



The nature of cybersecurity work can create demanding environments, as practitioners are often expected to remain attentive to potential adversary activity.[5] The top three reasons why cybersecurity professionals choose to leave their jobs are high work stress (52%), limited promotion and development opportunities (47%), and poor financial incentives (46%). Thirty-five percent of respondents said that a lack of remote work options caused talent to leave. **Figure 11** shows the full list of reasons why cybersecurity professionals may leave their jobs.

5 Nobles, C.; "Stress, Burnout, and Security Fatigue in Cybersecurity: a Human Factors Problem," *HOLISTICA – Journal of Business and Public Administration*, vol. 13, iss. 1, 2022, p. 49–72, https://www.semanticscholar.org/paper/Stress%2C-Burnout%2C-and-Security-Fatigue-in-A-Human-Nobles/3f00a50f9515f28b5469ee0fee394e4187ce0f7b

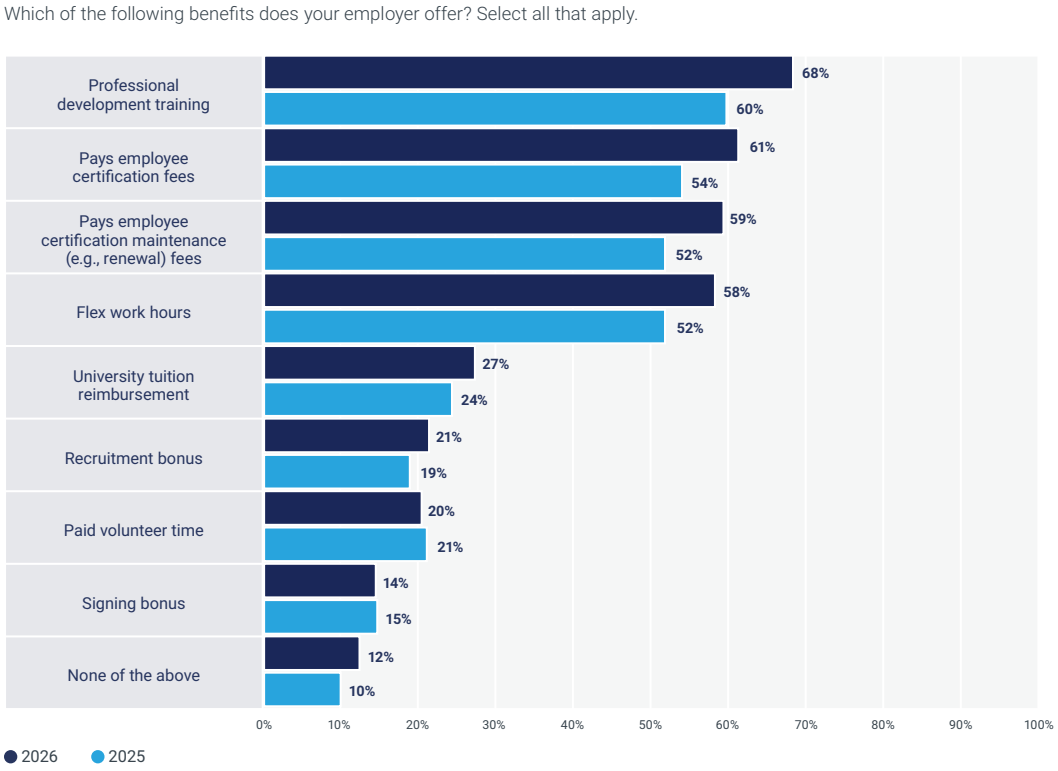
FIGURE 11: Reasons for Leaving Current Job



Across the full benefits that employers offer (**figure 12**), professional development and certification-related support are the most common and growing benefits. Professional development training increased from 60% in 2025 to 68% in 2026, certification fee coverage rose from 54% to 61%, and certification maintenance support increased from 52% to 59%.

Flexible work hours also grew from 52% to 58%, while tuition reimbursement, recruitment bonuses, paid volunteer time, and signing bonuses continue to be less commonly offered. Overall, the survey results suggest that employers are placing greater emphasis on skill development and credential support in their employee benefits strategy.

FIGURE 12: Employer Benefits



Upskilling, whether through professional development training or certification, remains a primary benefit offered to cybersecurity professionals.

Upskilling, whether through professional development training or certification, remains a primary benefit offered to cybersecurity professionals.

According to survey respondents, upskilling was funded through:

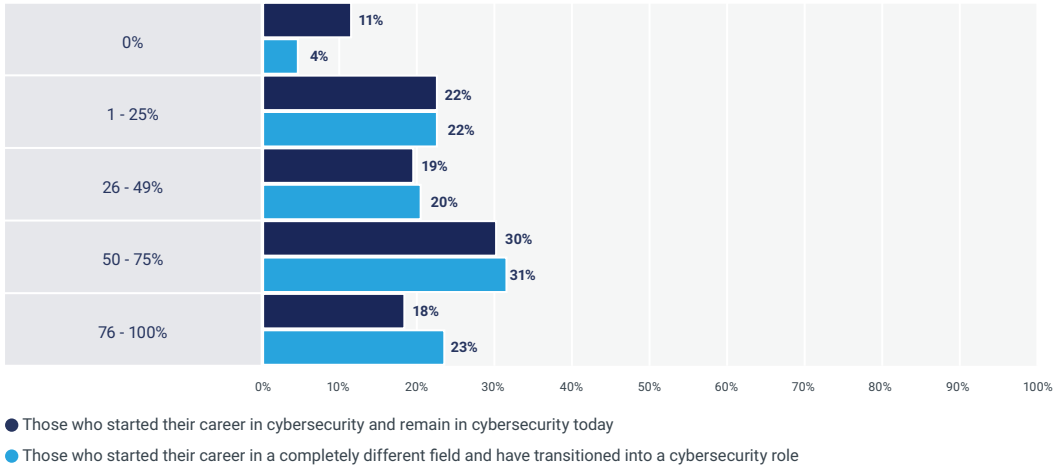
- Operational budget (40%)
- Both operational and HR budgets, depending on the circumstances (36%)
- HR budget (13%)

The Talent Pipeline

There are many options available in pursuit of a career in cybersecurity. Forty-eight percent of respondents said that half or more of their cybersecurity staff started their careers in cybersecurity and remain in the profession today, while 54% said that half or more of their cybersecurity staff started their careers in completely different fields and transitioned into cybersecurity roles (**figure 13**).

FIGURE 13: Cybersecurity Staff Backgrounds

What percentage of your cybersecurity staff is comprised of the following individuals?

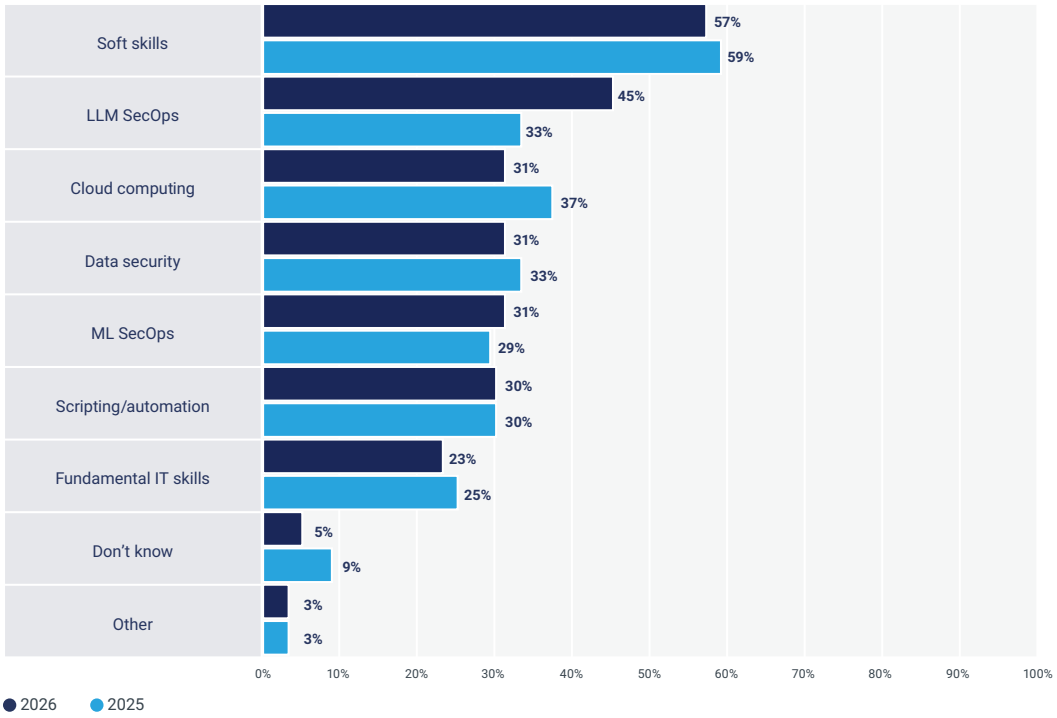


Skill Gaps

AI has significantly adjusted the skill gaps that survey respondents observe in cybersecurity professionals. In 2026, 45% reported that LLM SecOps was a skill gap, which is a 12 percentage-point increase from 2025 and a 21 percentage-point increase from 2024. At the top again this year, 57% of respondents identified soft skills as a significant skill gap in cybersecurity professionals (**figure 14**).

FIGURE 14: Skill Gaps in Today's Cybersecurity Professionals

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



Soft skills remain highly valued among security professionals.

Soft skills remain highly valued among security professionals.

The top five most important soft skills security professionals need are:

- Critical thinking: 59%
- Communication (listening, speaking, conflict resolution): 57%
- Problem solving: 53%
- Teamwork (collaboration and cooperation): 47%
- Adaptability/flexibility: 43%

Other important soft skills included self motivation (32%), integrity/honesty (32%), leadership (31%), work ethic (30%), attitude (28%), organization (25%), writing skills (16%), and empathy (12%).

To address these nontechnical skill gaps in cybersecurity professionals, enterprises are:

- Leveraging online learning websites (49%)
- Mentoring (40%)
- Providing corporate training events (32%)
- Offering academic tuition reimbursement (18%)

Twenty-two percent of respondents reported that their enterprises are doing nothing to address this skill gap, and 6% said their enterprises do not have nontechnical skill gaps.

Cybersecurity professionals must be well rounded in their development and expertise. The top five most important security skills identified by survey respondents are:

- Data security: 56%
- Threat detection and response technologies: 54%
- Vulnerability management: 53%
- Identity and access management: 51%
- Incident response: 49%

Figure 15 provides the full list of results.

In 2025, the top mitigation tactic used to address technical cybersecurity skill gaps was the use of contract employees (30%). This tactic dropped to third place this year (26%), continuing the decline seen from 2024 to 2025. Increased reliance on AI or automation took the lead in 2026—35% of respondents identified this mitigation tactic, which is a 12 percentage-point increase from last year. Training nonsecurity staff interested in moving to security roles remains in second place (27%). Other methods to address these gaps show little change from last year and include:

- Increasing use of reskilling programs (21%)
- Increasing use of performance-based training to attest to actual skill mastery (18%)
- Leveraging apprenticeships/internships (18%)
- Increasing reliance on credentials to attest to actual subject matter expertise (16%)

Over half of all respondents (54%) typically required entry-level cybersecurity professionals to have a university degree in 2026 (**figure 16**). Latin America showed a sharp 17 percentage-point decrease in required degrees this year. Perceptions of university graduates' preparedness for working in cybersecurity vary but are consistent with 2025 survey results. Only 4% of 2026 respondents strongly agreed, and 22% agreed, that university graduates are well prepared for the cybersecurity challenges within organizations. Most respondents said that they neither agreed nor disagreed (38%), while 21% disagreed and 7% strongly disagreed (**figure 17**).

FIGURE 15: Most Important Security Skills

Please choose the top five most important security skills needed by security professionals in your organization today.

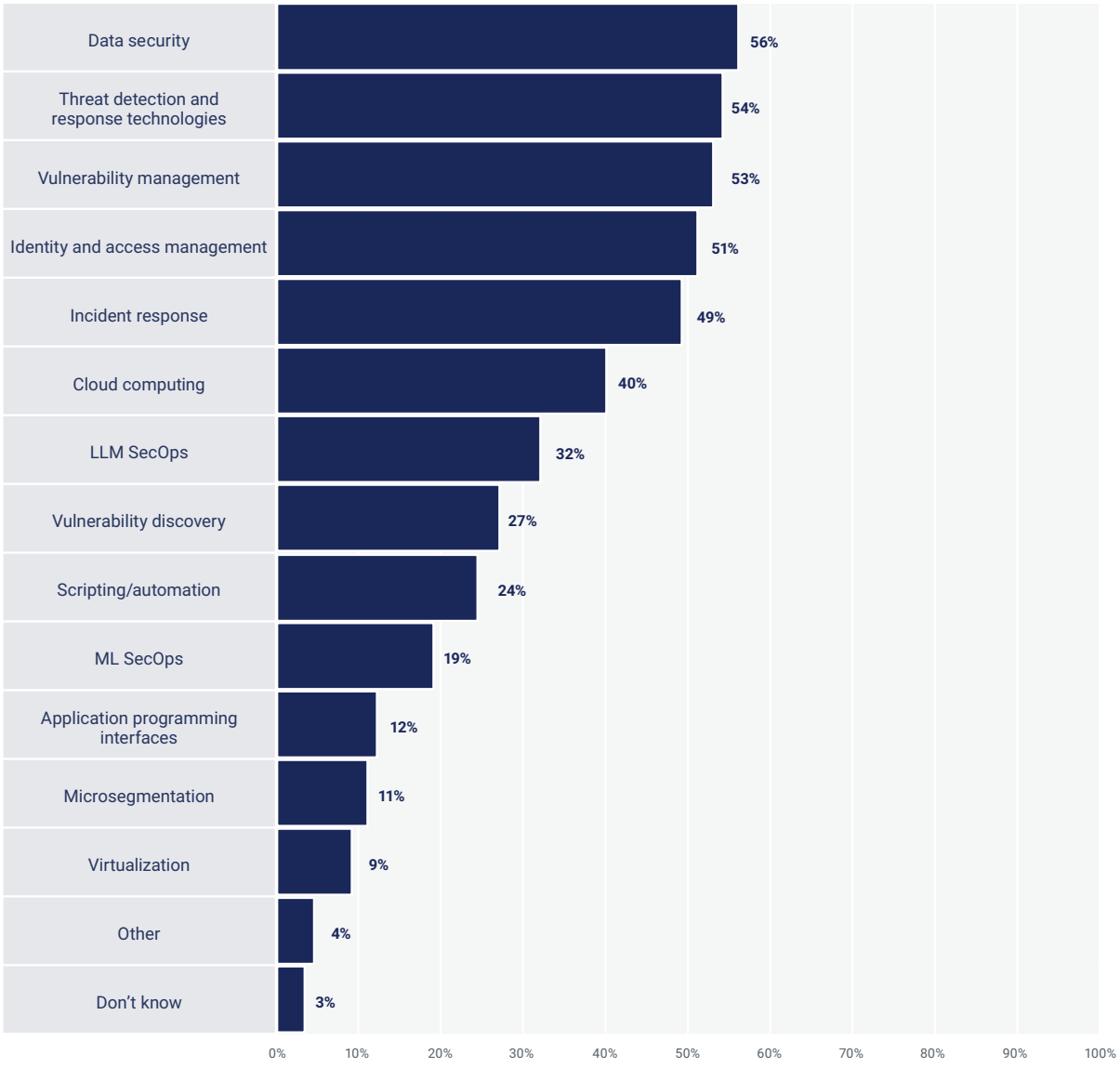


FIGURE 16: Global University Degree Requirements

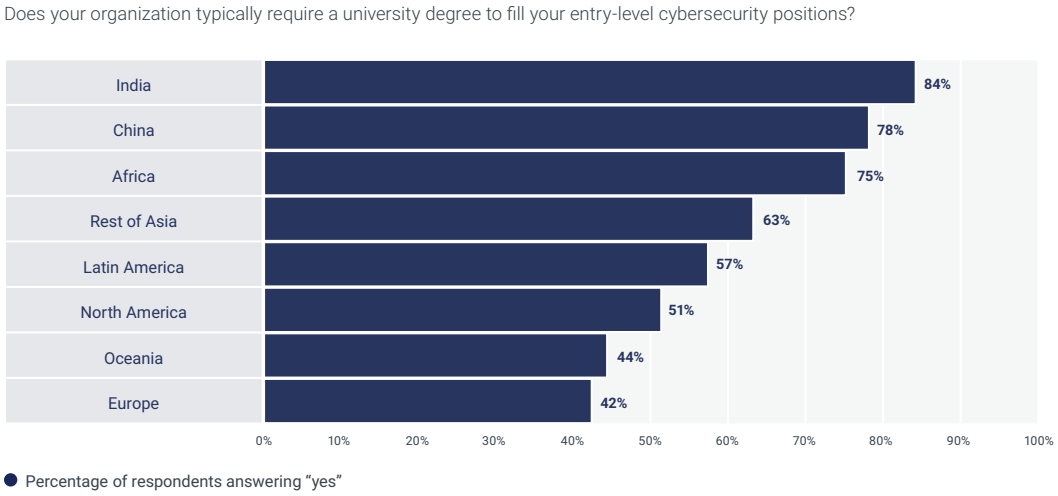


FIGURE 17: Career Preparedness

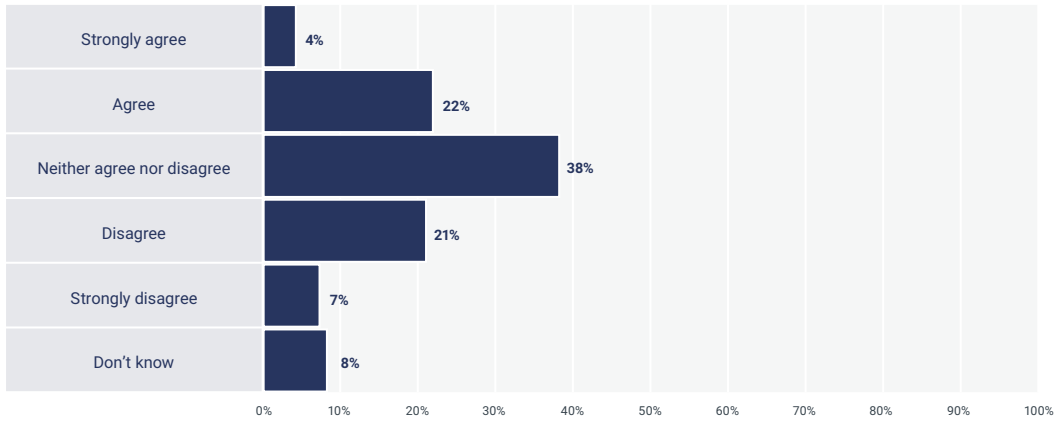


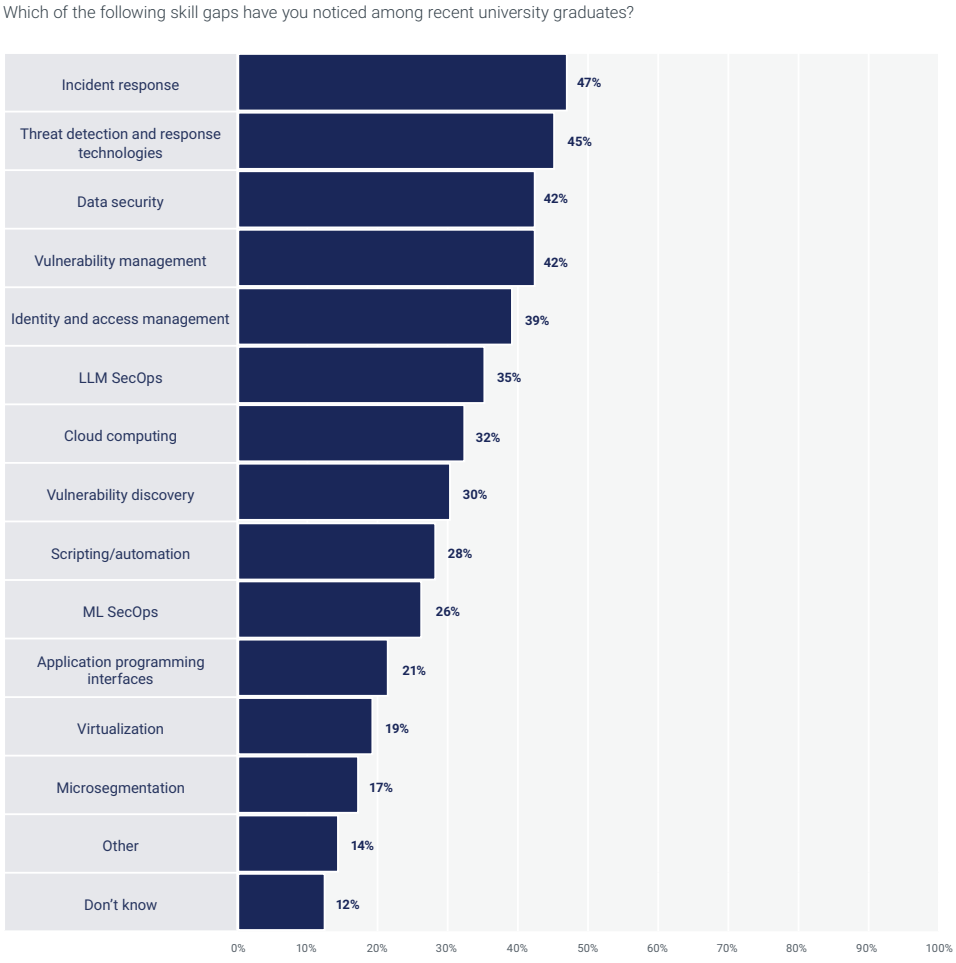
Figure 18 outlines common skill gaps observed in recent university graduates. Responses highlight the need for understanding and addressing the complexities of AI security—LLM SecOps increased 9 percentage-points from 2025, while incident response increased by 4 percentage-points and threat detection and response increased by 6 percentage-points. This was expected given the advances and updates to LLM enterprise expansion in 2026, with cybersecurity professionals adjusting to their operating environment. Data security and other skill gaps also increased slightly from 2025.

Forty-two percent of survey respondents manage security staff who have less than three years of work experience.

Respondents identified the following top areas in which these employees most need professional development and training:

- Incident response (54%)
- Data security (50%)
- Vulnerability management (45%)
- Identity and access management (43%)
- Threat detection and response technologies (43%)

FIGURE 18: Common Skill Gaps of Recent University Graduates



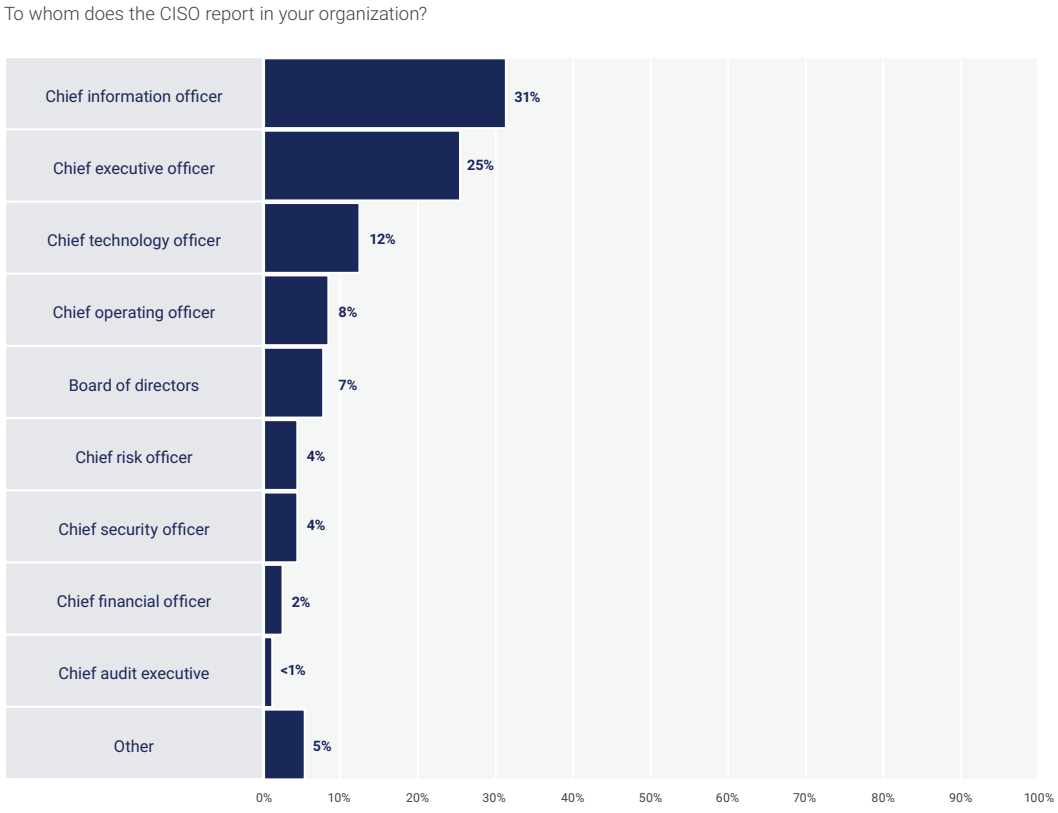
Cybersecurity Operations

Most survey respondents reported that chief information security officer (CISO) and senior management roles are not growing within their organizations. Whether an enterprise is likely to have a CISO depends on its size–close to 60% of small enterprises (with less than 499 employees) have CISOs, while 73% of enterprises with 500 to 5,000 employees, and 87% of enterprises with 5,000 to 10,000 employees, have CISOs. If an enterprise does not have a CISO, it does not mean that information risk is not accounted for or that the enterprise is in some way minimizing the importance of information security. It is not uncommon for small-to-medium enterprises not to employ a formal CISO, but the responsibilities are likely associated with a director or an information security manager.[6] **Figure 19** shows to whom CISOs report.

In organizations without CISOs, the security team reports to another executive. The most common roles include chief information officer (31%), chief executive officer (25%), and chief technology officer (12%).

6 IANS, "New Report from IANS and Artico Search Reveals CISO Compensation Remains Strong Despite 2024 Market Slowdown," 2 October 2024, www.iansresearch.com/resources/press-releases/detail/new-report-from-ians-research-and-artico-search-reveals-ciso-compensation-remains-strong-despite-2024-market-slowdown

FIGURE 19: CISO Reporting



Budgets

Consistent with last year's results, 41% of respondents reported that their cybersecurity budgets were appropriately funded, and 55% reported that their budgets were either somewhat or significantly underfunded (**figure 20**). **Figure 21** shows most respondents forecast that cybersecurity budgets will somewhat increase or not change in the next 12 months.

FIGURE 20: Cybersecurity Budget Funding

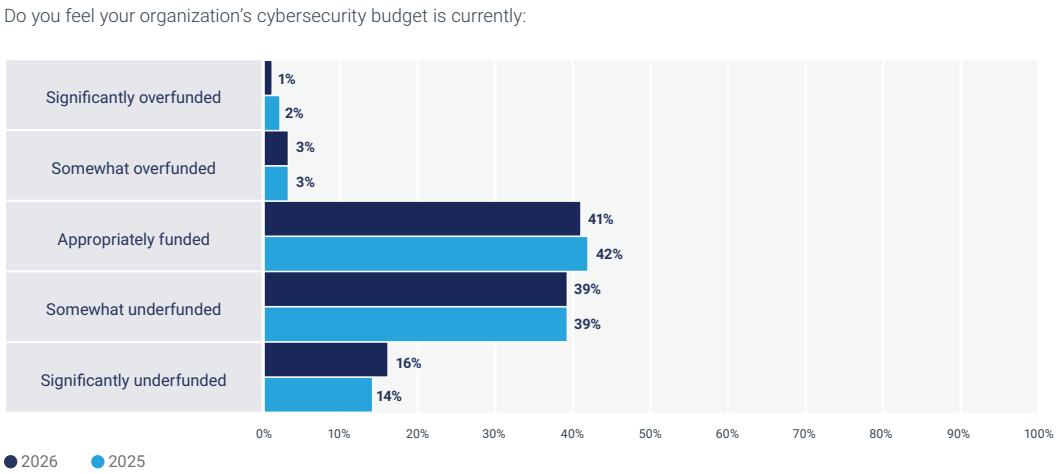
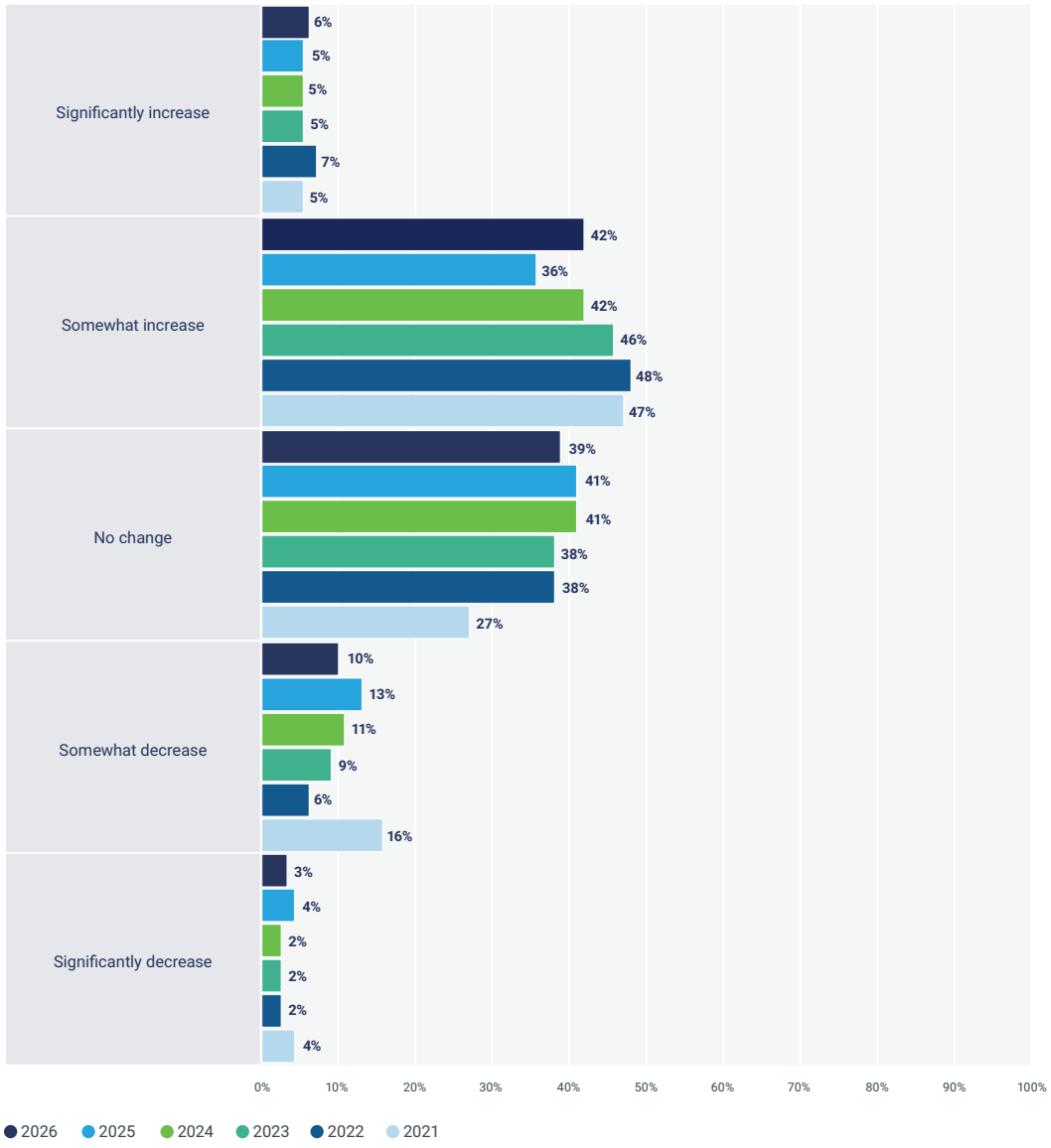


FIGURE 21: Cybersecurity Budget Forecasts

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



Boards and Cybersecurity Prioritization

Fifty-six percent of respondents reported that their board of directors adequately prioritizes cybersecurity, and 77% said their enterprise cybersecurity strategy is aligned with organizational objectives, which is slightly higher than last year (74%).

Predictably, among those respondents whose boards adequately prioritize cybersecurity, strategy alignment jumped to 95%.

When evaluating organizations with boards that effectively prioritize cybersecurity versus those that do not, several distinct trends arise.

Boards focused on cybersecurity can empower teams with necessary resources and bolster confidence in their cybersecurity capabilities:

- 56% of respondents whose boards adequately prioritize cybersecurity expressed complete or strong confidence in their cybersecurity team's ability to identify and address cyberthreats, in contrast to just 22% among those whose boards do not sufficiently prioritize security.
- Approximately 37% of respondents whose boards prioritize cybersecurity said that their cybersecurity funding is inadequate, whereas 85% of respondents whose boards lack focus on security shared this view.
- Enterprises with boards that prioritize cybersecurity were significantly more likely to provide attractive benefits, such as professional development opportunities and employee certification costs, than respondents with boards that do not adequately prioritize cybersecurity.

Enterprises with boards that prioritize cybersecurity were significantly more likely to provide attractive benefits, such as professional development opportunities and employee certification costs, than respondents with boards that do not adequately prioritize cybersecurity.

- Only 48% of respondent enterprises whose boards adequately prioritize cybersecurity faced difficulties retaining skilled cybersecurity personnel, unlike 67% of those whose boards do not.

Cyberrisk and Cyberattacks

Thirty-five percent of survey respondents said that their enterprises are experiencing an increase in cyberattacks from last year (**figure 22**). This is similar to the percentage of respondents who reported increased attacks in 2025.

Figure 23 shows the primary threat actors responsible for attacks, which are similar to last year. Slight declines in hackers and malicious insiders were reported.

FIGURE 22: Attack Trends

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

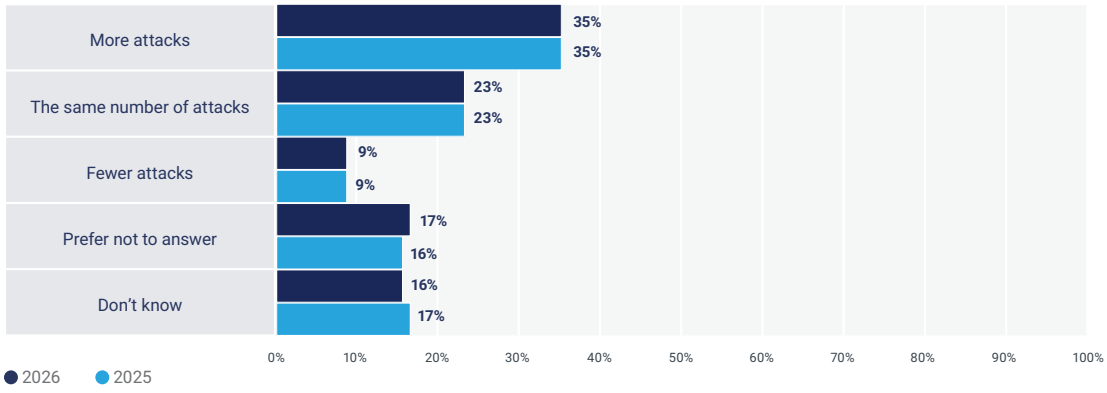
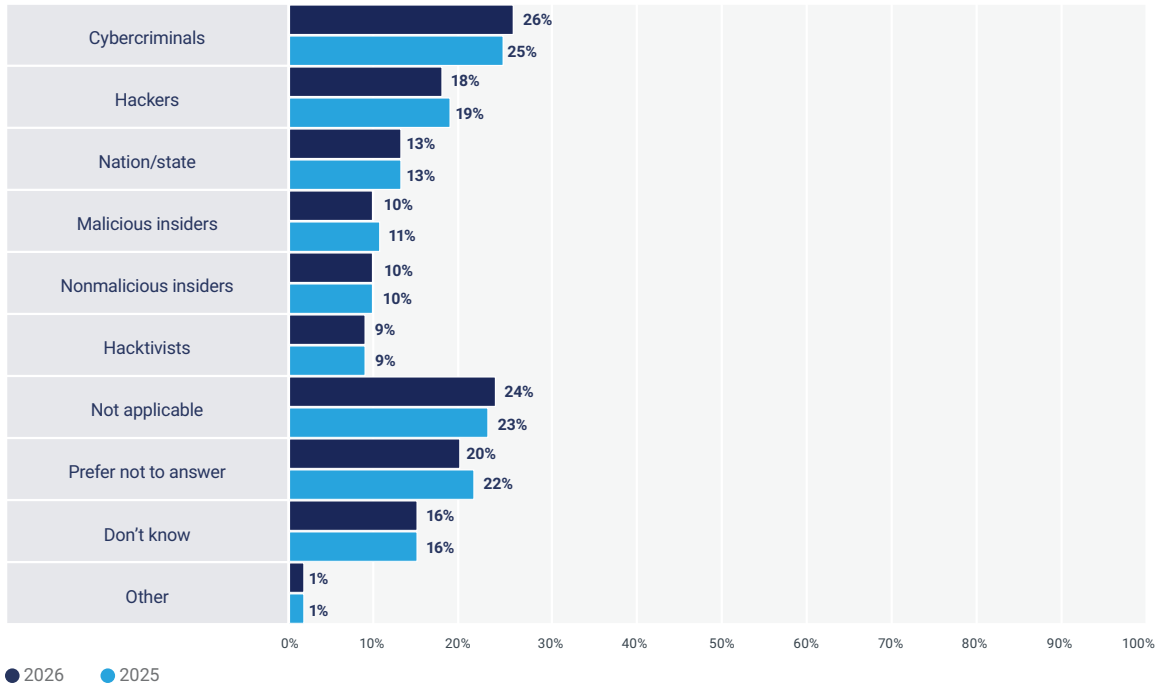


FIGURE 23: Threat Actors

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



Only 10% of respondents said their enterprise had been compromised since June 2025. Sixty-four percent said their enterprises were not compromised, and 25% of respondents said they do not know. **Figure 24** shows the main attack vectors used to compromise enterprises. Ransomware dropped 6 percentage-points from 2025, while remote access increased 5 percentage-points.

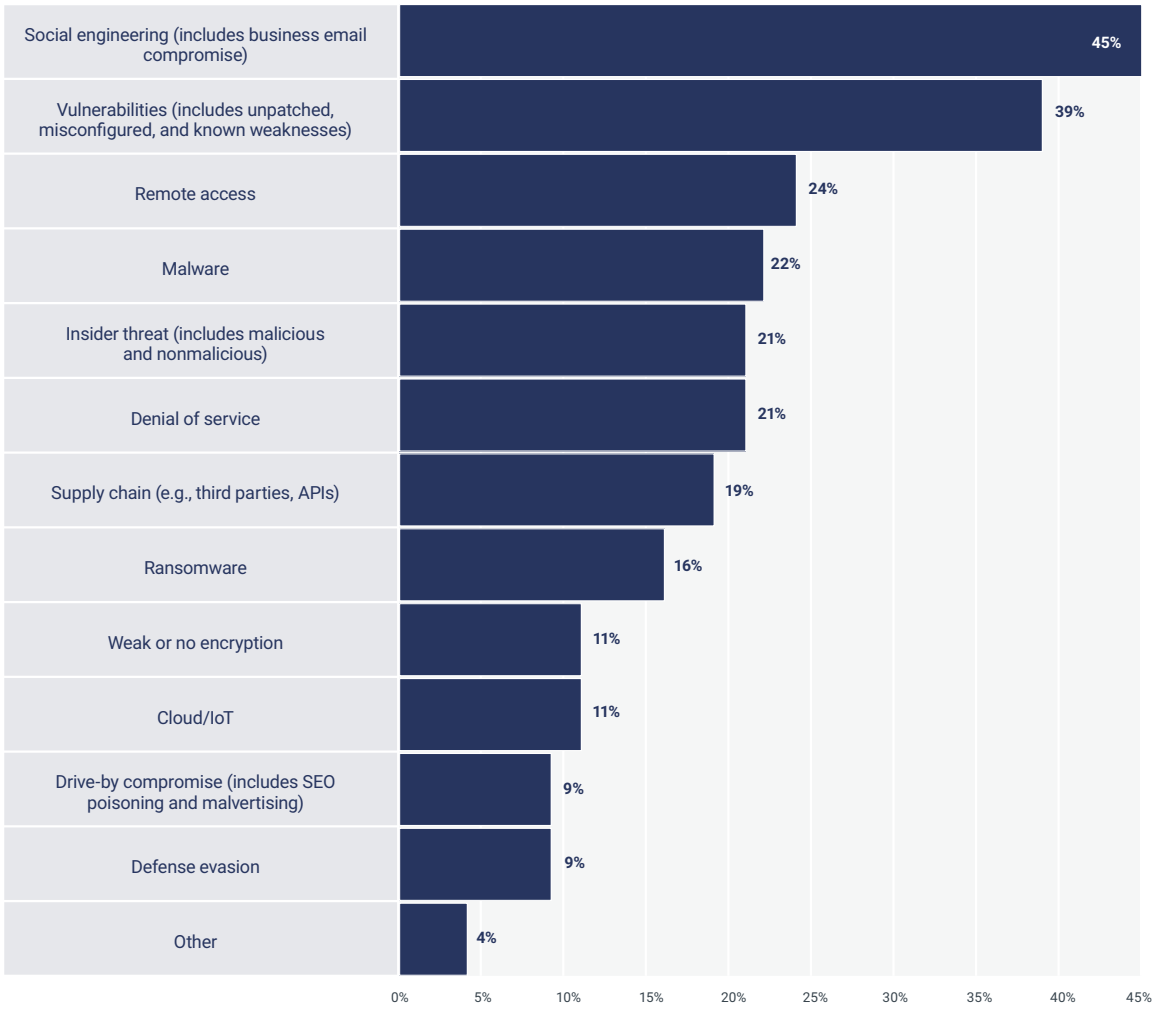
Sixteen percent of respondents confirmed or believed that the attacks on their enterprises were AI driven, while one-third (33%) did not know if the attacks were AI driven.

Almost half (45%) of respondents believed that their enterprise will likely or very likely experience a cyberattack in the next year (**figure 25**), which is a slight increase from 2025.

Almost half (45%) of respondents believed that their enterprise will likely or very likely experience a cyberattack in the next year.

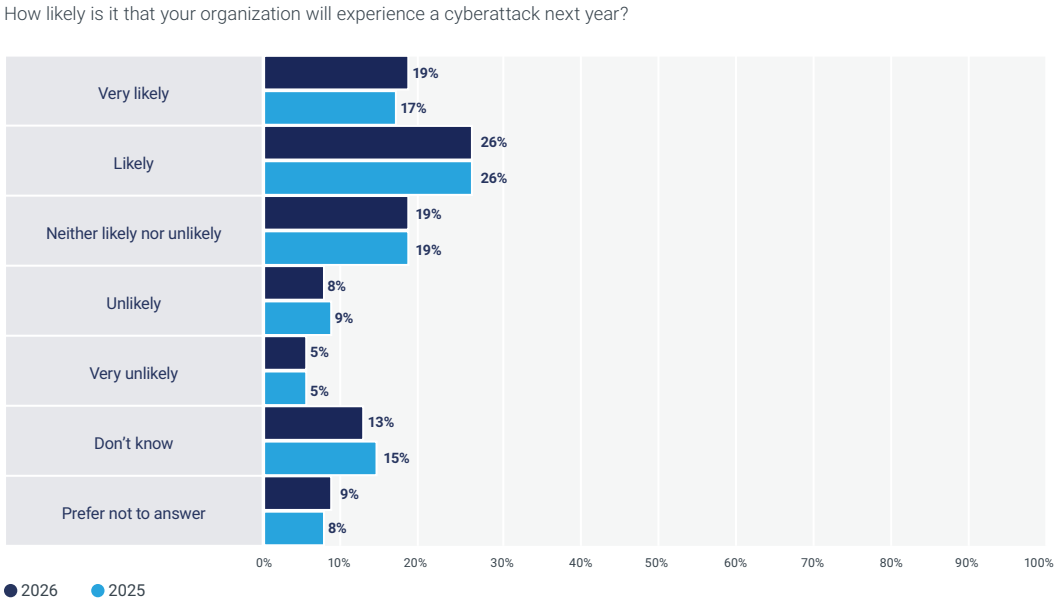
FIGURE 24: Attack Vectors Used[7]

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



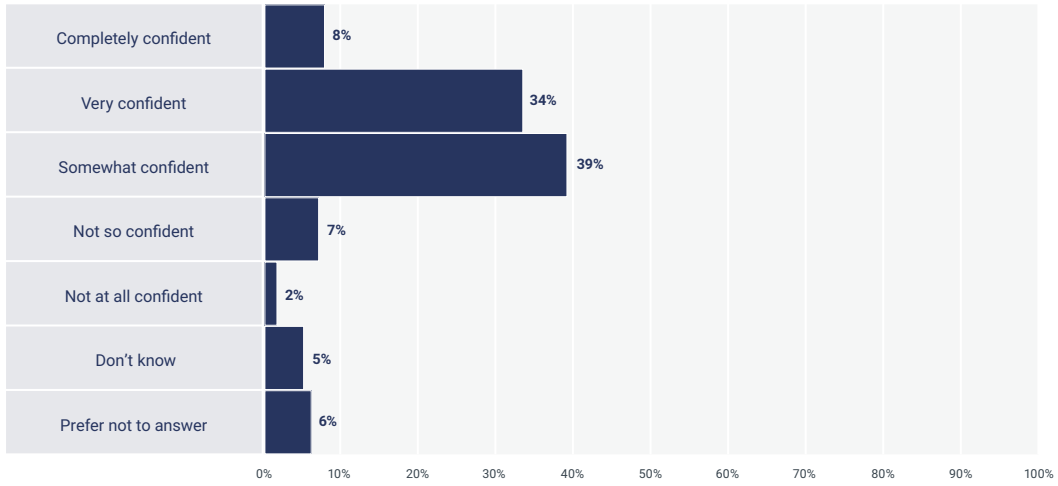
7 This figure excludes "Don't Know" responses and those who did not answer this question.

FIGURE 25: Likelihood of a Cyberattack



Just 42% of respondents were completely or very confident in their cybersecurity team's ability to detect and respond to cyberthreats (**figure 26**). Fifty-two percent of those who reported that their cybersecurity team is appropriately staffed were completely or very confident in the team's ability to detect and respond to cyberthreats, and of those in organizations with more than 10,000 employees, 48% feel completely or very confident in their team's ability to detect and respond to cyberthreats.

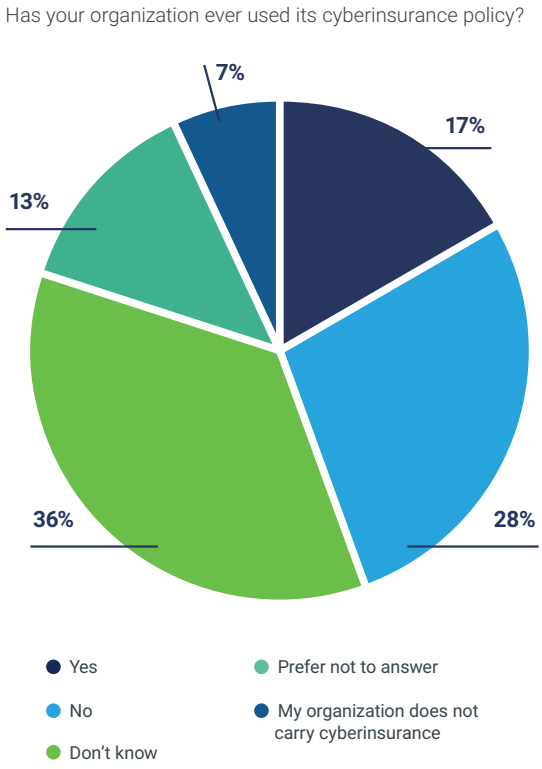
FIGURE 26: Confidence in Detecting and Responding to Cyberthreats



Thirty-eight percent of respondents said that most organizations underreport cybercrime even if they are required to report it, and 18% said they underreport cybercrime even if they are not required to report it. Only 20% said that cybercrime is accurately reported.

Many enterprises have cyberinsurance policies, which are used in the event of a cybersecurity incident, yet many respondents said that their enterprise has never used its cyberinsurance policy (**figure 27**). The percentage of respondents who said their enterprises have used their policies is 4% lower than last year. Twenty-eight percent of respondents who stated that their enterprises were compromised last year said they used their cyberinsurance policies, while 19% did not.

FIGURE 27: Use of Cyberinsurance Policy



Cyberrisk

This year's survey results show that enterprises are making positive strides away from annual risk assessments to more frequent risk assessments.

The percent of respondents that perform cyberrisk assessments monthly (13%) or every one to six months (22%) improved by 2 percentage-points from last year and 5 percentage-points from 2024 (**figure 28**).

FIGURE 28: Frequency of Cyberrisk Assessments

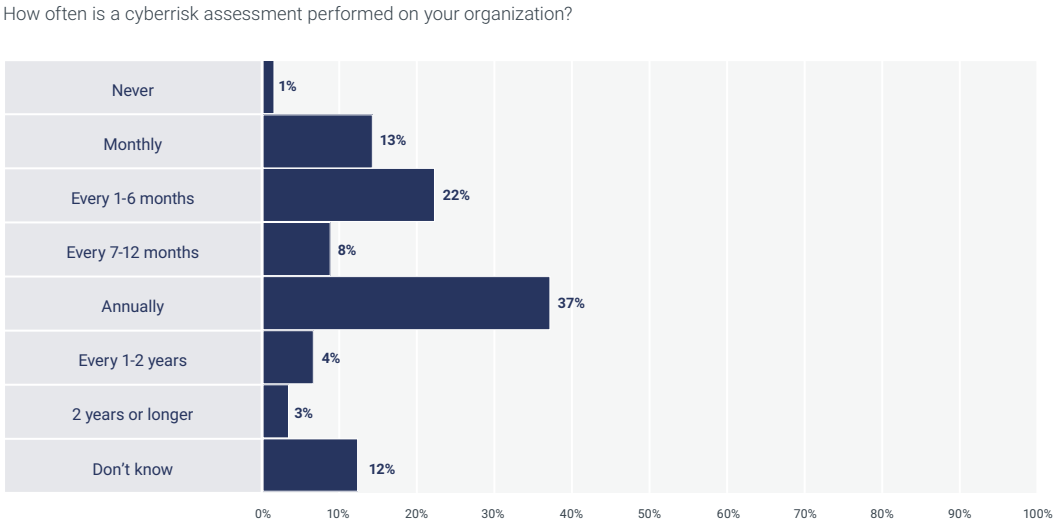
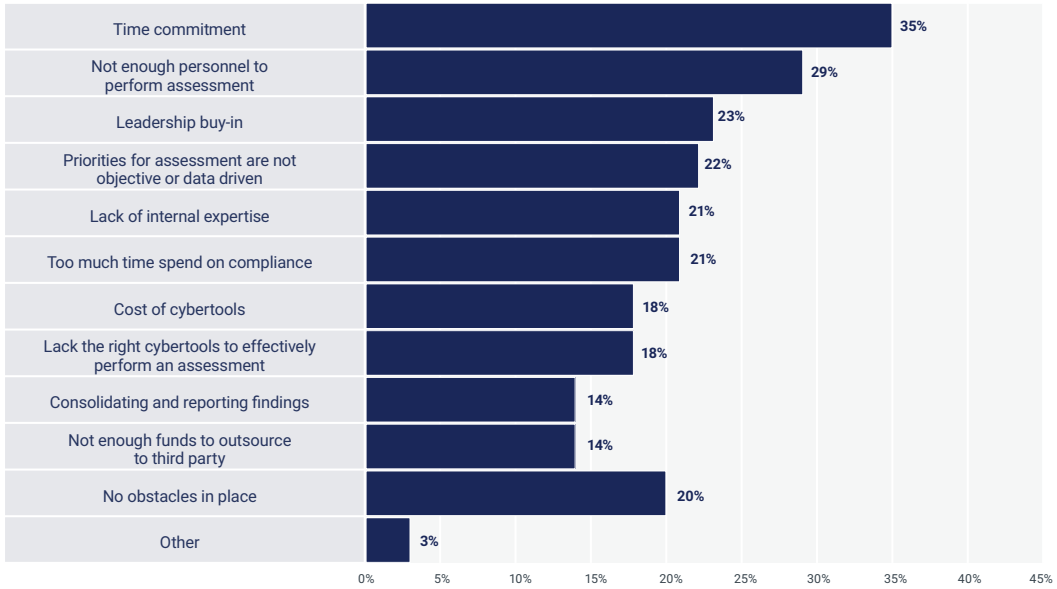


Figure 29 shows the obstacles organizations face when conducting cyberrisk assessments. Time commitment (35%) and not having enough personnel (29%) remain the top two obstacles—with almost the same percentages as last year—but are down from two years ago when they were 41% and 37%, respectively. Thirty-nine percent of respondents with understaffed cybersecurity teams conduct annual cyberrisk assessments, whereas overstaffed teams conduct them more frequently.

FIGURE 29: Obstacles to Conducting Cyberrisk Assessments



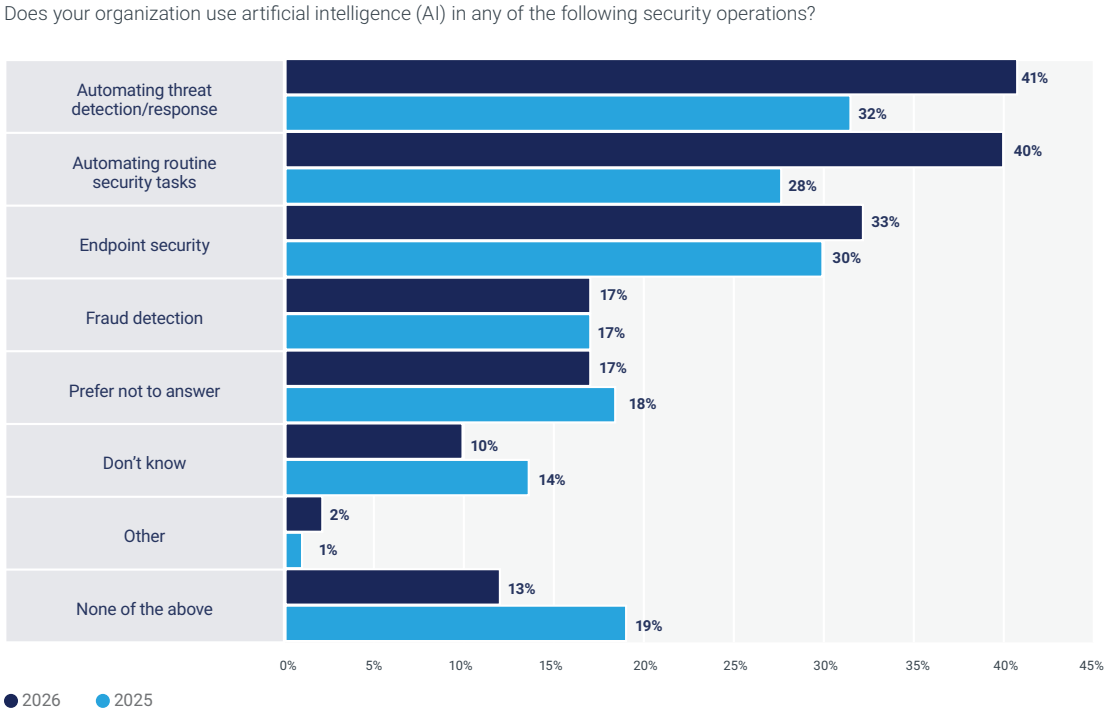
AI and Cybersecurity

The use of AI tools for various security operations continues to increase (**figure 30**).

The use of AI tools for various security operations continues to increase.

Respondents identified the two leading categories of AI use in security operations—automated threat detection/response (41%), which increased 9 percentage-points over 2025, and automating routine security tasks (40%), which jumped 12 percentage-points from 2025.

FIGURE 30: Use of AI for Security Operations



Over half (51%) of respondents indicated that they or someone from their team was involved in the development, onboarding, or implementation of AI solutions, which is considerably greater than last year (40%) and two years ago (29%) (**figure 31**). And 56% of respondents said that they or someone from their team was involved in the development of a policy governing the use of AI in their organization, which is 9% higher than in 2025 (**figure 32**).

FIGURE 31: Involvement in AI Life Cycle

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

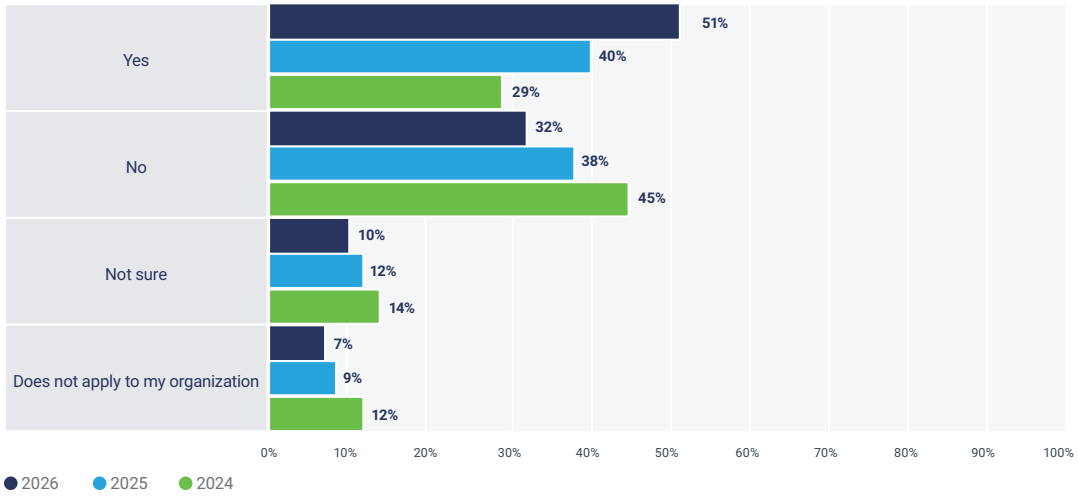
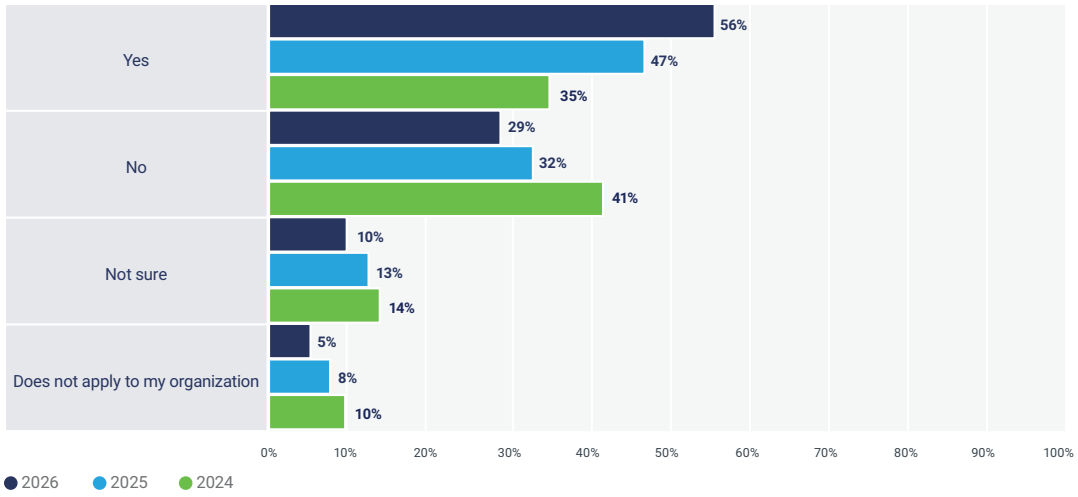


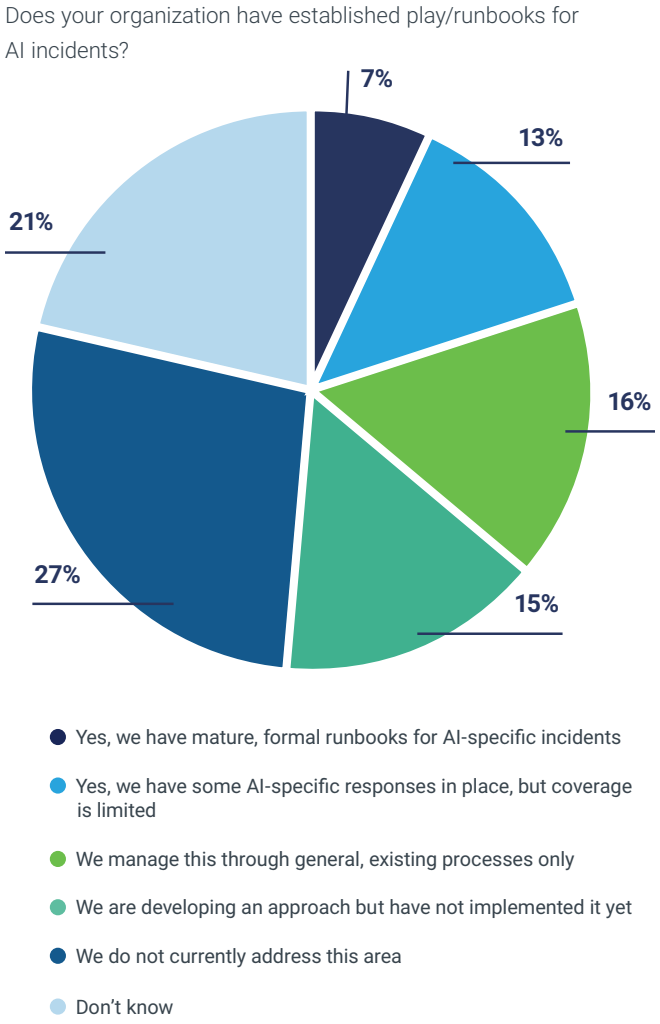
FIGURE 32: Involvement in Developing AI Policy

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



This year's survey introduced questions about incident response activities for AI solutions. Only 20% of respondents stated they have either mature or limited coverage of AI-specific incident runbooks established, while 27% stated they do not currently address this area within their organization (**figure 33**).

FIGURE 33: Play/Runbooks for AI Incidents



Adoption of AI in 2026 impacted cybersecurity teams, which are responsible for addressing the new incident response approaches for these solutions. Ten percent of enterprises conducted at least one AI-specific incident response exercise, and only 8% conducted exercises regularly (**figure 34**).

FIGURE 34: AI Incident Response Exercises

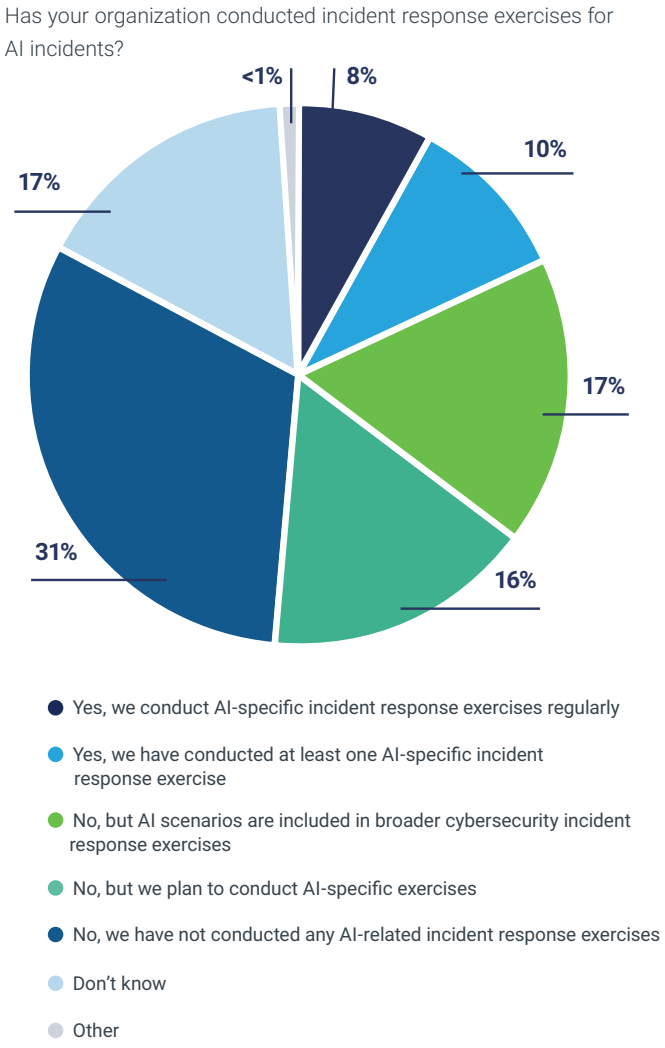
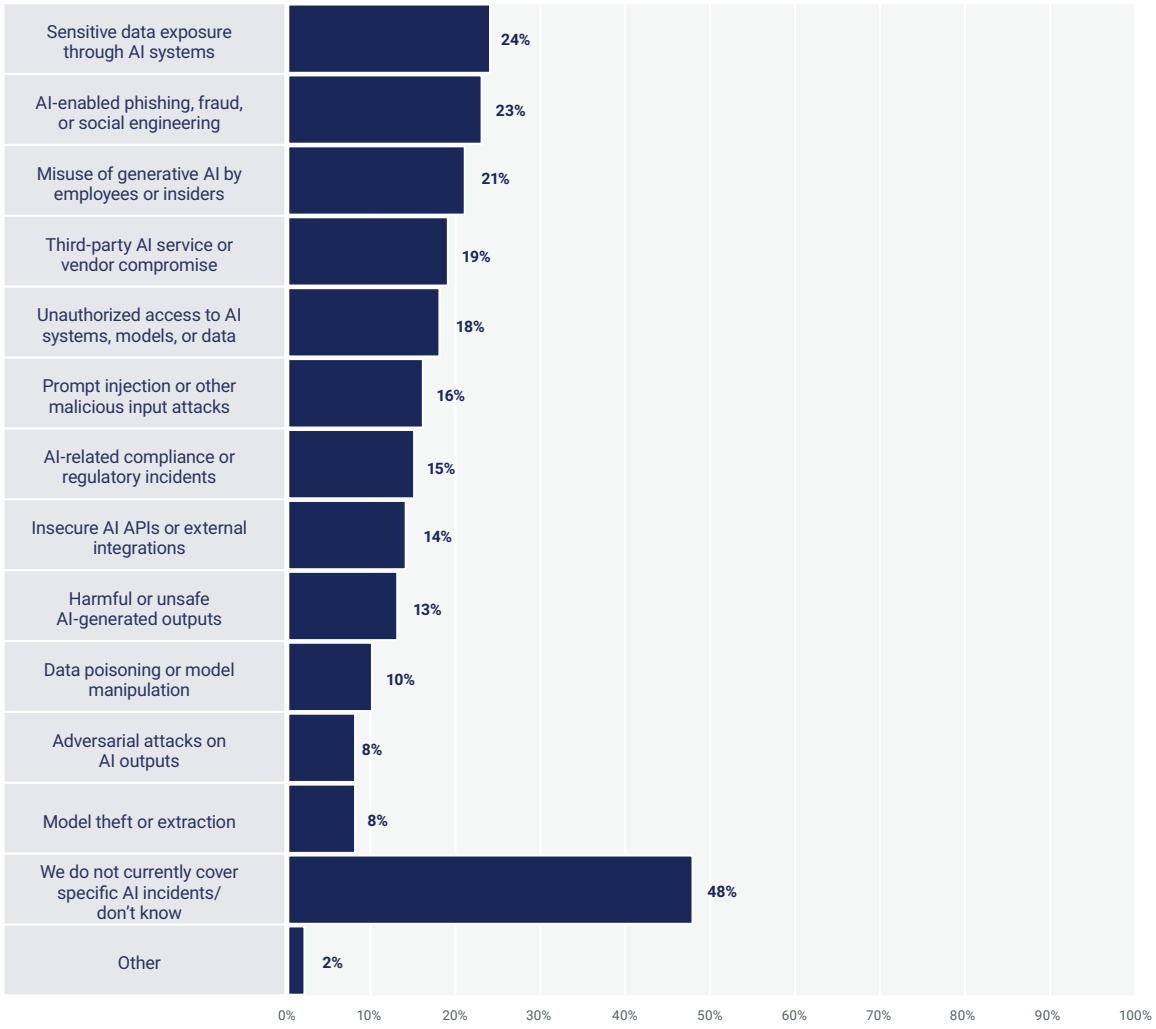


Figure 35 shows the types of AI-related incidents covered in incident response exercises. The top AI-related incidents include sensitive data exposure through AI systems (24%), AI-enabled phishing, fraud, or social engineering (23%), and misuse of generative AI by insiders (21%). Eight percent of respondents reported that adversarial attacks on AI outputs are included in their incident response exercises. These results suggest that, when adopting AI, the focus for the industry is on managing the user community that has access to sensitive information and datasets within an organization.

FIGURE 35: Types of AI-Related Incidents in Exercises

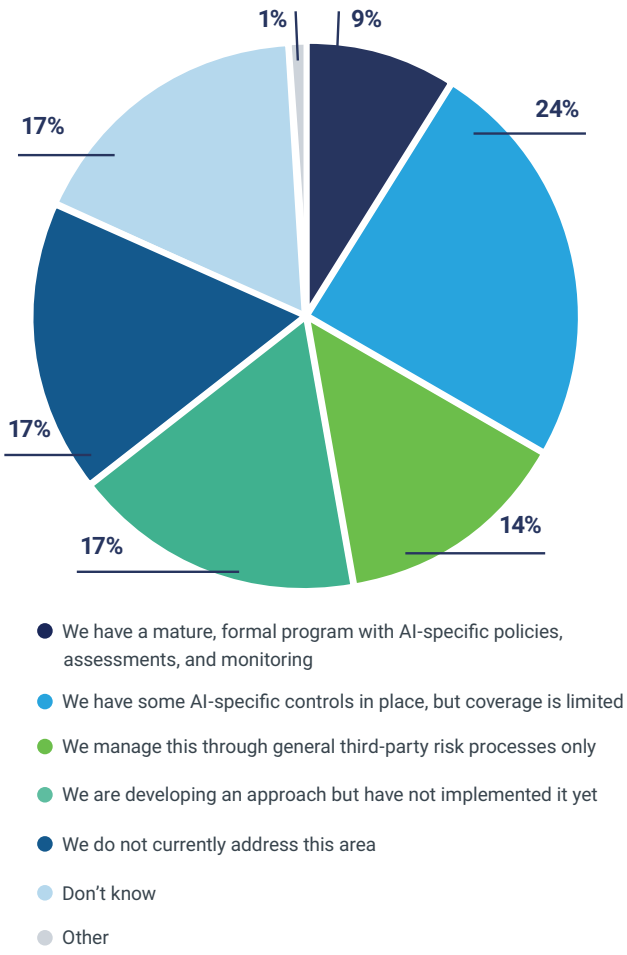
Which type of AI-related incidents are covered in your organization's incident response exercises?



For those enterprises that have some controls in place, organizational preparedness to respond to AI risk associated with third parties and vendors is limited (24%). Only 9% of respondents reported that their enterprises have mature programs with established policies, assessments, and monitoring for AI systems used by third parties, and many are either developing an approach (17%) or do not address this area in their programs (17%). This is demonstrated in **figure 36**.

FIGURE 36: Cyberrisk of AI Systems Used by Third Parties

How would you describe your organization's approach to responding to cybersecurity risk associated with AI systems used by third-party providers, vendors, or partners?



Conclusion: Cybersecurity Under Pressure at Inflection Point

The 2026 survey results show a cybersecurity environment under sustained pressure, with persistent longstanding challenges. AI is intensifying this pressure by reshaping workflows, influencing the threat landscape, and expanding governance demands, but AI use has not reduced the need for skilled practitioners, human oversight, or strong security fundamentals.

The workforce findings remain notable. Enterprises struggle to fill cybersecurity roles, and the profession continues to rely heavily on talent moving in from other fields. At the same time, few enterprises report open entry-level roles because demand is strongest for experienced practitioners and technically skilled individual contributors. This imbalance creates a long-term concern—if employers continue to prioritize experience

while routine work becomes more automated, new cybersecurity professionals may have fewer opportunities to build the practical skills they need to enter and advance in the field. This concern points to the need for more intentional workforce development.

Retention remains closely linked to operating conditions. Respondents cited high stress, limited promotion and development opportunities, and insufficient financial incentives as the leading reasons for leaving cybersecurity jobs. Flexible schedules and vacation help retain workers, but these solutions do not fully address the structural strain of understaffing, the complex threat landscape, and sustained workloads. In this sense, talent retention is not only a workforce issue; it is a resilience issue.

Talent retention is not only a workforce issue; it is a resilience issue.

Across operations and governance, the impact of AI is clear. Security teams use AI in some capacity, particularly for detection, response support, and routine tasks. However, adoption is outpacing readiness. Many respondents report only partial involvement in AI implementation, policy development, and governance, and relatively few enterprises have conducted AI-specific incident response exercises or created dedicated runbooks. The implication is not that AI requires a separate security model, but that existing disciplines—especially data security, incident response, access management, and governance—must be executed proficiently to address AI-related risk more fully.

The threat findings reinforce this message. Respondents view the threat environment as increasingly complicated, and AI-assisted attacks are a growing concern. However, among organizations that experienced compromise, the most common attack vectors remain familiar—social engineering and vulnerabilities. This suggests that even as attack methods evolve, outcomes continue to be shaped by core weaknesses in human behavior, exposure management, and control execution. For practitioners and leaders, the message is clear: resilience still depends on disciplined attention to the fundamentals.

However, among organizations that experienced compromise, the most common attack vectors remain familiar—social engineering and vulnerabilities. This suggests that even as attack methods evolve, outcomes continue to be shaped by core weaknesses in human behavior, exposure management, and control execution.

Overall, this year's survey results show a profession adapting to new demands without relief from old ones. AI is now part of cybersecurity's operating reality, but the results do not support the idea that technology alone will solve cybersecurity's core challenges. To sustain digital trust and resilience, organizations will need stronger approaches to workforce development, governance, operations, and risk management.

Acknowledgments

Lead Developer

An ISACA Staff Publication

Board of Directors

Massimo Migliuolo, Chair

Founder and Director of Cedro and Kibe, Malaysia

Jamie Norton, Vice-Chair

CISA, CISM, CGEIT, CIPM, CISSP, FGIA, GAICD, NACD.DC

Chief Information Security Officer, Australian Securities and Investments Commission, Australia

Stephen Gilfus

NACD.DC

Harvard University Certified Corporate Director, USA

Niel Harper

CISA, CRISC, CDPSE, CISSP, NACD.DC

Germany

Gabriela Hernández-Cardoso

NACD.DC

Former President and CEO, GE Mexico, Mexico

Jason Lau

CISA, CISM, CGEIT, CRISC, CDPSE, AAIA, AAISM, CEH, CIPM, CIPP/E, CIPT, CISSP, FIP, HCISPP, SM IEEE

Global Chief Information Security Officer, Crypto.com, Singapore

Maureen O'Connell

NACD.DC

Former Executive Vice President and Chief Financial Officer, Scholastic Corporation, USA

Erik Prusch

CEO, ISACA, USA

Tim Sattler

CISA, CISM, CGEIT, CRISC, CDPSE, CCSP, CISSP, ISO 27000 LI/LA, NACD.DC

Vice President of Corporate Information Security and Chief Information Security Officer, Jungheinrich AG, Germany

Asaf Weisberg

CISA, CISM, CGEIT, CRISC, CSX-P, CDPSE

Founder and CEO, introSight Ltd., Israel

John De Santis

ISACA Board Chair, 2023-2026

USA

Pamela Nigro

ISACA Board Chair 2022-2023

CISA, CGEIT, CRISC, CDPSE, CRMA

Senior Vice President and Security Officer, Medecision, USA

Tracey Dedrick

ISACA Board Chair, 2020-2021

Board Member and Chair of the Risk Committee for First Bancorp Puerto Rico, former Chief Risk Officer, Hudson City Bancorp, USA

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 195,000+ 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 195 countries and with more than 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.

About Wolters Kluwer TeamMate

Wolters Kluwer TeamMate delivers purpose-built GRC and audit solutions that empower audit, risk, compliance, and controls teams to operate with confidence and precision. With flexible, configurable solutions, TeamMate adapts to how teams work today while scaling seamlessly to support their evolving needs of tomorrow. TeamMate's global reach with strong local expertise supports organizations wherever they are. By unifying data across assurance, risk, and compliance disciplines, TeamMate provides leadership with a connected, real-time view of risk, strengthening decision-making and driving more resilient enterprise performance.

DISCLAIMER

ISACA has designed and created *State of Cybersecurity 2026: 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/

Wolters Kluwer

TeamMate®

TeamMate GRC Software

Audit and GRC expert solutions for stronger enterprise resilience

- Over 150 Frameworks
- 50% Faster Risk Assessments
- Consolidate Tools