FORTINET
Training Institute

2026 Cybersecurity Skills Gap

Global Research Report

Contents

Methodology

The findings in this report are based on responses obtained from online interviews and an email survey of 2,750 IT and/or cybersecurity decision-makers (compared to 1,850 in previous reports). The sample closely aligns with last year's cohort, with a variance of +/-1 to 3% across role, industry, company size, and gender. The research was conducted by Sapio Research in December 2025. Responses were collected from participants across 32 locations, with expanded coverage including Poland, Saudi Arabia, and Vietnam.

- Argentina
- Australia
- Brazil
- Canada
- Colombia
- France
- Germany
- Hong Kong
- India
- Indonesia
- Israel
- Italy
- Japan
- Mainland China
- Malaysia
- Mexico
- The Netherlands
- New Zealand
- The Philippines
- Poland
- Saudi Arabia
- Singapore
- South Africa
- South Korea
- Spain
- Sweden
- Taiwan
- Thailand
- United Arab Emirates
- United Kingdom
- United States of America
- Vietnam

Overall results are accurate to ± 1.9% at a 95% confidence level.

Size of Company

100–499 employees **23%**
500–999 employees **25%**
1,000–2,499 employees **22%**
2,500–4,999 employees **16%**
5,000+ employees **14%**

Role Type

11% of respondents held owner positions
35% of respondents held C-level executive positions
9% of respondents held vice president positions
9% of respondents held head positions
35% of respondents held director positions

Gender

65% of respondents were male
35% of respondents were female

Top Three Business Sectors

Technology **22%**
Manufacturing **16%**
Financial Services **11%**

Total respondents: 2,750

Asia-Pacific **29%**
Europe, Middle East, and Africa **27%**
Latin America **22%**
North America **22%**

Executive Summary

As organizations continue to grapple with ongoing skill shortages and the ever-evolving threat landscape, many are looking to AI-enabled cybersecurity solutions to fill key gaps and strengthen their security posture.

Organizations are leaning heavily on AI to keep them safe

- **91%** of respondents are using or experimenting with AI-powered cybersecurity solutions.
- **84%** say AI-enhanced security tools are helping IT and security teams be more effective and efficient—up from 80% last year.
- **42%** would trust AI to handle core security functions independently.

Breach costs and recovery times remain high

- **86%** of organizations report one or more breaches in the past 12 months. Over a quarter (29%) had 5 or more.
- **52%** say breaches cost them more than $1 million—up from 38% in 2021.
- For the past three years, IT leaders say that the top three causes of security breaches are:
  - lack of cybersecurity skills (**56%**)
  - lack of security awareness (**55%**)
  - lack of cybersecurity products (**54%**)

Board inaction is driving cyber risk

- **73%** of organization's boards say cybersecurity is a high business priority, but only 59% prioritize spending on it.
- **50%** say board members or executives have faced penalties after a cyberattack.
- **50%** of leaders believe their board members are "fully aware" of potential risks from AI use.

The cybersecurity skills gap is growing with AI

- **60%** of respondents say their top recruiting challenge is finding cybersecurity talent with specific experience in AI.
- **63%** expect more need for AI oversight and governance roles on cybersecurity teams over the next three years.
- **51%** say that, in general, they need senior-level cybersecurity skills most of all.

Certifications are still in high demand

- **91%** of IT decision-makers prefer candidates with technology-focused certifications.
- **92%** would pay for an employee to get certified.
- **92%** are likely to invest in AI-related cybersecurity training or certifications in the next 12 months.

Recruiting from broader talent pools remains a challenge

- **71%** have formal targets for cybersecurity hiring from underutilized talent pools.
- **92%** use internships, apprenticeships, partnerships, and programs to attract underrepresented groups.
- **75%** have structured recruiting initiatives targeting women, up from 70% last year.

INTRODUCTION

The Convergence Crunch: AI and the Cybersecurity Skills Shortage

Now in its fifth year, the Fortinet *Cybersecurity Skills Gap* survey continues to surface compelling insights and occasionally unexpected findings. One key takeaway in 2026 is that while organizations recognize the importance of cybersecurity, their investments don't always show it.

Based on a survey conducted at the end of December 2025, this report also finds that AI is helping cybersecurity teams be more effective and efficient. However, AI can also pose new risks, including AI-enhanced threats and unprepared employees who misuse AI. While respondents generally have high hopes for AI-enabled security solutions, implementation isn't without its perils. The more AI organizations take on, the more they need the AI skills that are proving hard to come by.

This puts pressure on executive leaders and boards of directors to assert cybersecurity as a corporate strategic imperative, yet, once again, the results show that boards may not have the awareness or knowledge they need.

Closing the skills gap continues to require outreach to underutilized talent pools. Many organizations seem to be aware of this, yet the makeup of the IT and cybersecurity workforce has not changed significantly, and the difficulty in finding qualified candidates appears to be on the rise.

As in previous years, we've added new questions and expanded others to drill deeper into the data. We also expanded our survey from 1,850 respondents to 2,750 and added three countries: Poland, Saudi Arabia, and Vietnam. The survey closely aligns with last year's cohort, with a variance of +/-1 to 3% across role, industry, company size, and gender.

This 2026 report also includes "big movers," callouts in each core chapter highlighting the most significant year-over-year (YoY) shifts, and a dashboard-style index of all three-, four-, and five-year datasets.

91% of respondents say they are using or experimenting with AI-powered cybersecurity solutions.

Organizations Are Leaning Heavily on AI to Keep Them Safe

Nearly every respondent (91%) to our survey said their organization is either already using (49%) or experimenting with (42%) AI-powered cybersecurity solutions—8% have plans to implement within the next year.

Most organizations (84%) report that AI-enhanced tools have made their IT and security teams more effective and efficient, up from 80% in 2024. Many indicate at least some degree of trust in AI solutions to work autonomously:

- 42% say they would rely on AI to handle core security functions* independently.
- 41% say they would trust it to do so with limited human oversight.
- 15% say they would trust AI tools provided they had significant oversight.
- Only 1% say they would not trust AI for core security functions.

While AI is clearly seen as holding great promise for cybersecurity, respondents acknowledge implementation comes with some definite challenges. Half (50%) express concerns about data privacy and information security, up from 47% last year. Meanwhile, 45% worry about a lack of staff with sufficient AI expertise, down slightly from 48% in 2024.

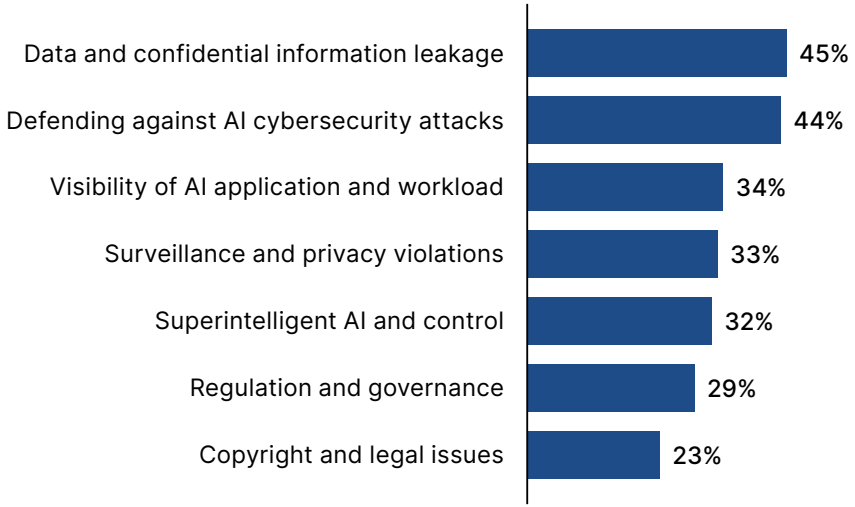
Other implementation-related concerns include understanding and managing potential AI risks (43%, virtually even with 44% last year), compatibility issues or challenges with existing infrastructure (43%, holding with 42% in 2024), and skepticism or uncertainty about AI for cybersecurity (38%, down from 43% in 2024).

* Core security functions refer to the essential defensive operations that protect systems, data, users, and business operations from compromise.

Information Leakage and AI Attacks Are Top Concerns

When asked which aspects of AI are most concerning for their cybersecurity plans and strategies, respondents were clear that confidential data leaks and AI-powered attacks are top of mind.

Areas of AI that organizations are most concerned about



Note: Other = 0%

DIGGING DEEPER

AI for Cybersecurity Demands an Intentional Approach

IT leaders are driving AI adoption for cybersecurity

While other executives are also on board, CIOs and IT heads are leading the charge to augment security with AI:

- 36%: CIO or IT leadership
- 19%: CISO or security leadership
- 19%: Entire leadership team
- 17%: AI or innovation team

AI implementation requires skilled and trained talent

Organizations are preparing for AI adoption through a combination of training, reskilling, and hiring:

- 59%: Training or reskilling programs developed internally
- 58%: Hiring new AI-skilled talent
- 52%: Procuring training or reskilling from industry vendors

Analysts are the top go-to for trusted AI information

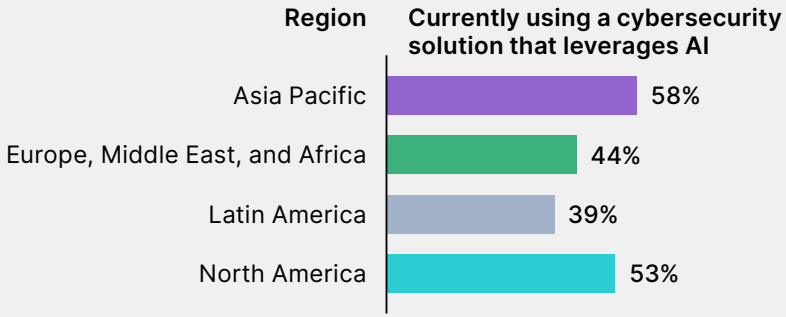
Organizations trust a mix of sources for information about AI solutions:

- 52%: Independent analyst firms
- 49%: Industry associations/ standards bodies
- 47%: Academic or research publications

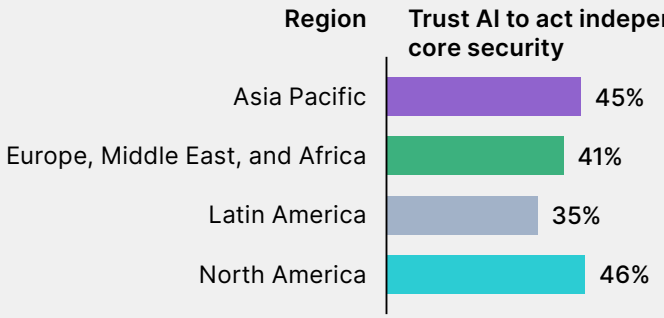
44% of respondents cited defending against AI cybersecurity attacks as a top concern.

Regional Highlights

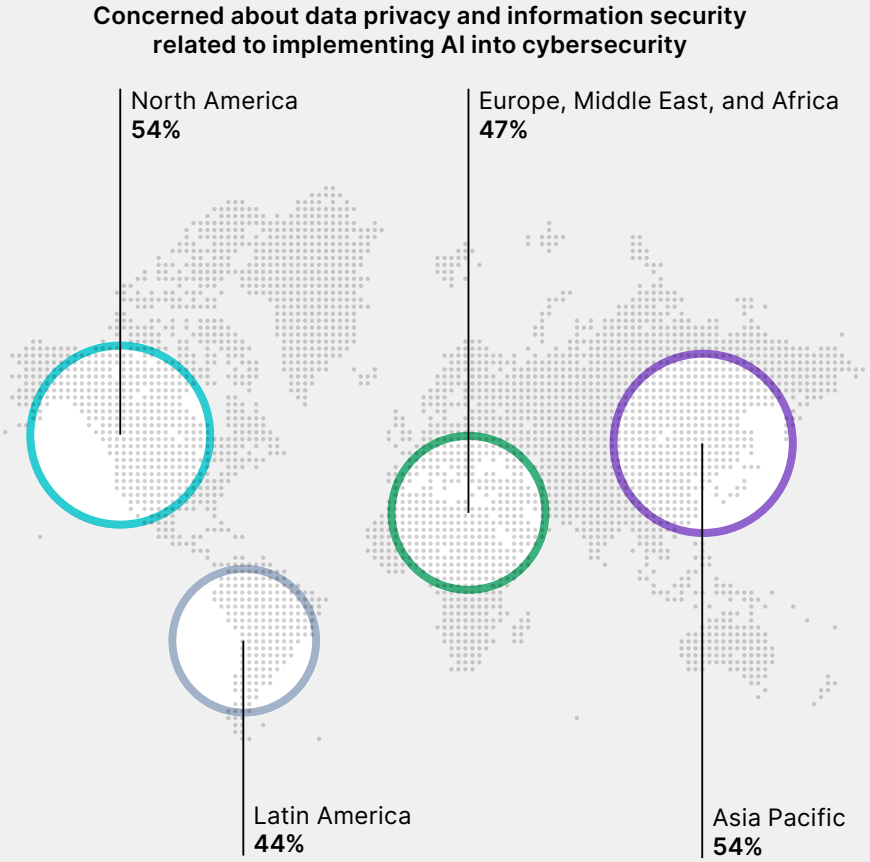
Asia Pacific is top user of AI for cybersecurity



AI trust is highest in North America and Asia Pacific



North America and Asia Pacific are most concerned about AI-security data leaks

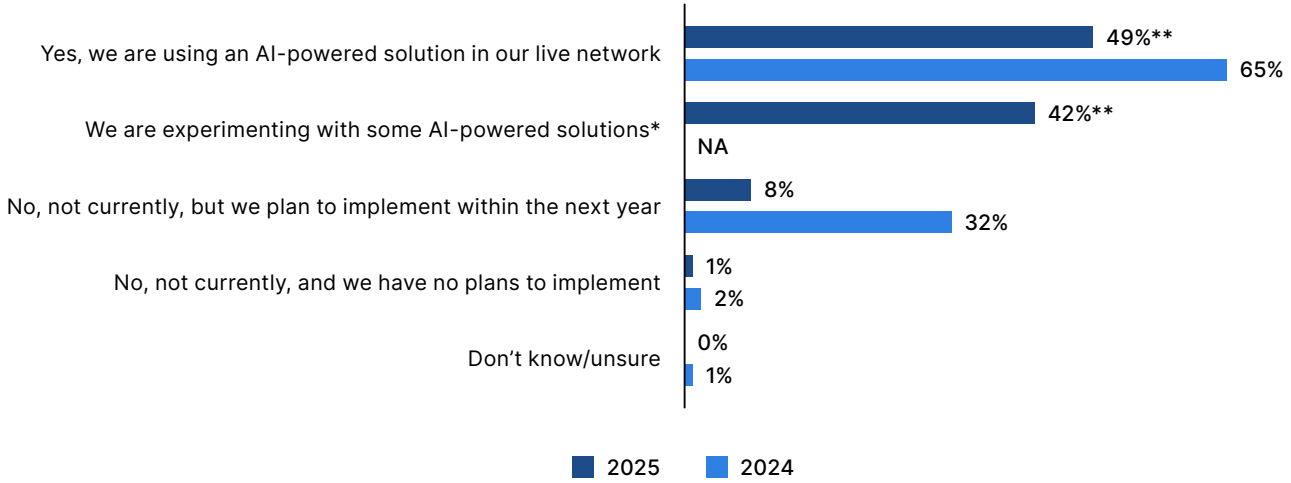


Big Movers

YoY Highlights

In 2024, 65% of respondents said they were using an AI-powered solution in their live network, and 32% said they planned to use one. As the chart below shows, both figures dropped significantly in 2025, likely due to the addition of a new answer option: "We are experimenting with some AI-powered solutions."

USING AN AI-ENABLED CYBERSECURITY SOLUTION



* New answer option added this year, cannot be tracked.
** 2025: 91%

Taking Action

It's probably fair to say that every organization today is wrestling with the impacts and implications of AI, whether as a tool to use or a threat to defend against. The concerns expressed by respondents in our 2025 survey reflect this, ranging from accidental data leaks to challenges in recruiting AI-skilled professionals and a lack of sufficient understanding of the potential risks that need to be managed.

Partner to find the right training

Organizations do not need to tackle the AI challenge alone. Partnering with vendors or training providers that offer structured AI education and certification pathways can help organizations accelerate adoption while reducing uncertainty. These programs allow security teams to develop the skills required to deploy AI responsibly and to better understand how adversaries may also leverage AI in attacks.

Ensure everyone gets training

Equally important is ensuring that AI literacy extends beyond the security team. IT staff, developers, and business leaders should all have a foundational understanding of how AI systems operate, the risks they pose, and how to mitigate those risks. Building this shared knowledge base allows organizations to unlock the productivity and security benefits of AI while minimizing unintended consequences.

86% of organizations had one or more breaches in the past 12 months.

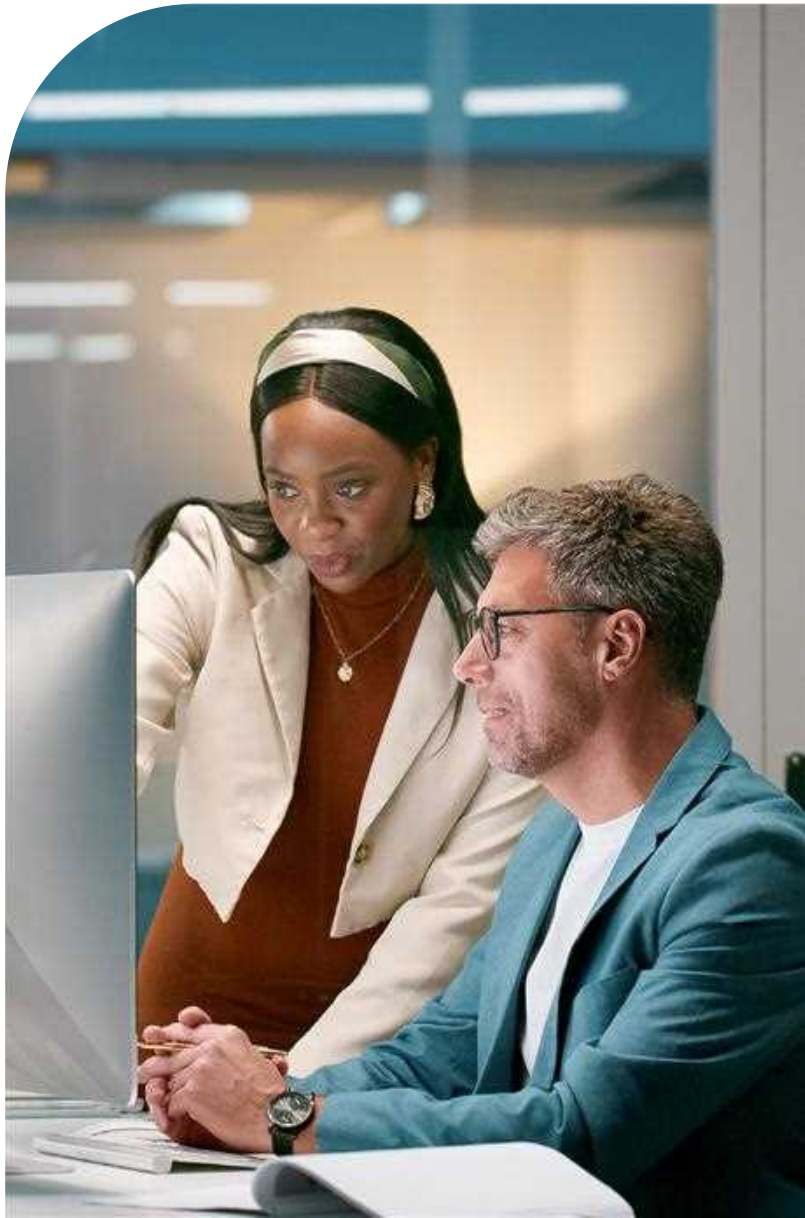
Breach Costs and Recovery Times Remain High

Breaches continue to take a toll on organizations worldwide. The majority of respondents (86%) report experiencing at least one breach in the past 12 months, with 29% reporting five or more. Those volumes are in keeping with levels reported last year (86% and 28%, respectively) and may mark a "new normal" when considered in light of five-year trends.

In 2021, only 19% of respondents reported five or more breaches. That figure jumped to 29% in 2022 and has held steady since. In contrast, the share of organizations reporting no breaches declined from 20% in 2021 to 14% in 2025.

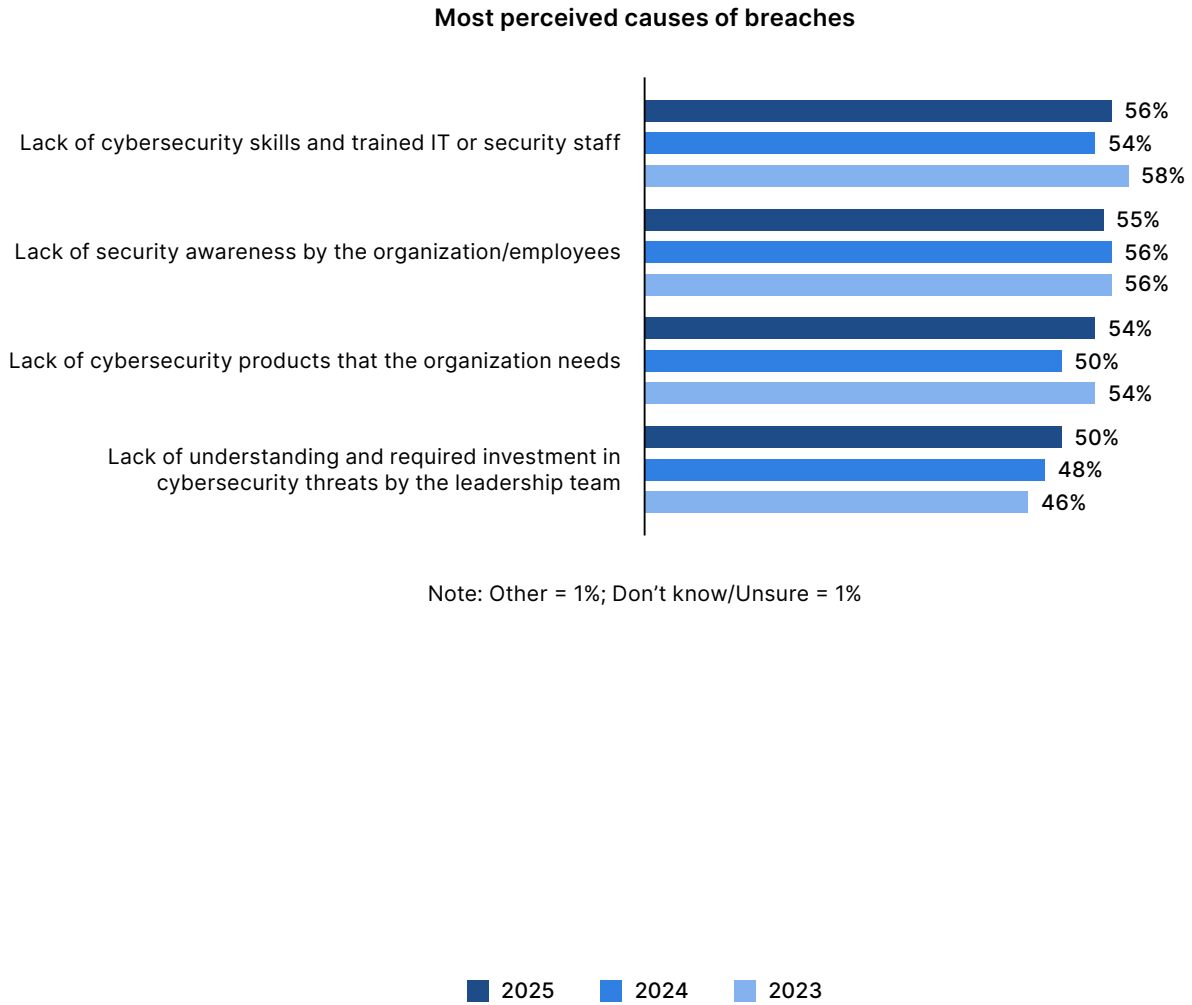
Recovery times also increased in 2025: 20% of organizations report it took four to six months to recover from a cyberattack, up from 14% in 2024.

More than half (52%) say breaches cost them more than $1 million, a percentage that's held basically stable for the past three years—up from 38% in 2021. Today, only 18% say breaches cost them nothing, a sharp decline from 36% five years ago.



Human Factors Remain the Top Perceived Cause of Breaches

Consistent with previous surveys, more than half of respondents say insufficient skills (56%) and awareness (55%) have caused the breaches they've experienced. Lack of tools (54%) and lack of understanding and investment (50%) round out the top four.



Note: Other = 1%; Don't know/Unsure = 1%

DIGGING DEEPER

Strong Teams and Training Are Seen as Key to Cybersecurity

The most common attacks remain consistent

Malware, phishing, and web attacks together account for 78% of cyberattacks experienced (the same as 2024 and down just slightly from 80% in 2023):

- Malware attacks: 39% (40% in 2024)
- Phishing attacks: 36% (32% in 2024)
- Web attacks: 31% (30% in 2024)

Staffing up is the top response to a breach

Decision makers are inclined to take a range of actions in the wake of a cyberattack:

- Expand IT or security team: 59% (63% last year)
- Introduce security awareness and training for all employees: 56% (59% last year)
- Mandate cybersecurity certifications for IT and security personnel: 54% (62% last year)
- Purchase new, more, or better security solutions that leverage AI: 54% (new option in 2025)

Cybersecurity teams are growing

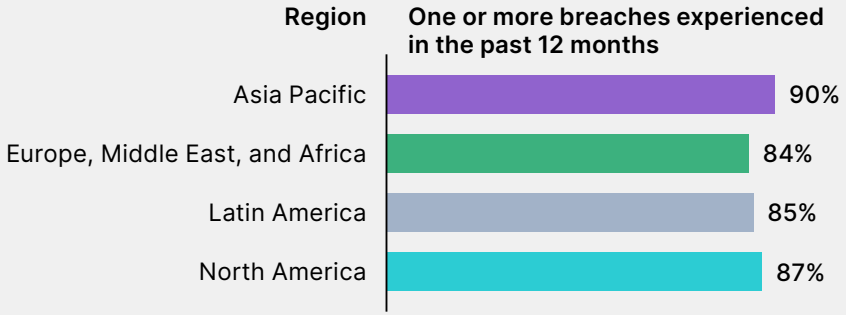
Most respondents (87%) expect to increase the size of their cybersecurity team in the next 12 months:

- 39%: Increase significantly
- 48%: Increase slightly
- 11%: Stay the same

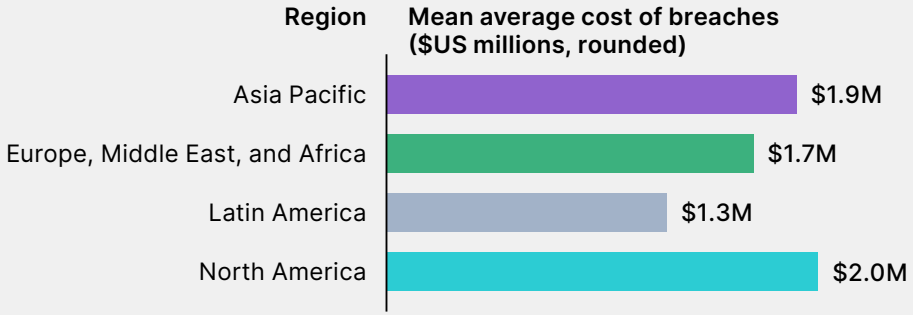
87% of respondents expect their cybersecurity team to grow in the next 12 months.

Regional Highlights

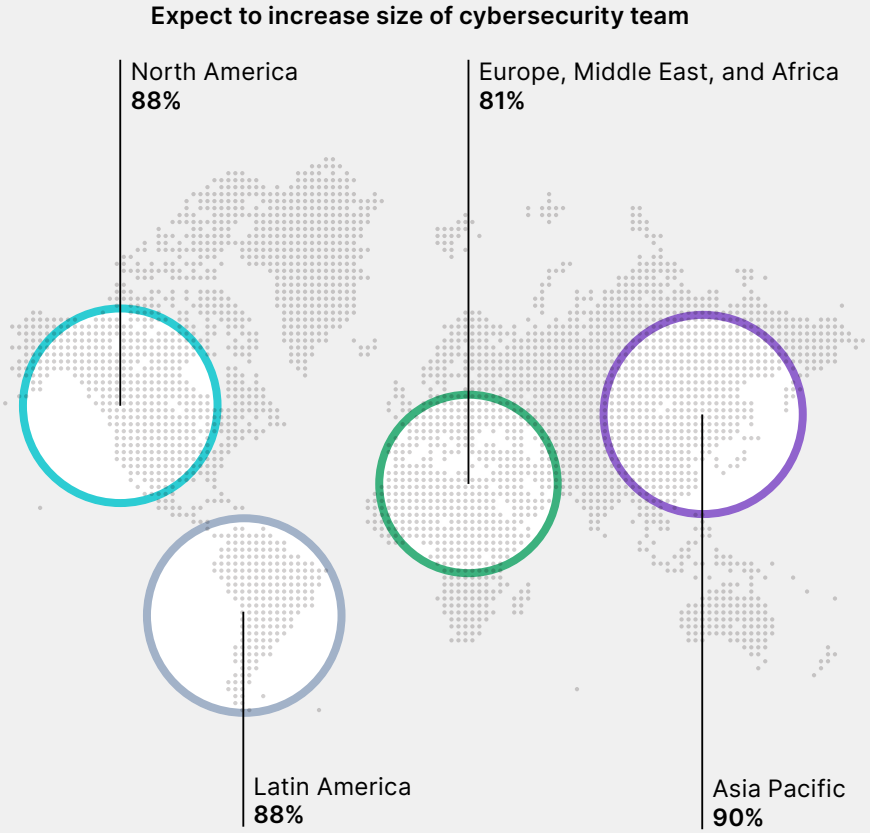
Organizations in Asia Pacific experienced the most breaches last year



Breaches cost most in North America



Cybersecurity teams are most likely to grow in Asia Pacific

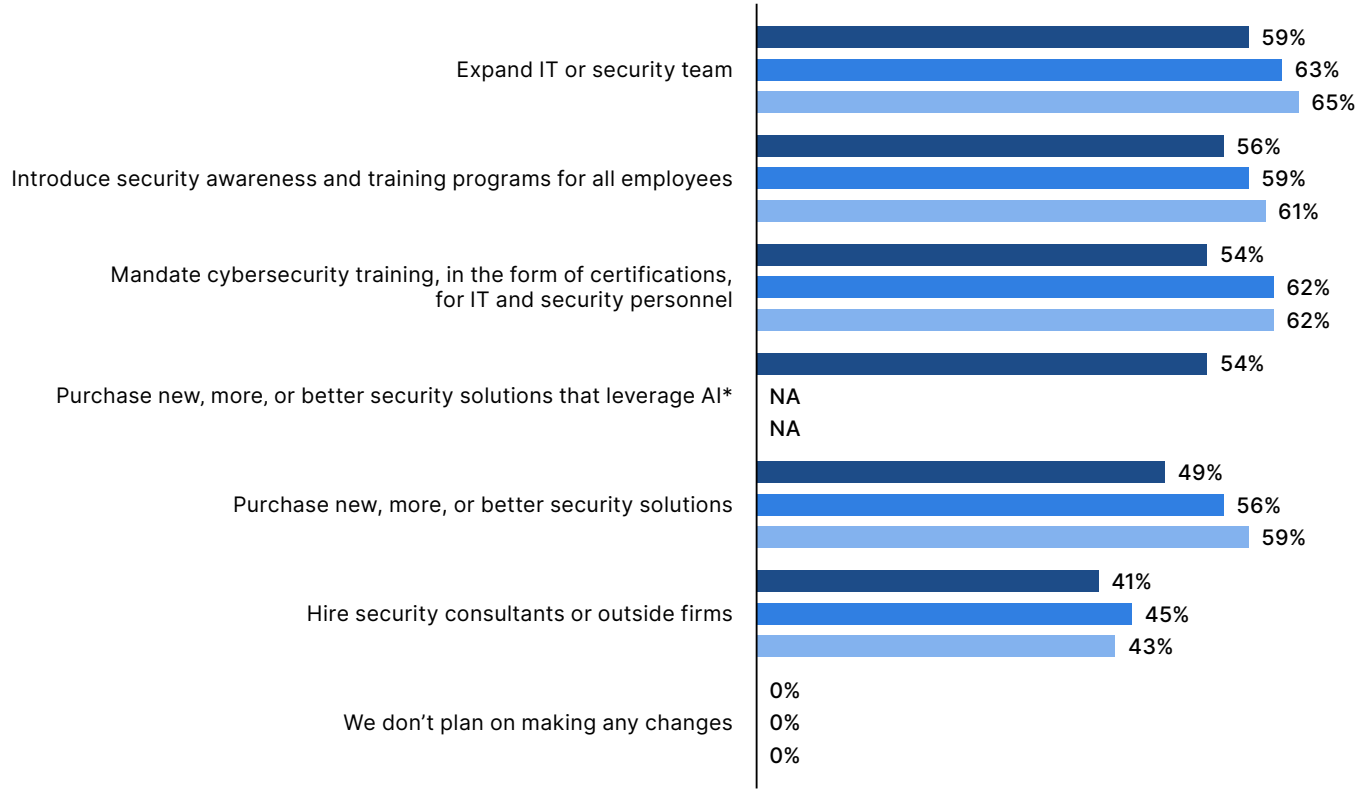


Big Movers

YoY Highlights

Data shows continued prioritization of internal capability building among organizations following a cyberattack in the past 12 months, with expanding IT and security teams remaining the top response from 2023 to 2025. Investment in awareness and training also holds steady, reinforcing a focus on internal resilience and a shift toward in-house capabilities.

PLANNED CHANGES FOLLOWING AN ATTACK

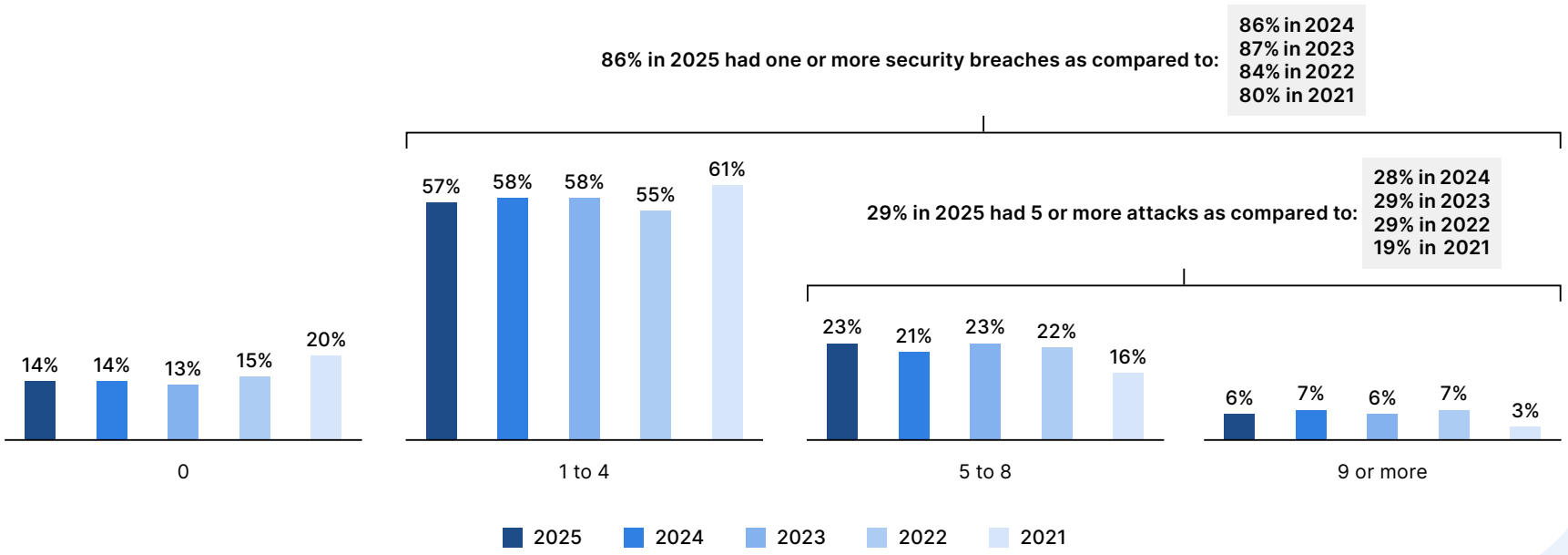


Note: Other = 0%; None of the above = 0%; Don't know/Unsure = 0%

* New answer option added this year, cannot be tracked.

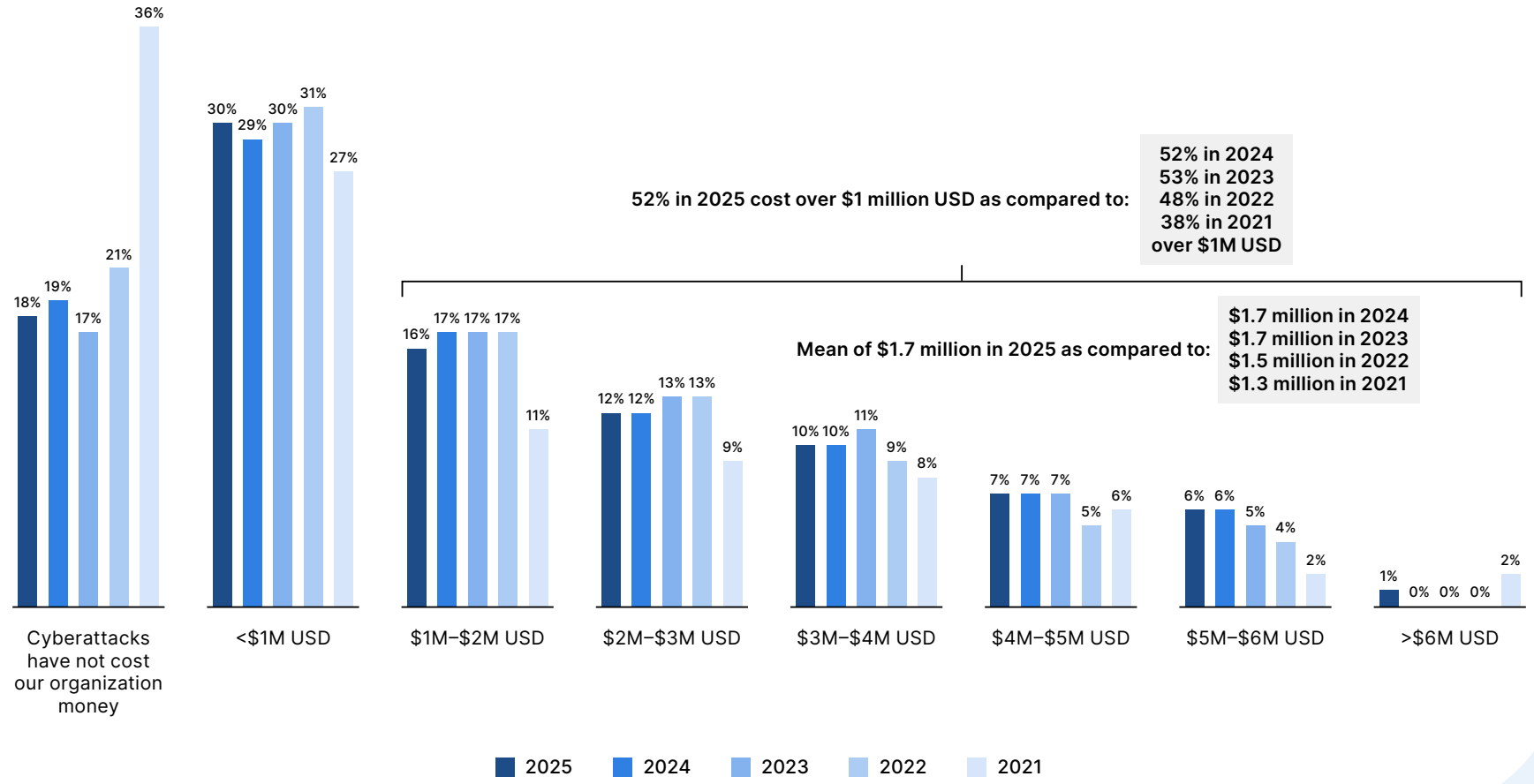
YoY Highlights

PERCENTAGES OF CYBERSECURITY BREACHES



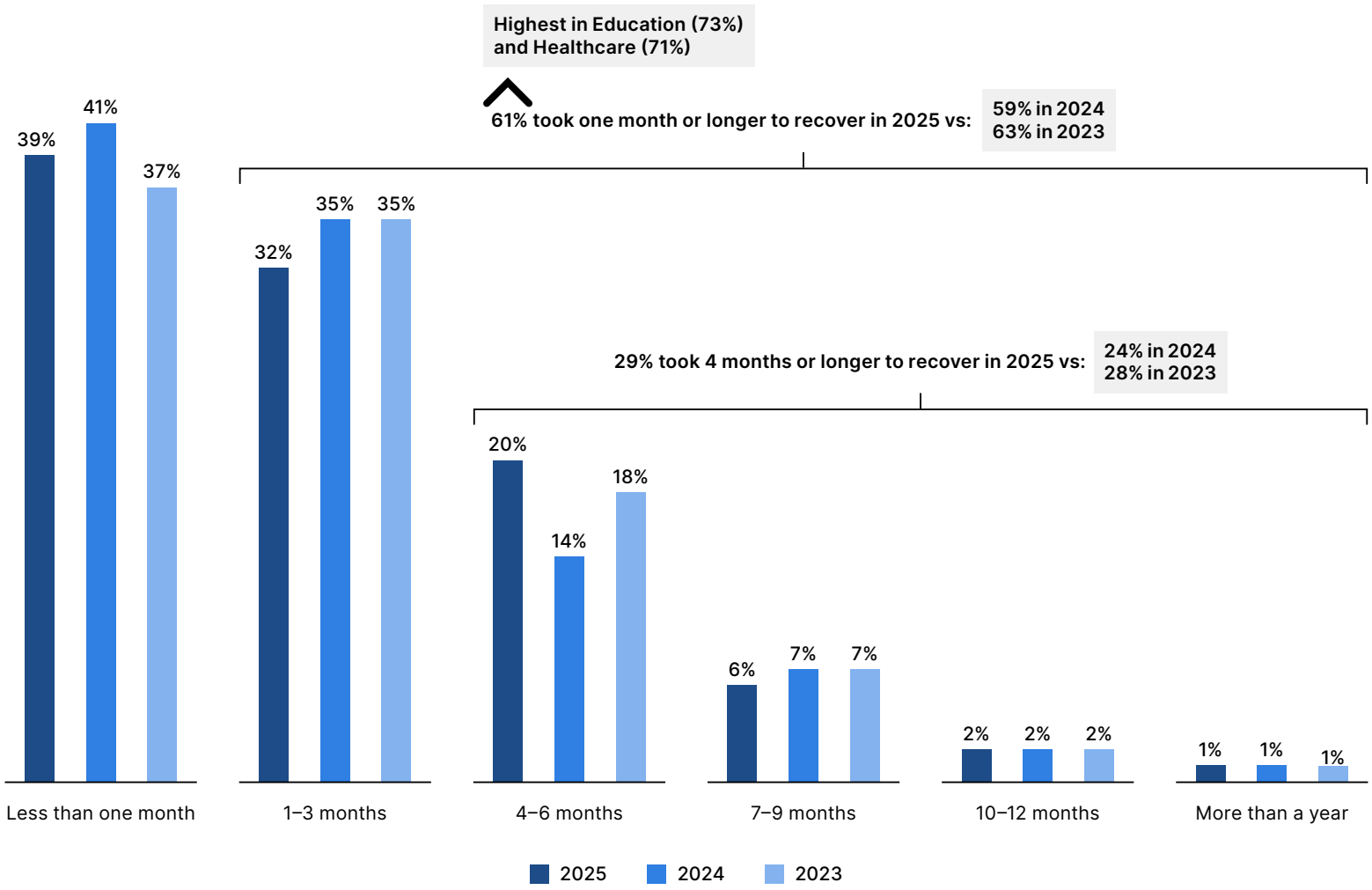
YoY Highlights

COST OF BREACHES



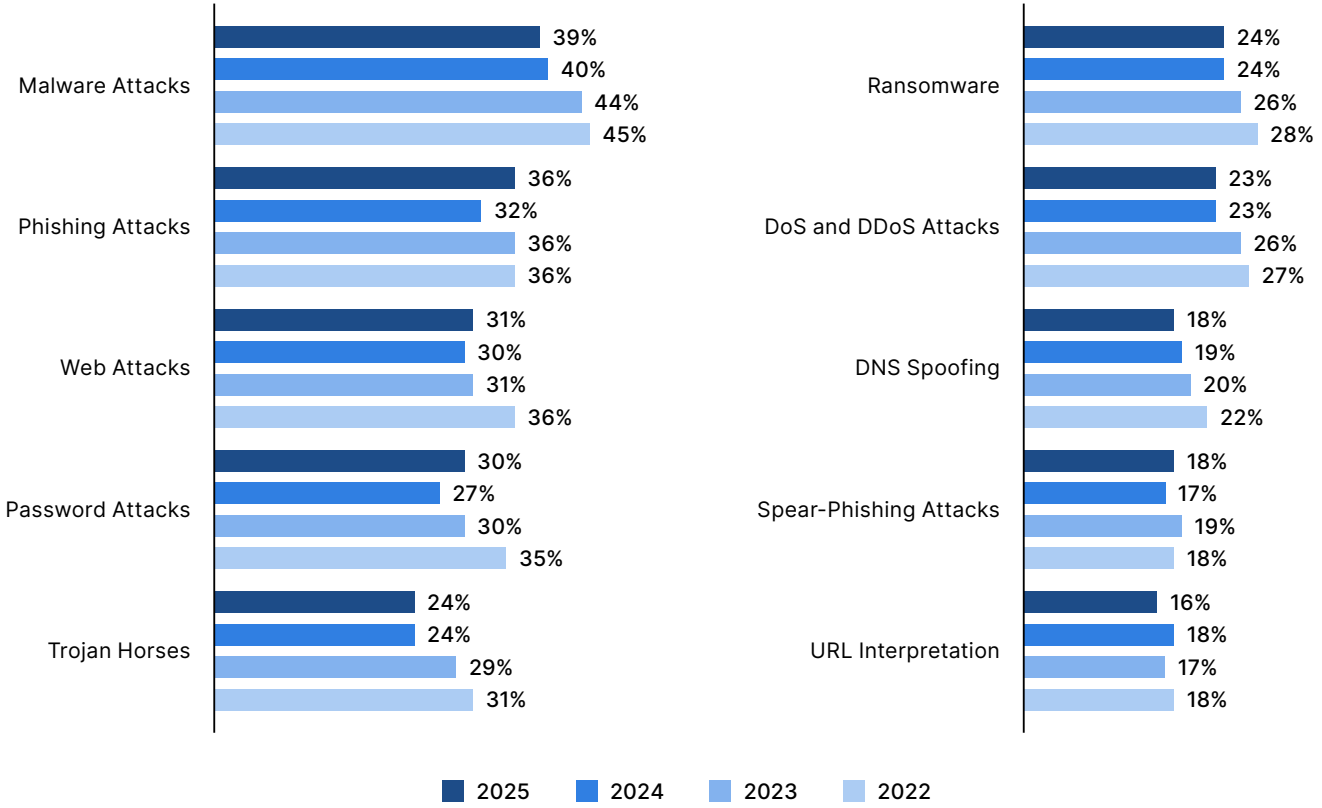
YoY Highlights

RECOVERY TIMES



YoY Highlights

TOP 10 ATTACK TYPES



Taking Action

Because humans are likely to remain the primary targets of cyberattacks for the foreseeable future, it is not surprising that human factors continue to be viewed as the leading cause of breaches. Phishing campaigns, credential theft, social engineering, and increasingly sophisticated deepfake attacks all exploit the human element of cybersecurity.

Expanding cyber teams and training

Organizations are responding by expanding cybersecurity teams, investing in employee awareness programs, and prioritizing certifications when hiring security professionals. The *2025 Security Awareness and Training Global Research Report* indicates that external threats remain the primary driver for implementing security awareness and training initiatives. Results show that 67% of organizations have seen a reduction in intrusions, incidents, and breaches since implementing training. However, a truly resilient security posture depends on integrating human capability with technological support. These efforts are critical, but they are most effective when combined with technology that helps compensate for human limitations.

Augmenting defense with AI

AI is emerging as one of the most promising tools to strengthen defenses. AI-enabled solutions can analyze massive volumes of security data, identify subtle anomalies, and surface threats that might otherwise go unnoticed. In areas such as detection and response, AI is already helping security teams detect patterns and respond more quickly to potential incidents.

However, AI should be viewed as an augmentation of human expertise rather than a replacement for it. The most resilient organizations combine strong security awareness programs with advanced detection technologies and well-trained cybersecurity professionals.

Maintaining this layered approach—blending people, processes, and technology—will remain essential as attackers continue to evolve their tactics and increasingly leverage AI themselves.

50% of leaders think their board members are fully aware of AI risks.

Board Inaction Is Driving Cyber Risk

In last year's report, we asked respondents to rate their corporate board members' awareness of the potential risks posed by AI use. The answer remains essentially unchanged this year, with just half (50%) saying their board members are "fully aware" (49% in 2024).

An additional 42% (same as in 2024) say their board members are "moderately" aware of AI risks. Because these numbers haven't improved, it suggests boards aren't getting better at understanding or educating themselves about AI risk and cybersecurity risk more broadly. Given how quickly AI is evolving, this low level of board awareness translates into strategic risks for organizations.

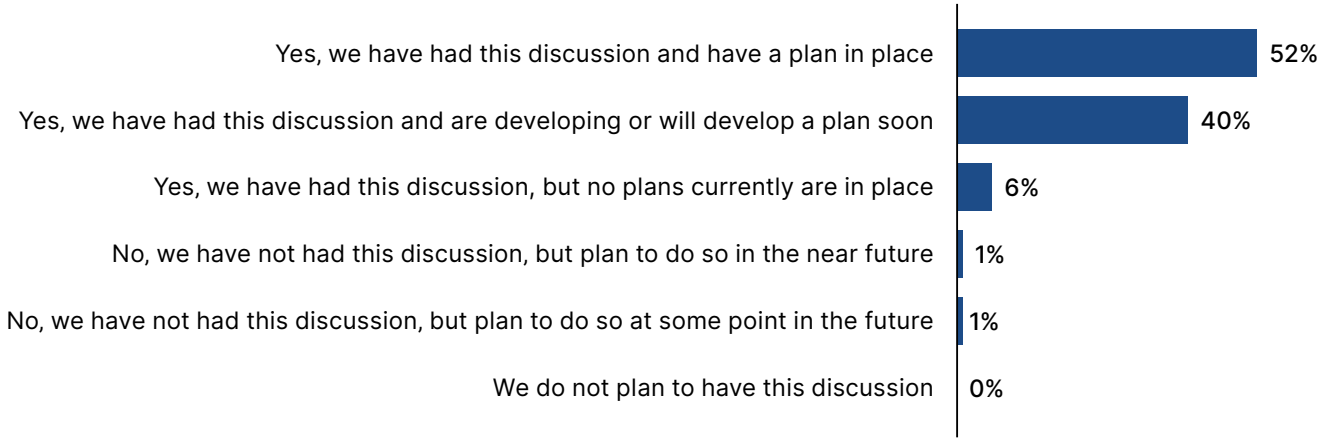
Testament to that, while 73% of respondents say cybersecurity is a business priority for their board of directors (up from 68% in 2024), only 59% say it is also a financial priority with budget behind it—down from 63% last year.

These shortcomings persist even though board members and executives continue to face penalties for cyber breaches, with 50% having faced fines, jail time, or loss of position or employment (down just slightly from 52% last year).

Breaches Call Out the Need for Cyber Resilience

Among organizations that experienced a cyberattack, slightly more than half (52%) say their board subsequently called for the creation of a cyber-resiliency plan.

Board response to resiliency plan discussions



Note: Don't know/Unsure = 0%

DIGGING DEEPER

Boards Need to Be Better Informed

Boards seem to recognize that cybersecurity matters

Despite the perception that board members are insufficiently aware of cyber and AI risks, many respondents say their boards continue to increase focus on cybersecurity:

- 78% report more board focus on cybersecurity (up from 76% in 2024 and 72% in 2023).
- 19% say the board's focus has remained the same (down from 21% in 2024 and 24% in 2023).
- 3% say their board is less focused on cybersecurity (2% in 2024, 3% in 2023).

Larger organizations have more confidence in board awareness of AI risks

Respondents from large and very large organizations are more likely to say board members are "fully aware" of risks from AI use:

- 62%: 2,500–4,999 employees
- 53%: 5,000+ employees
- 50%: 1,000–2,499 employees
- 49%: 500–999 employees
- 40%: 100–499 employees

Boards may not grasp the skills shortage risk

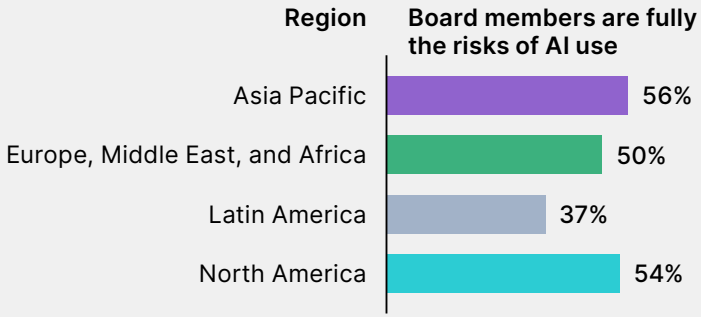
The potential risks associated with the cybersecurity skills shortage are not as widely recognized as they should be:

- 50% say their board has a "deep understanding" of skills shortage risks.
- 42% say their board has "general understanding."
- 7% say their board has "limited understanding."

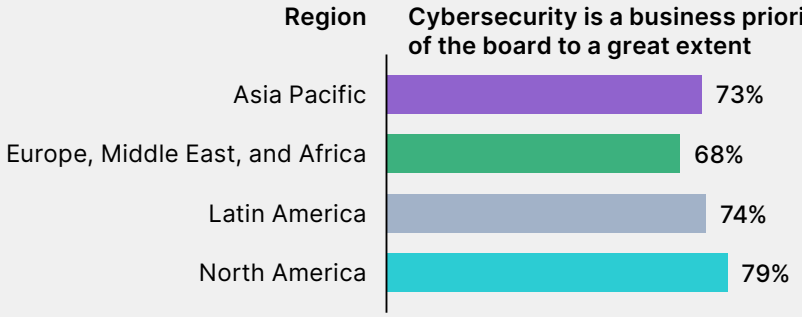
Just **50%** of organizations think their board has a "deep understanding" of the cybersecurity talent shortage and its potential risks.

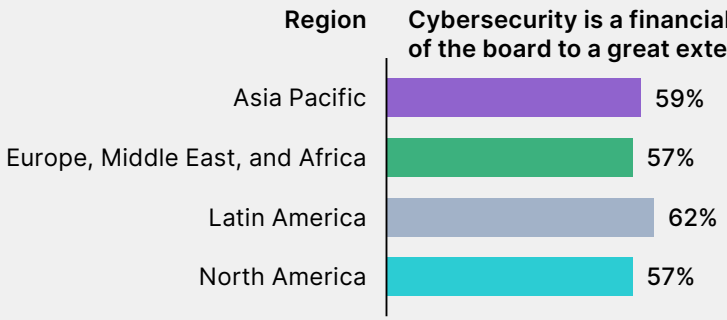
Regional Highlights

Board AI risk awareness is lowest in Latin America

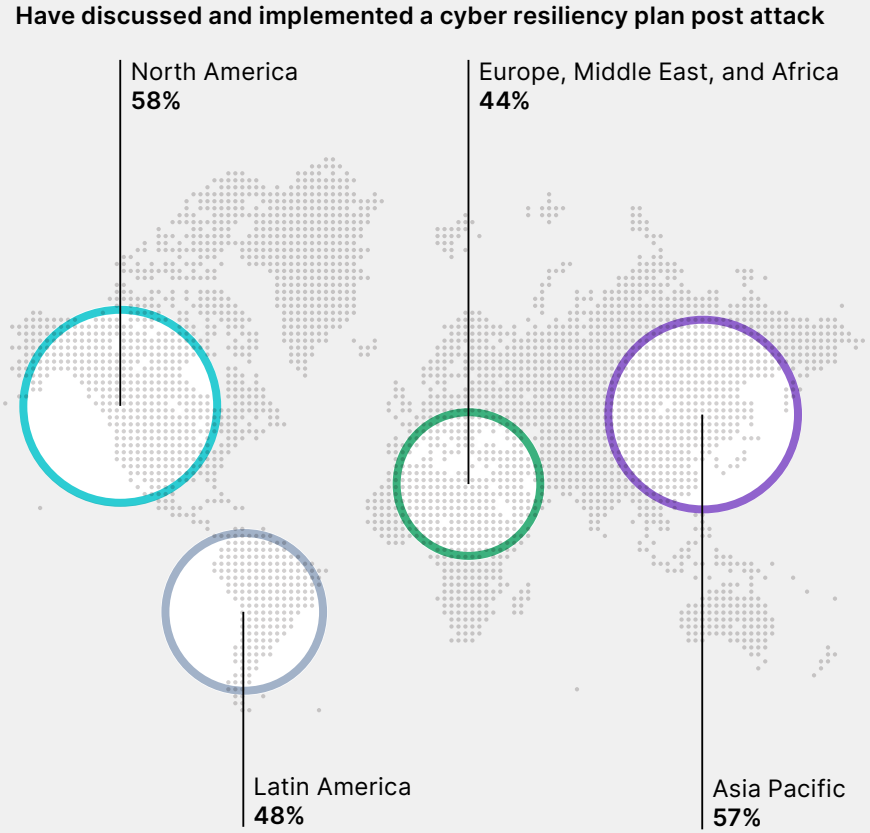


North American firms prioritize cybersecurity; Latin American firms prioritize spend on it





North America and Asia Pacific are most likely to have cyber resiliency plans

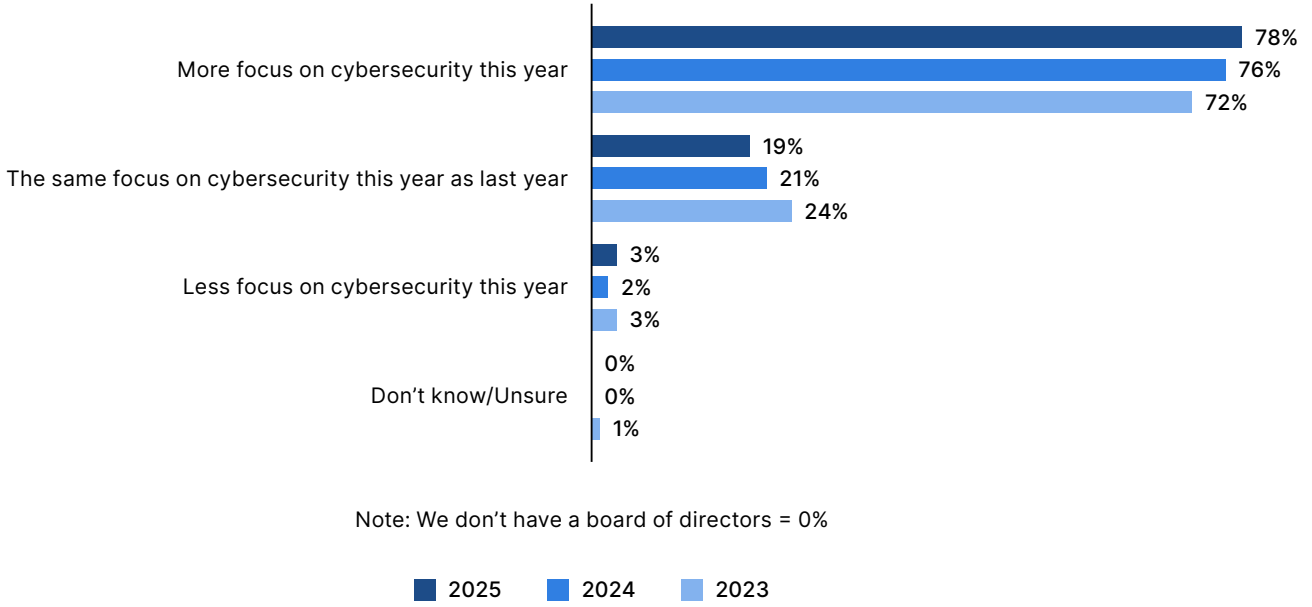


Big Movers

YoY Highlights

Each year, more respondents say their boards are increasing their focus on cybersecurity. Yet spending often lags behind prioritizing cybersecurity as a business concern, and respondents continue to have only moderate confidence in board awareness of AI-related cyber risks or the implications of the cybersecurity skills gap. Together, these data points raise a question about what exactly increased board focus on cybersecurity entails.

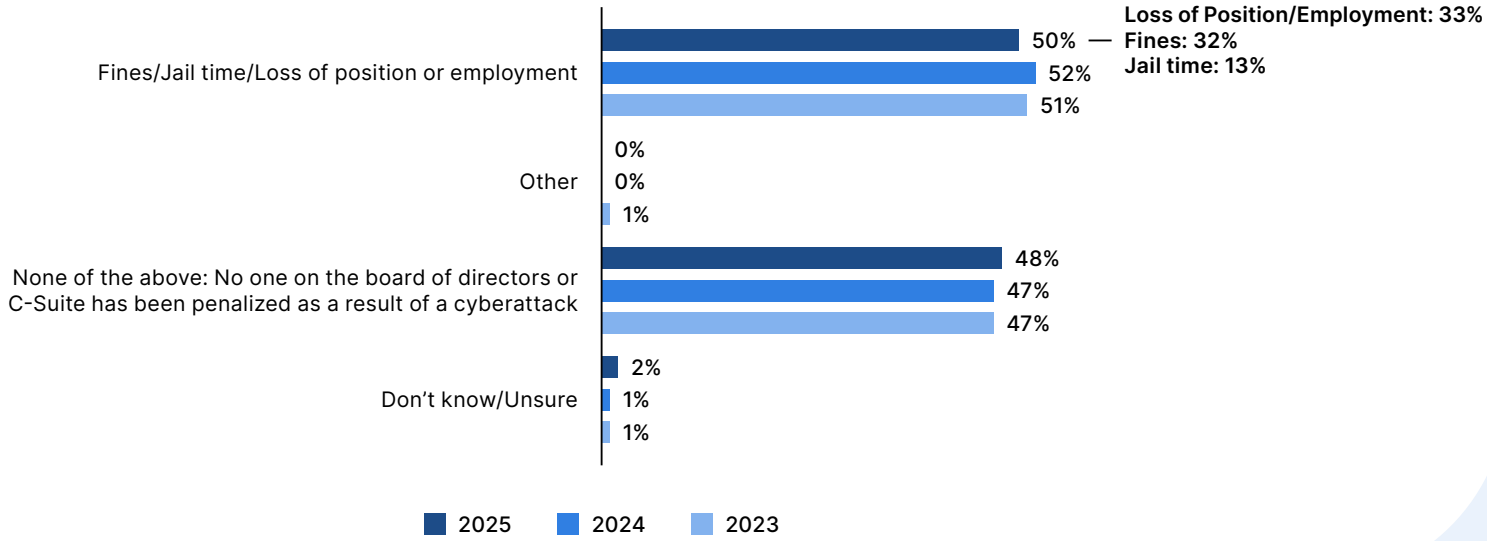
INCREASED BOARD FOCUS ON CYBERSECURITY



YoY Highlights

Three-year perspective

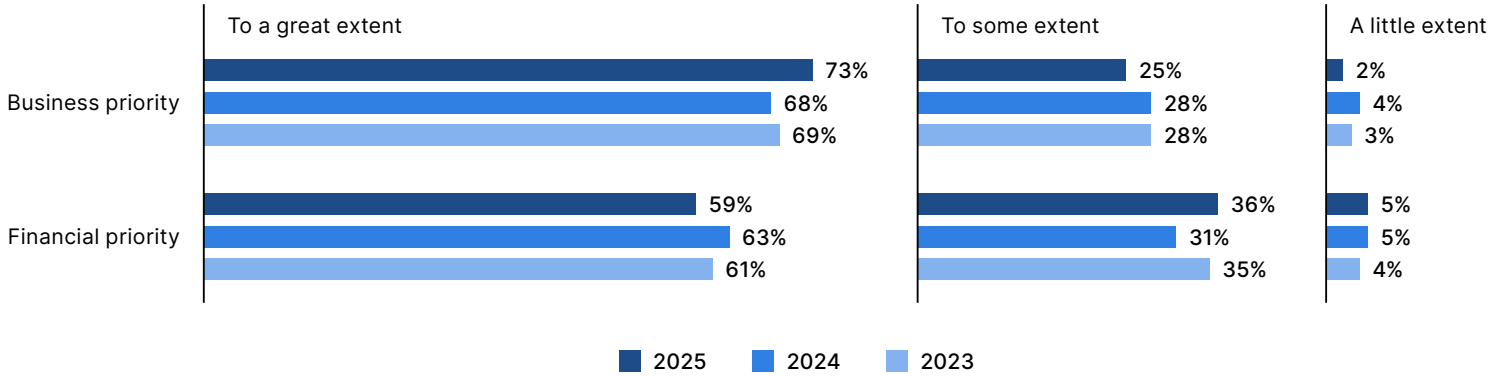
DIRECTOR AND C-SUITE PENALTIES FOR CYBERATTACKS



YoY Highlights

Three-year perspective

CYBERSECURITY AS A BUSINESS PRIORITY AND FINANCIAL PRIORITY



Taking Action

In recent years, there has been growing recognition that cybersecurity is not simply a technical issue but a strategic business risk. As a result, corporate boards are expected to play a greater role in overseeing cybersecurity management within their organizations.

This year's findings suggest that while boards generally recognize the importance of cybersecurity, many remain only partially engaged in addressing key issues such as emerging AI risks and the ongoing cybersecurity skills shortage.

Training is a must for board members

Boards can take meaningful action by investing in their own cybersecurity education and ensuring that cybersecurity expertise is represented at the board level. This may involve bringing in board members with cyber experience, engaging external advisors, or participating in structured training programs that help directors better understand evolving threats.

A cyber-aware board is better positioned to ask the right questions, allocate appropriate resources, and ensure that cybersecurity is treated as a core component of enterprise risk management.

Develop cyber-resilience strategies

Boards also play an important role in driving the development of cyber-resilience strategies. Cyber resilience refers to an organization's ability to continue operating even during or after a cyber disruption. Effective resilience planning requires leadership alignment across business units not just technical teams.

Rather than focusing on day-to-day security controls, boards should prioritize high-level preparedness and response by asking:

- Are we protecting the systems and data that matter most to the business?
- How quickly would we detect a breach?
- How quickly could we restore critical operations?
- Are leadership teams prepared to manage a cyber crisis?

To reinforce readiness, organizations should conduct regular tabletop exercises that simulate real-world cyber incidents. These exercises help validate response plans, clarify roles and decision-making processes, and expose gaps in coordination across leadership teams.

By prioritizing these strategic discussions and preparedness activities, boards can ensure cybersecurity is embedded within broader business continuity and risk management planning.

60% of respondents say their top recruiting challenge is finding cybersecurity talent with specific experience in AI.

The Cybersecurity Skills Gap Is Growing with AI

Most respondents (71%) say the cybersecurity skills shortage continues to pose a risk to their organizations, an increase from 67% in 2024. Finding candidates with AI experience in cybersecurity is emerging as a growing recruitment challenge, with 60% of respondents reporting it in 2025 (up from 57% last year).

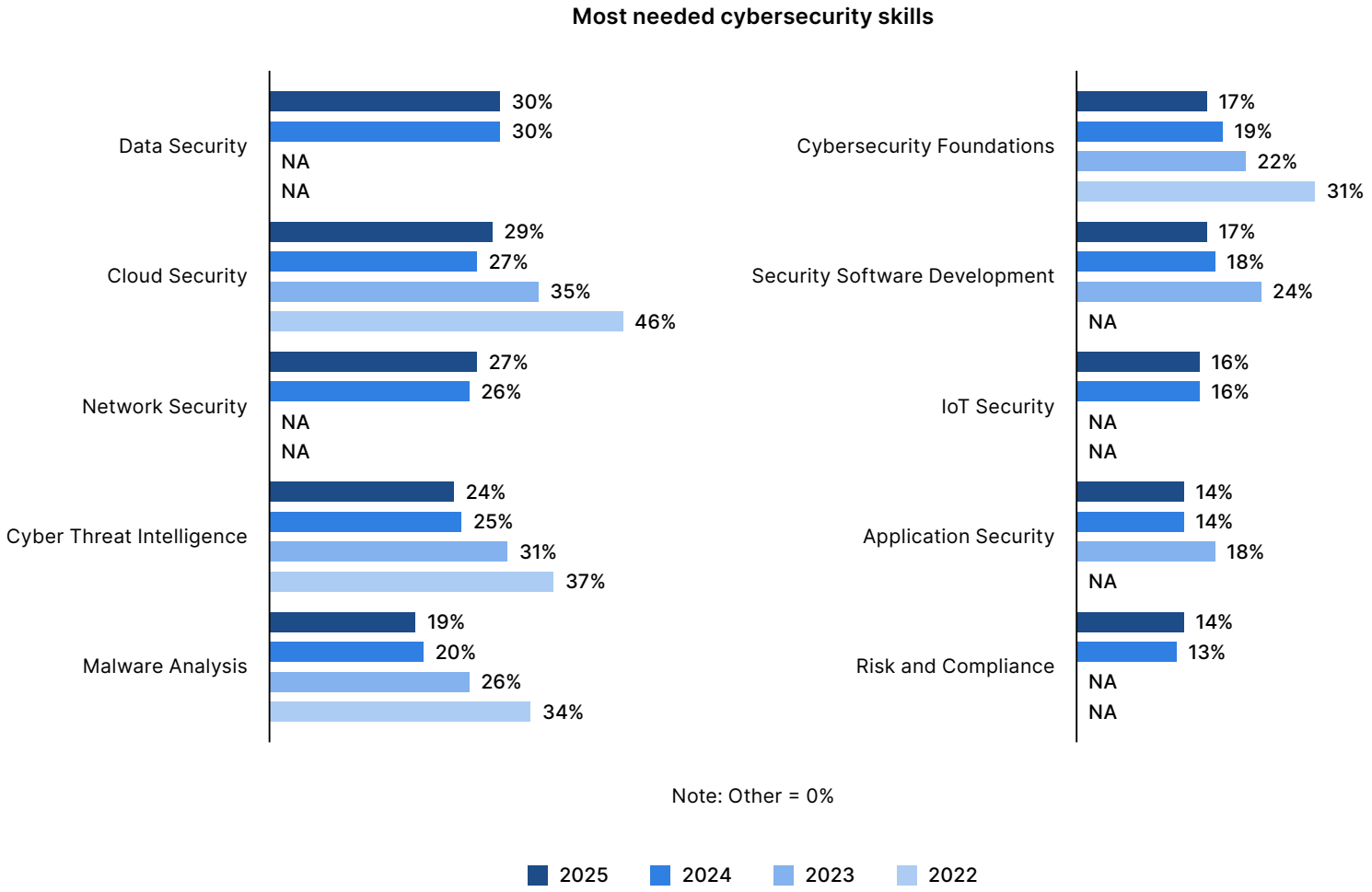
This could be concerning, given that 63% expect greater need for AI oversight and governance roles over the next three years, and 49% believe they may need to create new AI-driven roles. Fifty-seven percent (57%) expect to require reskilling or upskilling of existing staff to work with AI tools.

AI, of course, is not the only area where organizations face recruitment challenges. More than half of respondents (56%) say they struggle to recruit and hire cybersecurity talent (up from 52% in 2024), and 49% report difficulty securing approval for additional cybersecurity headcount (47% last year). Fifty-one percent (51%) say they need senior-level cybersecurity skills most of all, compared to 32% for mid-level and 13% for entry-level roles.

Beyond recruitment, 52% of respondents say their organization also struggles to retain cybersecurity talent (50% last year).

Top Skills Continue to Evolve

The most in-demand cybersecurity skills have shifted over the past four years, reflecting the introduction of new roles and emerging technologies. While some core capabilities remain consistently important, changing priorities highlight how organizations are adapting to an increasingly complex threat landscape and continuing to face challenges in finding the right talent.



DIGGING DEEPER

Scarce Talent Makes Hiring Fiercely Competitive

Finding and competing for talent are top recruitment challenges

Respondents say they struggle to find candidates with specific skills and also to compete on compensation:

- 60% struggle to find candidates with specific AI experience in cybersecurity (57% last year).
- 59% struggle to find candidates with specific network engineering and security experience (58% last year).
- 31% find it challenging to compete with other organizations on salary and benefits (30% last year).

Retention continues to hinge on training and upskilling

Employees value training and upskilling opportunities enough that not offering them can erode retention, along with other factors:

- Lack of training and upskilling (48%, same as last year)
- Better salaries and benefits offered by competitors (40%, down from 42% last year)
- Remote and hybrid work arrangements (35%, down from 38% last year)

AI adoption demands new skillsets

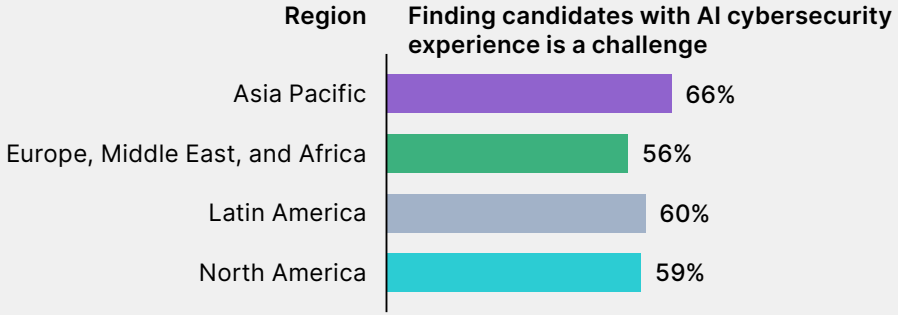
Organizations say they require staff with new skillsets to support their adoption of AI, including:

- AI model development (55%)
- AI tool oversight (54%)
- Security automation (52%)

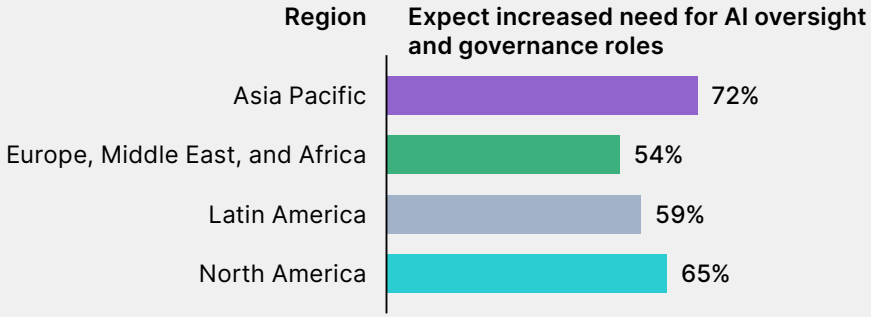
48% of organizations say a lack of training and upskilling opportunities can negatively affect retention.

Regional Highlights

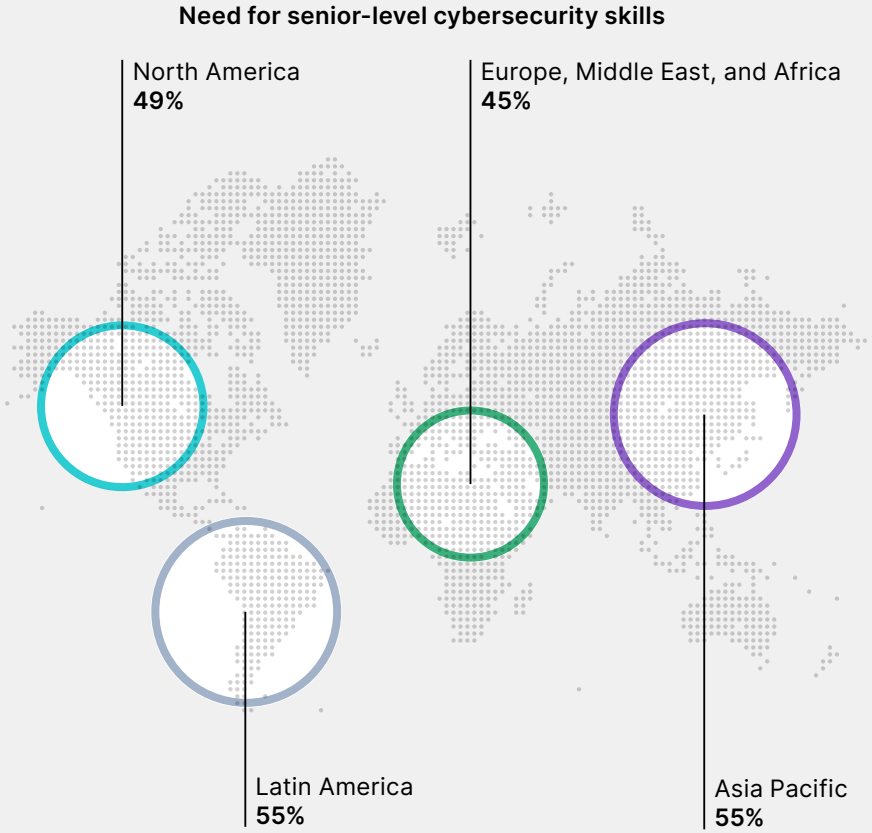
Asia Pacific organizations say it's hardest to find AI cybersecurity experience



Asia Pacific organizations most expect to need AI roles



Latin American and Asia Pacific organizations most need senior skills

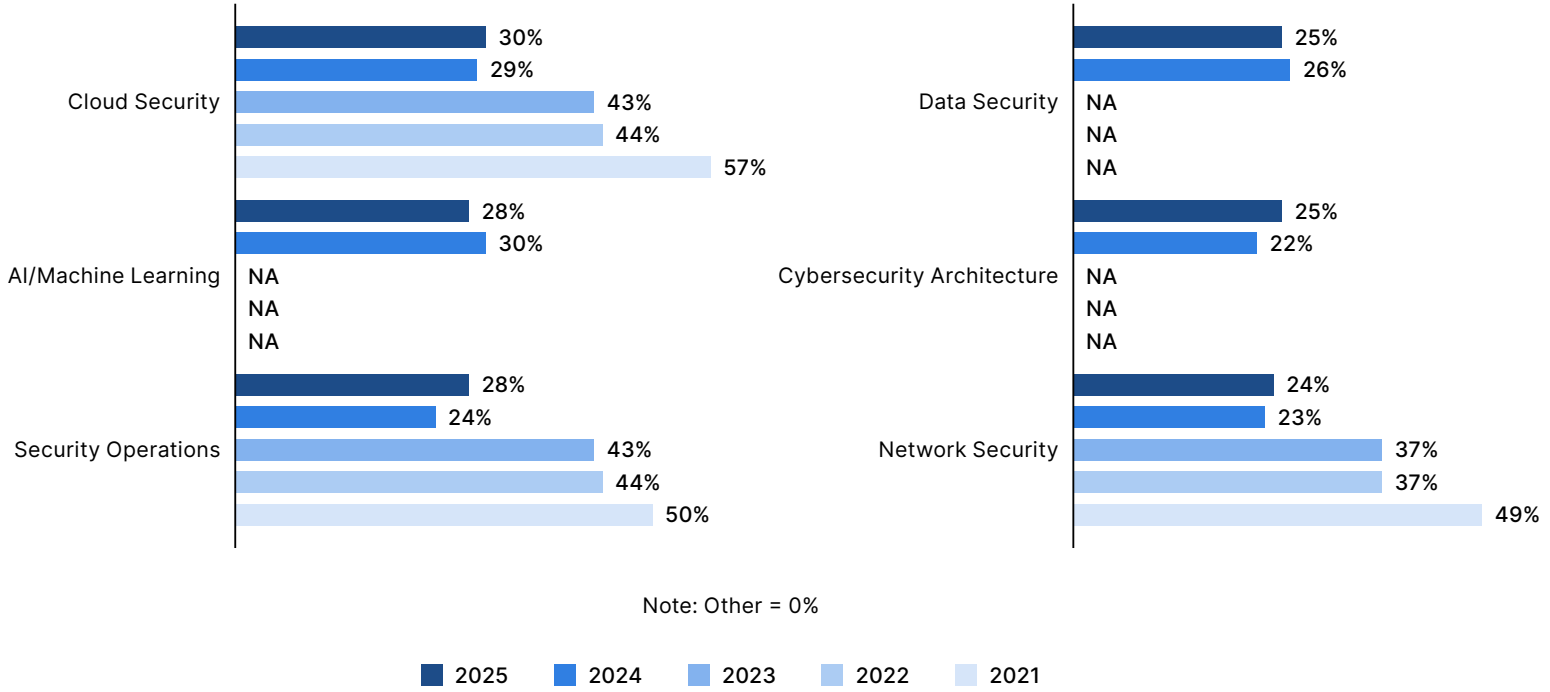


Big Movers

YoY Highlights

Five years ago, Cloud Security, Security Operations, and Network Security were reported as being the hardest cybersecurity roles to fill. The addition of new categories—AI/Machine Learning, Data Security, and Cybersecurity Architecture—significantly shifted the balance, with AI/Machine Learning roles jumping to second place.

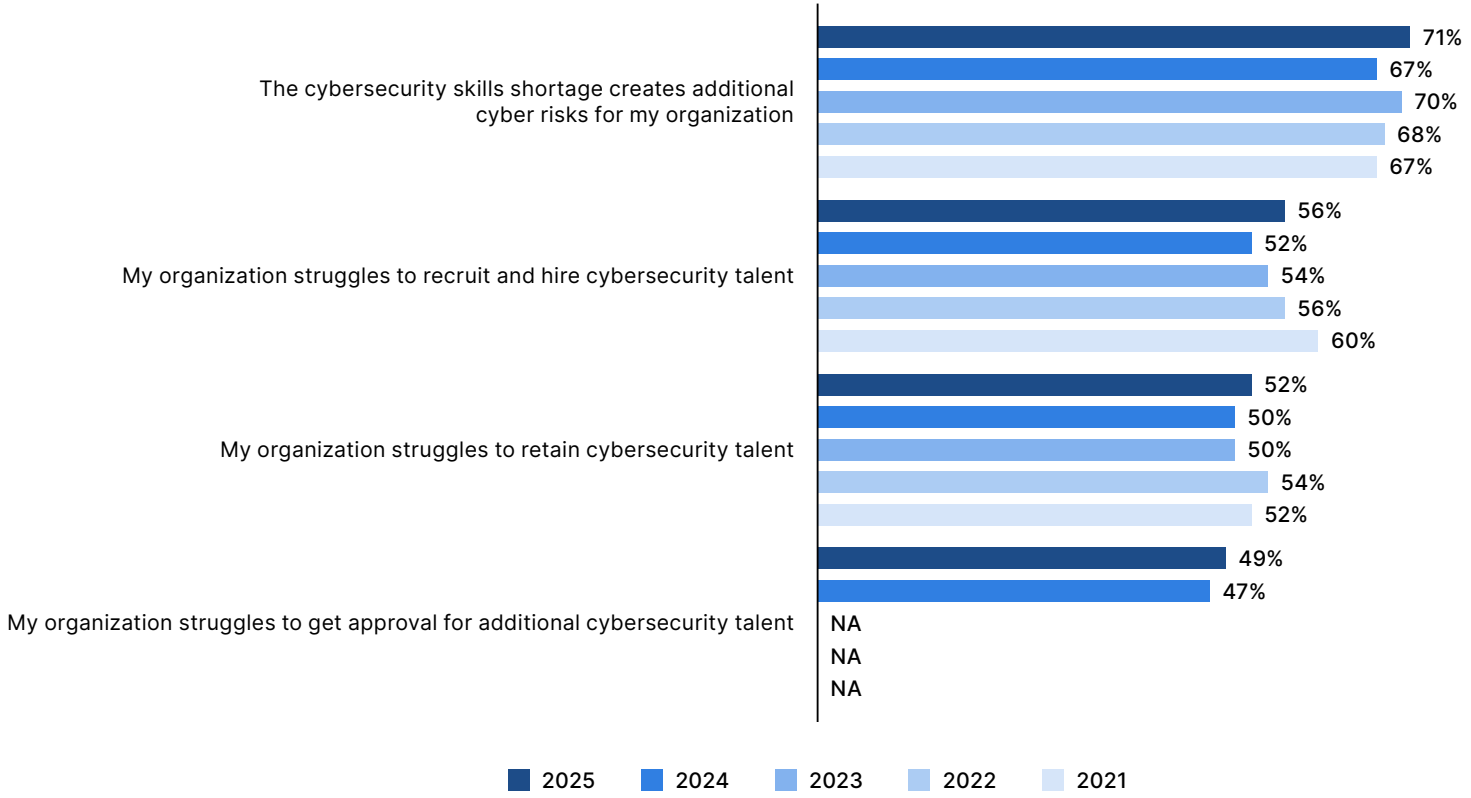
SKILLS SHORTAGE CHALLENGES



Note: Other = 0%

YoY Highlights

SKILLS GAP CHALLENGES



YoY Highlights

TOP RECRUITING CHALLENGES

Note: Other = 0%; Don't know/Unsure = 0%

YoY Highlights

TOP RETENTION CHALLENGES

Note: Other = 0%

Taking Action

This year's findings reinforce a familiar reality. The cybersecurity skills shortage remains a significant challenge for organizations worldwide. In fact, the rapid emergence of AI technologies may be intensifying the problem by creating demand for specialized skills that are still relatively scarce.

While recruiting new talent remains important, organizations should recognize that their existing cybersecurity workforce is one of their most valuable assets. Investing in retention and professional development can help alleviate the pressure caused by limited hiring pools.

Retain talent through growth, training, and opportunity

Survey results show that compensation and benefits remain important factors for retaining talent, but they are not the only ones. Opportunities for training, career growth, and professional certification are often just as influential in keeping skilled cybersecurity professionals engaged and motivated.

Organizations can take several practical steps to strengthen retention:

- Provide structured training and certification pathways
- Encourage cross-training in emerging areas such as AI and automation
- Offer clear career progression opportunities within cybersecurity roles

Upskilling existing team members can also help organizations fill skill gaps more efficiently than relying solely on external hiring. Experienced security professionals who understand the organization's environment can often adapt quickly to new technologies with the right training.

Leverage AI for the simple tasks

Finally, organizations should seek opportunities to use AI and automation to reduce repetitive workloads—such as alert triage and log analysis—enabling cybersecurity professionals to focus on higher-value activities like threat hunting, strategic defense planning, and incident response.

91% of IT decision makers prefer to hire candidates with technology-focused certifications.

Certifications Remain Highly Valued

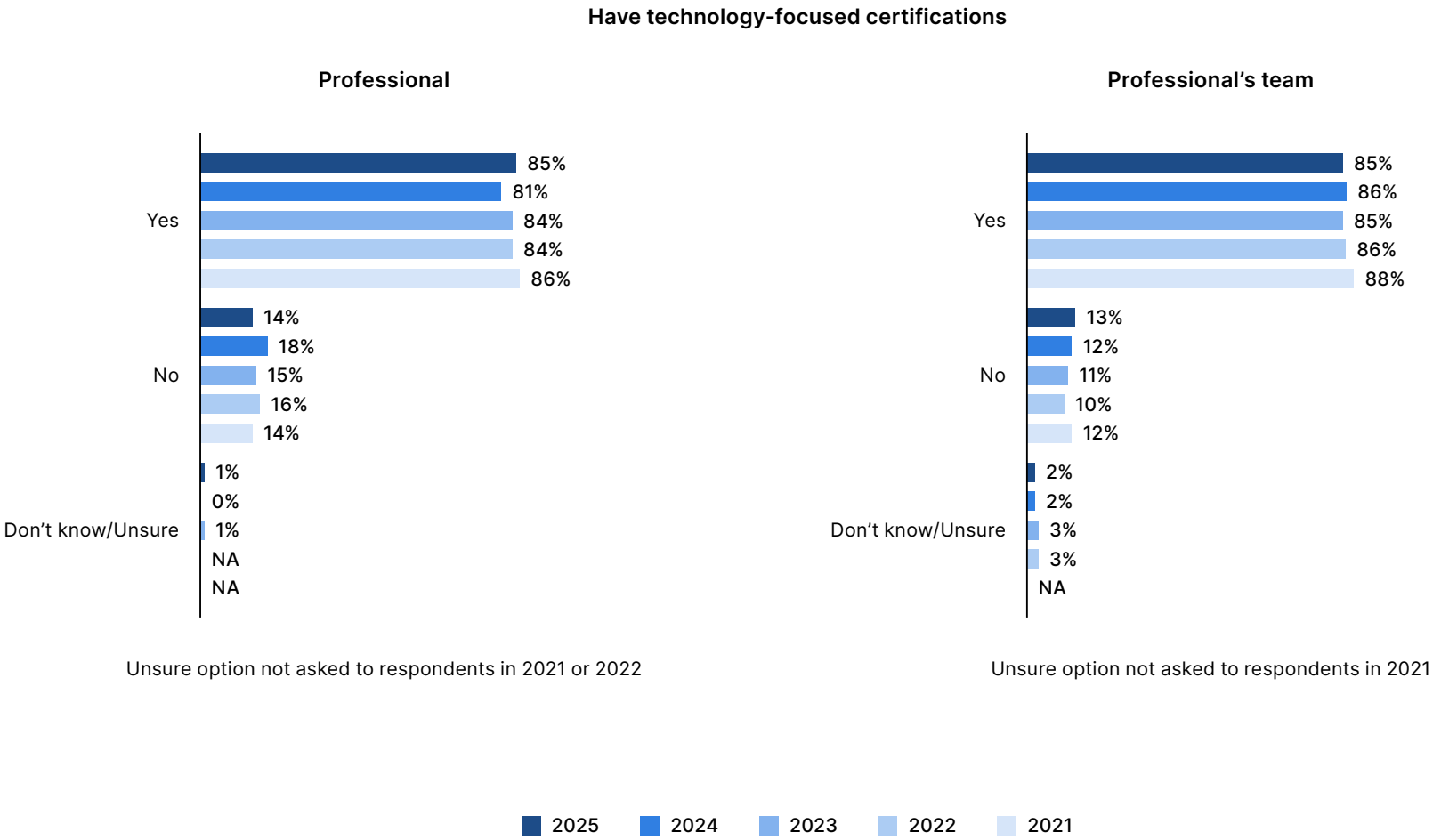
Nearly all (91%) IT decision makers say they prefer to hire candidates with technology-focused certifications, consistent with 89% in 2024 and 91% in 2023. Of those who have this preference, 67% say they look for certifications in a team member or direct report because it validates their cybersecurity awareness and knowledge (the same as in 2024 and 2023).

A surprise in last year's survey results was that only 73% of respondents were willing to pay for a candidate to obtain a certification—down from about 89% in 2023. In 2025, willingness to pay returned to historical levels at 92% for this specific measure.

Of those who continue to say they would not pay for employee certification, the top reasons given were the risk of losing talent after they've been certified (32%), budget constraints (28%), the belief that AI can teach the same skills as a certification (26%) and the belief that AI can simplify related tasks or the role in question (23%).

Respondents Are Equally Likely to Be Certified and Have Certified Team Members

Eighty-five percent (85%) of respondents say they have personally received technology-focused certifications. The same percentage of respondents report having someone on their team with such a certification.



Unsure option not asked to respondents in 2021 or 2022

Unsure option not asked to respondents in 2021

DIGGING DEEPER

Certifications Meet Expectations and Growing Needs

Certifications are the top-favored credential

Most employers prefer certifications to four-year degrees. This complements and supports the finding that 91% of IT decision-makers prefer to hire candidates with technology-focused certifications:

- 66% prefer candidates with professional certifications (65% last year).
- 56% prefer candidates with a four-year degree (52% last year).
- 42% prefer candidates with a diploma (43% last year).

Certifications are considered more often in certain sectors

Professional services and technology organizations are most likely to look for certifications, while educational and government organizations are least likely:

- 72% of professional services organizations look for certifications.
- 69% of technology organizations look for certifications.
- 56% of educational organizations look for certifications.
- 55% of government organizations look for certifications.

AI-related cybersecurity training is in the plans

Most organizations say they expect to invest in AI-related cybersecurity training or certifications in the next 12 months:

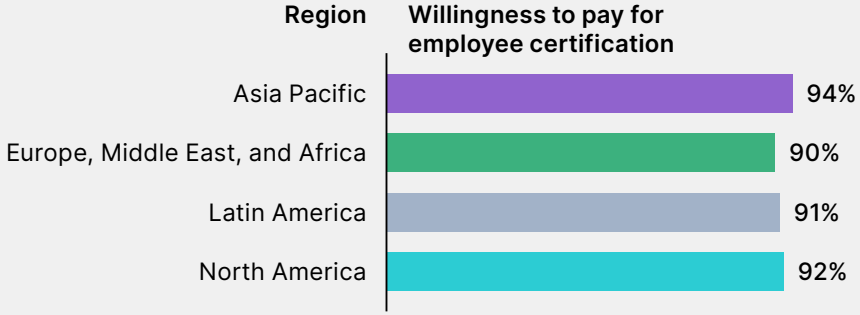
- 58% say they are very likely to invest in AI-related cybersecurity training or certifications.
- 34% say they are somewhat likely.
- 5% say they are neither likely nor unlikely.

92% of organizations say they are likely to invest in AI-related cybersecurity training or certifications in the next 12 months.

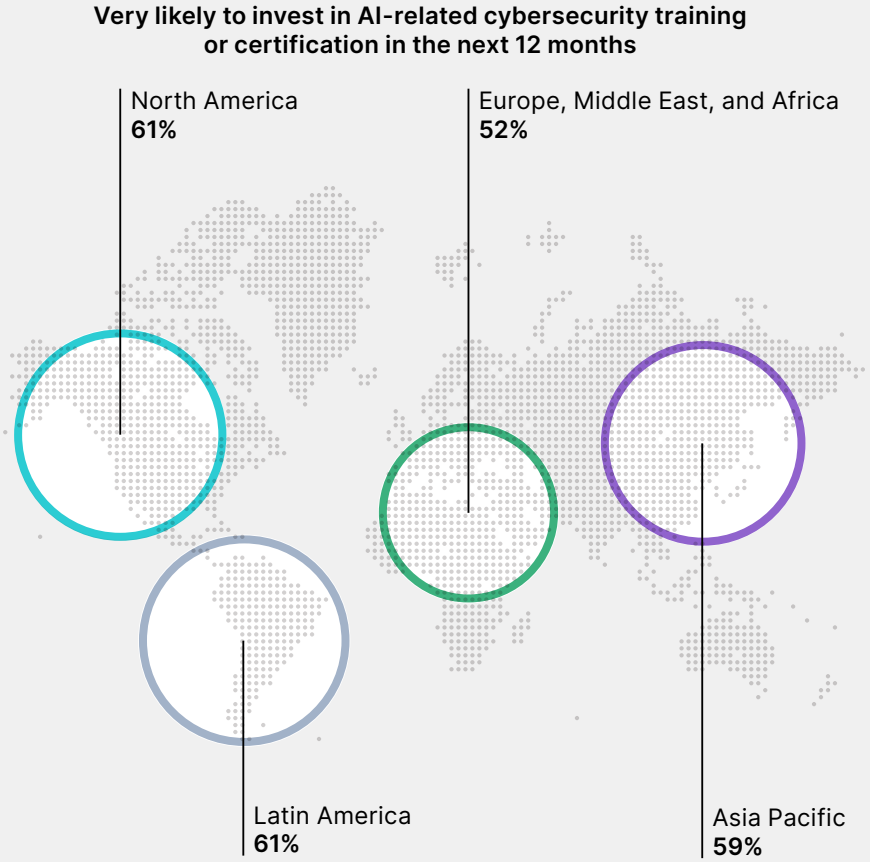
Regional Highlights

Certifications are most often considered in North America and Latin America

Asia Pacific organizations are most likely to pay for certifications



AI training and certification are likeliest in North America and Latin America

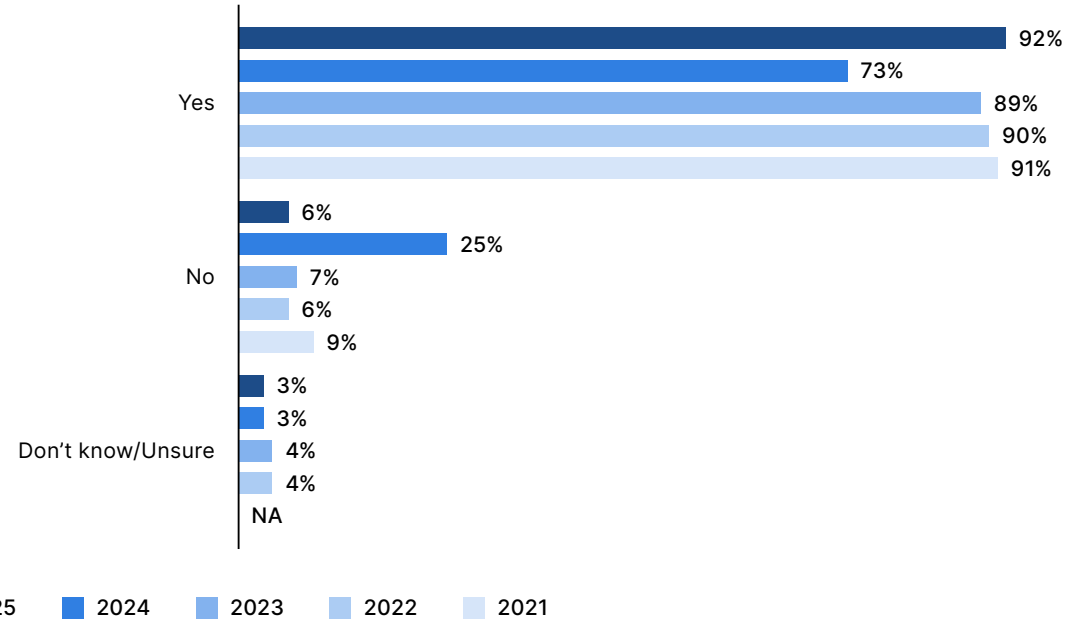


Big Movers

YoY Highlights

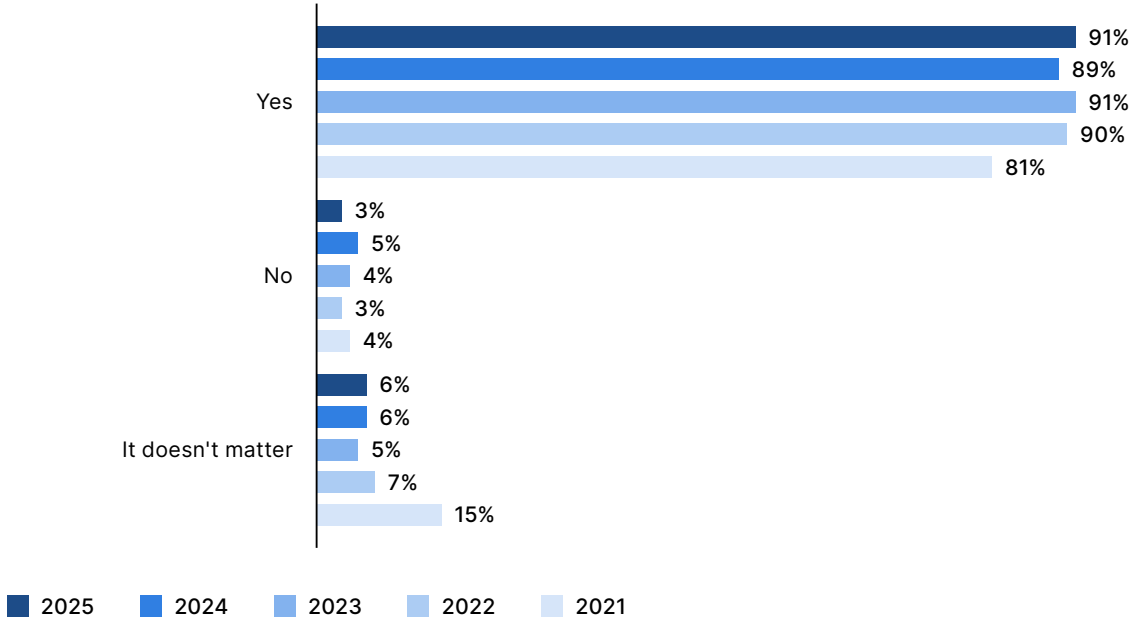
Willingness to pay for cybersecurity certification dropped off suddenly in 2024 but rebounded and even exceeded previous years in 2025. While the cause of the dip is unknown, new survey questions about why some organizations are unwilling to pay should shed light on any future changes.

WILLINGNESS TO PAY FOR CERTIFICATION



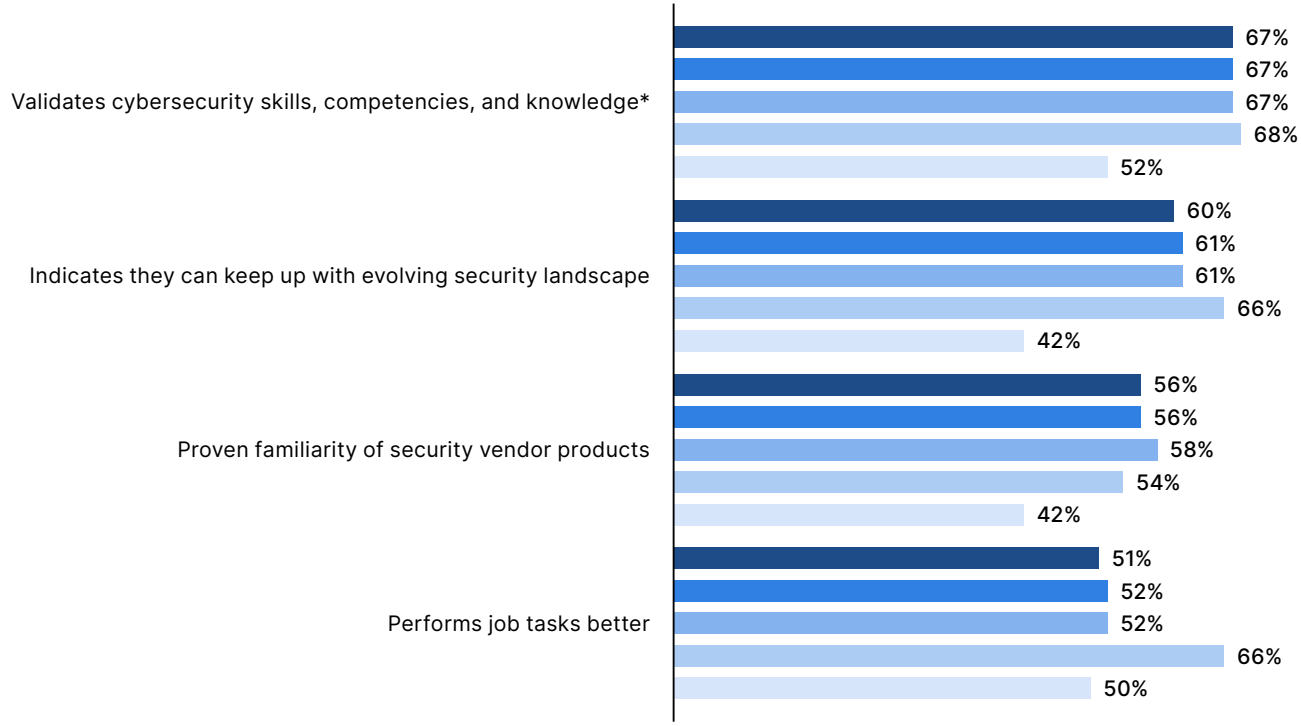
YoY Highlights

PREFERENCE TO HIRE PEOPLE WITH CERTIFICATIONS



YoY Highlights

WHY CERTIFICATIONS ARE PREFERRED



Note: Please note that this question was asked as a select all that apply since 2021
Note: Other=0%

* Answer option tweaked in 2024 from 'Validates cybersecurity awareness and knowledge' to include 'competencies'.

Taking Action

Certifications continue to play an important role in validating cybersecurity knowledge and skills, particularly from the perspective of IT decision-makers and hiring managers. For many organizations, certifications provide a reliable way to evaluate candidates and ensure that employees have demonstrated competence in key technical areas.

However, organizations can gain even greater value from certifications by adopting a more strategic approach to their use.

Align workforce skills with emerging technologies

One effective strategy is to align certification investments with the organization's risk profile and security priorities. By conducting regular risk assessments, organizations can identify which skill areas are most critical and ensure that training and certification programs support those needs.

Integrate certifications into career development strategies

Encouraging certification among existing employees can also support professional development and retention. When certifications are integrated into career progression plans or performance evaluations, they become powerful incentives for employees to continue building their expertise.

Support for employer willingness to pay for certifications rebounded this year after seeing a decline last year. Organizations may benefit from programs that identify internal champions who actively advocate for continued investment in certification programs.

Linking certifications to structured learning pathways, mentorship programs, and real-world experience can help ensure that credentials translate into practical capabilities that strengthen an organization's overall security posture.

71% have formal targets for cybersecurity hiring from underutilized talent pools.

Organizations Should Continue Broadening Cybersecurity Recruiting Efforts

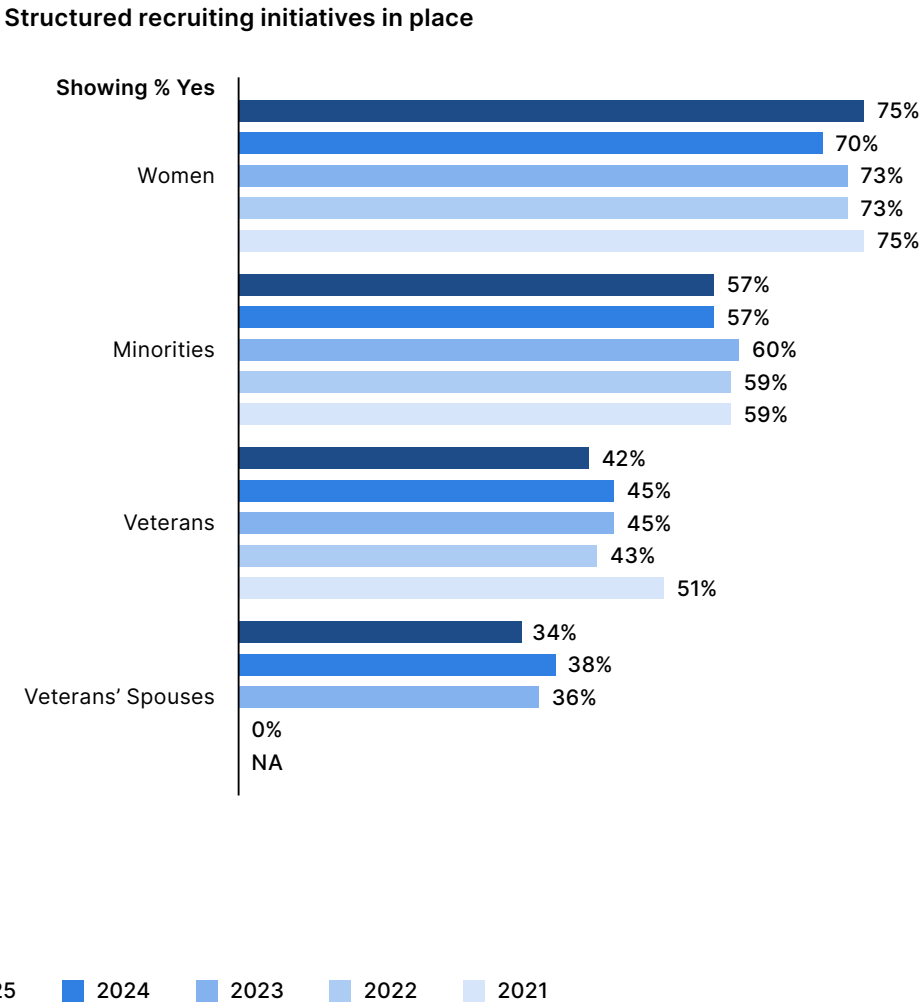
The ongoing skills shortage, combined with the emerging need for new AI-related roles and skillsets, reaffirms the importance of casting a wider net when organizations are trying to recruit talent. This seems to be understood, given that 71% of respondents report formal targets for cybersecurity hiring from underutilized talent pools.

Just as investors diversify portfolios to mitigate risk and companies broaden their customer base to avoid over-reliance on any single segment, organizations must also diversify their talent pools to meet cybersecurity skills needs.

While organizations have been making efforts in this regard, to date, the composition of the IT and cybersecurity workforce hasn't changed substantially. Twenty-six percent (26%) of respondents say their IT/cybersecurity employees are women, about the same as in 2024 (27%). Twenty percent (20%) are from minority populations, unchanged from the previous year; 16% are veterans, and 14% veterans' spouses (17% and 15% respectively in the last survey).

Women Are the Top Target of Structured Recruiting Initiatives

As in previous years, more organizations report structured initiatives to recruit women than any other underrepresented talent group, with people from minority backgrounds a distant second.



DIGGING DEEPER

Recruiting Underrepresented Talent Is Getting Harder

Organizations use a mix of tactics to attract underrepresented talent

To reach out to different talent pools, organizations rely on the following:

- Internships and apprenticeship programs: 51%
- Academic partnerships: 50%
- Partnerships with diversity-focused nonprofits or training programs: 49%

Smaller organizations are less likely to formally recruit from underutilized pools

Organizations with 100–499 employees are least likely to have structured or formal recruiting initiatives for:

- Women: 72% (highest is 76% for 2,500–4,999 employees)
- Minorities: 51% (highest is 60% for 5,000 or more employees)
- Veterans: 36% (highest is 47% for 2,500-4,999 employees)
- Veterans' spouses: 27% (highest is 41% for 2,500–4,999 employees)

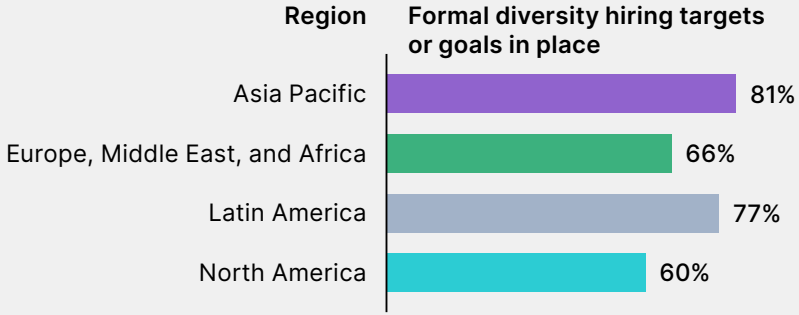
Qualified veterans and veterans' spouses remain elusive

- Veterans and veterans' spouses continue to be the most difficult qualified individuals to find, though minorities and women also show significant jumps in difficulty:
- Veterans: 43% difficult (43% last year)
- Veterans' spouses: 43% difficult (41% last year)
- Minorities: 34% difficult (29% last year, a notable jump)
- Women: 31% difficult (20% last year, also a significant jump)

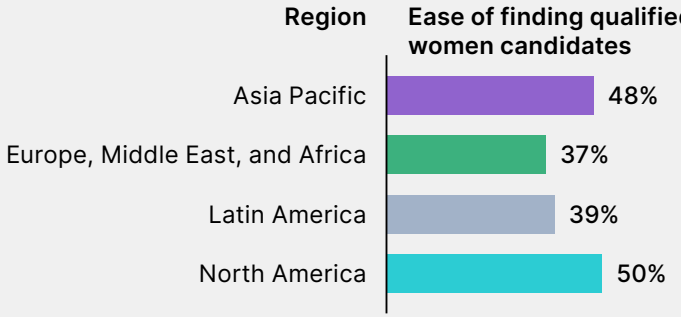
More organizations are finding it difficult to find qualified women candidates—**31%** compared to 20% last year.

Regional Highlights

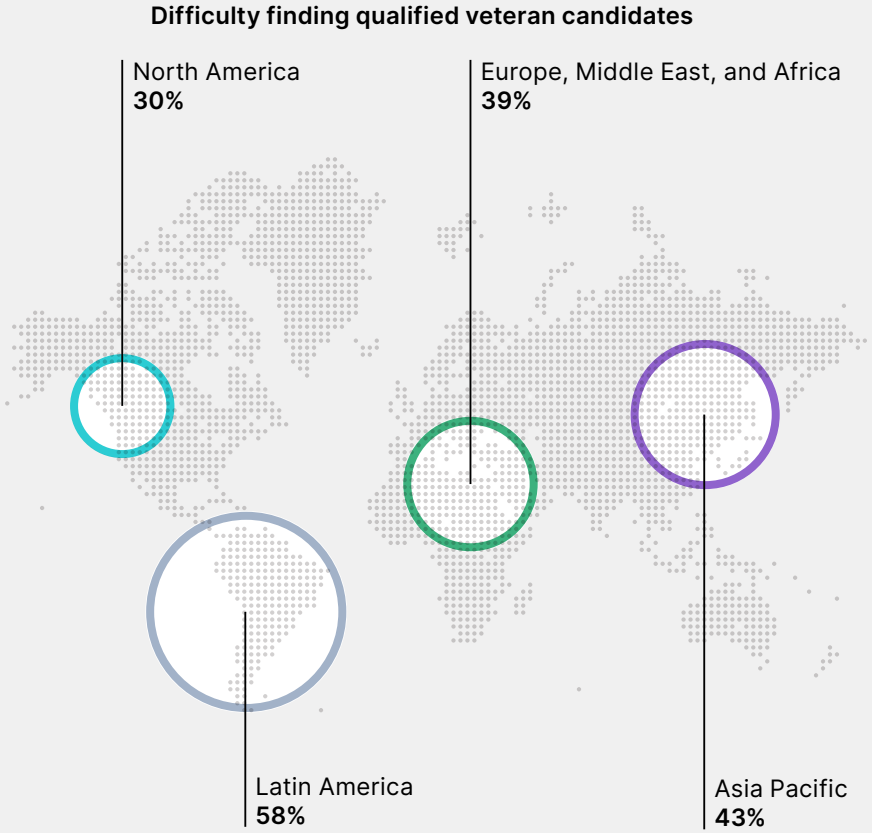
Asia Pacific organizations are most likely to have formal diversity targets



Qualified women candidates are easiest to find in North America



Qualified veteran candidates are hardest to find in Latin America

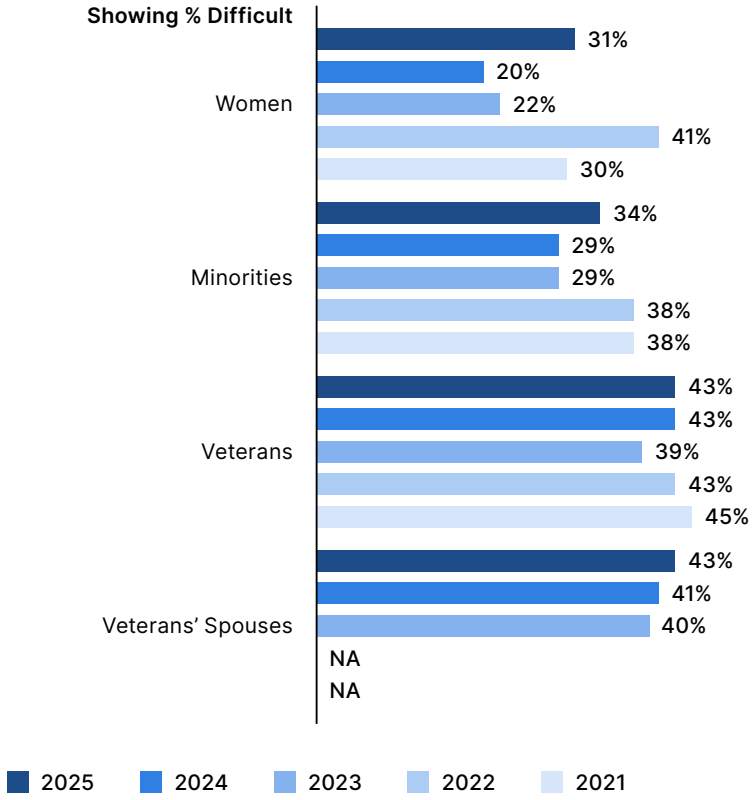


Big Movers

YoY Highlights

After a few years of improvement, organizations are suddenly saying it's hard to find qualified individuals in certain target talent pools again. The causes of these jumps, which are sizable in the case of women and minorities, are unclear, and trends in these areas are worth watching for going forward.

QUALIFIED INDIVIDUALS HARDEST TO FIND



Taking Action

The cybersecurity skills shortage continues to challenge organizations worldwide, and the rapid emergence of new technologies, particularly AI, is further increasing demand for specialized skills. As a result, organizations may need to rethink traditional approaches to recruiting and talent development.

Look beyond the standard requirements

One effective strategy is to broaden recruiting efforts beyond traditional talent pools. Many organizations historically relied on candidates with conventional educational backgrounds or specific technical credentials. While those qualifications remain valuable, expanding recruiting criteria can help organizations identify capable candidates who may have developed relevant skills through alternative pathways such as vocational training programs, military service, community colleges, career transitions, or self-directed learning.

Target new groups with the right mindset and ability to learn

Structured recruiting initiatives aimed at underutilized talent pools can also play an important role. The fact that 71% of organizations report formal hiring targets for these groups suggests that many organizations recognize the opportunity to expand the cybersecurity workforce by engaging candidates who have historically been underrepresented in the field.

Invest in training strategies

However, recruiting from broader talent pools is only the first step. Organizations must also ensure that onboarding, training, and career development programs are designed to help these new employees succeed. Mentorship programs, structured learning pathways, and certification opportunities can help individuals build the specialized technical skills required for cybersecurity roles while strengthening long-term retention.

Finally, organizations should view workforce diversity not simply as a recruiting initiative but as a strategic advantage. Teams composed of individuals with different experiences, backgrounds, and perspectives often bring stronger problem-solving capabilities and more creative approaches to identifying and mitigating security risks.

By combining expanded recruiting strategies with robust training and development programs, organizations can strengthen their cybersecurity workforce while making meaningful progress toward closing the global skills gap.

59% of organizations are developing internal training or reskilling programs to support AI adoption.

Conclusion

Coming out of 2025, organizations continue to struggle with the persistent skills shortage of the last several years, while facing the added challenge of expanding and staffing AI-related roles when relevant experience is hard to find.

That being so, AI is prominently seen as a partial solution to the skills gap at entry-level positions, whether by autonomously or semi-autonomously taking on core security functions or by augmenting training and filling in team capabilities.

At the same time, AI is clearly regarded as an indispensable tool for addressing increasingly sophisticated and destructive threats—though its implementation raises other cybersecurity concerns, such as the risk of unintentional data leakage.

All of this points to a situation of growing complexity, which may be why organizations say their greatest need is for senior-level cybersecurity talent. At the same time, the nature of entry-level positions is likely to change, with growing requirements for new hires to have AI skills and knowledge.

As noted in the introduction to this year's report, the urgency and strategic complexity of these issues demand clear, confident, and knowledgeable direction-setting by corporate leadership, including at the board level. Boards seem to understand this, increasing focus on cybersecurity and making it a business priority. But, given the relatively low perceptions of board awareness of the risks associated with AI and the skills shortage, more still needs to be done.

To face the challenges of today and prepare for those that are sure to come, board oversight needs to focus on preparedness, recovery, and leadership effectiveness—in other words, on building up, maintaining, and evolving organizational cyber resiliency for the long term.

About Fortinet

Founded in the San Francisco Bay Area in 2000, Fortinet continues to be a driving force in the evolution of cybersecurity and the convergence of networking and security. Securing people, devices, and data everywhere is our mission. To that end, our portfolio of over 50 enterprise-grade products is the largest integrated offering available, delivering proven cybersecurity everywhere you need it. More than 900,000 customers trust Fortinet solutions, which are among the most deployed, most patented, and most validated in the industry.

The Fortinet Training Institute provides one of the largest and broadest training programs in the industry to make cyber training and new career opportunities available to everyone.

Learn more by reading the Fortinet Blog or visiting FortiGuard Labs.

FORTINET
Training Institute

www.fortinet.com

April 21, 2026 1:35 pm / MKTG-3152-0-0-EN