FORTINET
Training Institute

2025 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 1,850 IT and cybersecurity decision makers, conducted by Sapio Research in February 2025. Responses were obtained from 29 locations:

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

Overall results are accurate to ± 2.3% at a 95% confidence limit.

Due to rounding, percentages may not total 100%.

Size of Company

100-499 employees **25%**
500-999 employees **24%**
1,000-2,499 employees **22%**
2,500-4,999 employees **14%**
5,000+ employees **15%**

Role Type

12% of respondents held owner positions
34% of respondents held C-level executive positions
9% of respondents held vice president positions
11% of respondents held head positions
33% of respondents held director positions

Gender

69% of respondents were male
31% of respondents were female

Top Three Business Sectors:

Technology **22%**
Manufacturing **16%**
Financial Services **12%**

Total respondents: 1,850

Asia-Pacific **30%**
Europe, Middle East, and Africa **27%**
North America **22%**
Latin America **22%**

Executive Summary

A sharpened focus on risk management formed cybersecurity strategy in 2024, driven by a continuously evolving threat landscape, the need to safeguard business continuity, and the growing influence of AI on corporate decision making. Organizations are maintaining a multi-pronged approach to cybersecurity—combining security awareness, certifications, and the deployment of the right technologies. This commitment spans from the boardroom down, recognizing that all employees remain key targets for cyberattacks.

AI is seen as a threat, an opportunity, and a challenge

49% of respondents worry that AI use by bad actors will increase cybersecurity attacks.

97% are using or plan to use a cybersecurity solution that leverages AI.

Lack of staff with sufficient AI expertise (**48%**) is the biggest challenge foreseen by IT decision makers when it comes to implementing AI in cybersecurity.

Boards lack cyber knowledge—even though it's a priority

Only **49%** of leaders think their board members are fully aware of the potential risks posed by using AI.

52% say directors or executives have faced fines, jail time, loss of position, or loss of employment following a cyberattack.

76% say their board has put more focus on cybersecurity in 2024, up from 72% in 2023. To improve cybersecurity, boards have discussed or implemented:

- Mandatory training or certifications for IT and security staff (**62%**)
- Security awareness training for all staff (**55%**)
- Purchasing security solutions that use AI (**55%**)

Lack of cybersecurity awareness and training remains the top cause of breaches

IT leaders continue to say the top three causes of breaches are:

- Lack of security awareness (**56%**)
- Lack of IT security skills and training (**54%**)
- Lack of cybersecurity products (**50%**)

After an attack, most decision makers look to expand their IT/security teams (**63%**) or mandate certifications (**62%**)

Data, cloud, and network security are the cybersecurity skills organizations need most.

Organizations want cybersecurity personnel with certifications

89% prefer to hire candidates with certifications.

67% of respondents say it validates cybersecurity awareness and knowledge.

Only **73%** would pay for an employee to obtain a cybersecurity certification—down from 89% in 2023.

Potential talent pools are being overlooked

70% of IT decision makers have structured recruiting initiatives targeting women, and **57%** have them for minorities. Only **45%** have them for veterans; just **38%** have them for veterans' spouses.

65% of respondents consider professional certifications when hiring.

Just over half (**52%**) consider whether a candidate has a four-year degree.

INTRODUCTION

A Growing Need to Manage Risk

Organizations are operating in a new cybersecurity "normal" where breaches are inevitable, AI is a real and present danger, and knowledge gaps are a critical liability. It's no longer enough to try to simply mitigate risk: Organizations need to find ways to manage risk proactively on an ongoing basis.

The vast majority (86%) of this year's *Cybersecurity Skills Gap survey* respondents say they had one or more breaches in 2024, with nearly one-third (28%) reporting five or more. Those levels are in line with the last couple of years—and are up notably from our first survey in 2021 (at 80% and 19% respectively), suggesting a trend that is here to stay.

The impact of those security incidents is significant. More than half (52%) of organizations surveyed say breaches cost them more than $1 million. This is roughly in line with last year's 53% and up from 38% in 2021.

In response, organizations are turning increasingly to AI to strengthen their capabilities and posture, even as they acknowledge AI could also be used against them as an engine of new or improved cyberattacks. The majority (80%) say AI tools are helping their IT and security teams be more effective—though almost all are aware that AI won't solve the ongoing skills shortage alone.

That shortage amounts to a deficit of more than 4.7 million cybersecurity professionals, according to the 2024 ISC2 Cybersecurity Workforce Study. The lack of skilled personnel leaves organizations more vulnerable to attacks, and governments are taking note. Many countries have made cybersecurity a national priority and have launched initiatives to grow the cyber workforce and make it more resilient.

Closing the gap requires a coordinated strategy built on three pillars: increased awareness and education, targeted training and certification, and the implementation of advanced security technologies. Organizations need to rethink the qualifications they seek in candidates, pursue multiple pathways to expertise, and continue to tap into underutilized talent pools.

Organizations must also invest in cybersecurity training and development. The decline this year in willingness to pay for certifications—down to 73% from 89% the previous year—is concerning in this regard. If this turns out to be an emerging trend, organizations should review this decision as part of their risk management strategy.

Skilled and aware employees and cybersecurity professionals are crucial to overall cyber risk management in a world that is moved beyond the attack-and-defend cycle. Today, to protect themselves, organizations need to maintain a posture of perpetual vigilance and continuous risk awareness.

49% of all respondents are concerned that AI will increase cyberattacks.

AI Is Seen as a Threat, an Opportunity, and a Challenge

While organizations have concerns about AI-related risks, they also see AI as a potentially powerful tool for shoring up defenses—though it is a tool that must be managed by skilled professionals. The vast majority (97%) of this year's respondents are either already using or planning to implement AI-enabled cybersecurity solutions.

The primary concern surrounding AI is its potential to drive an increase in cyberattacks (49%). This reflects growing unease about how AI can be leveraged by threat actors to develop more sophisticated, automated, and targeted attacks. Following that, a cluster of concerns emerges with similar levels of urgency: 39% worry about the spread of misinformation, because generative AI makes it easier to produce convincing fake content that can cause confusion, panic, or poor decision-making; 38% cite surveillance and privacy violations; and 37% express fears about the development of superintelligent AI and the broader risk of losing control—an issue that, while more speculative, is gaining traction in public debate.

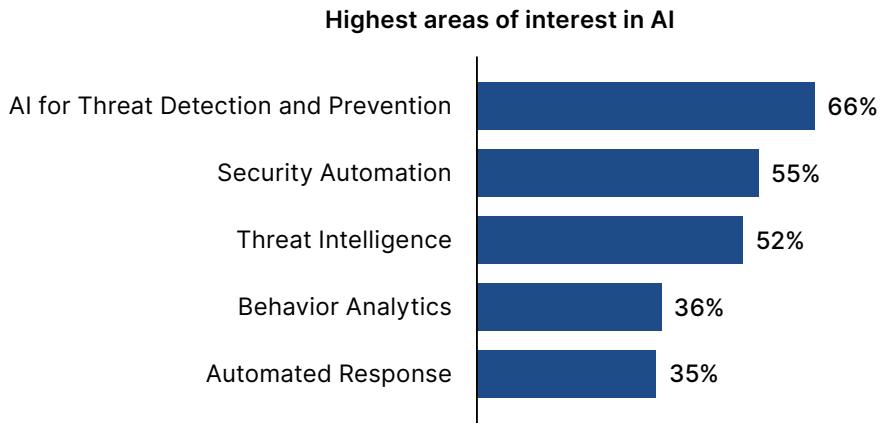
Concern about AI-enabled cyberattacks may be contributing to the adoption of AI-powered cybersecurity solutions—which 65% of respondents have already implemented, and another 32% plan to implement in the next year. Just 2% say they have no plans to implement such tools.

The more attacks an organization has incurred, the more likely it is to have AI-enabled cybersecurity solutions in place. Roughly three quarters (76%) of organizations that experienced nine or more cyberattacks in 2024 say they had AI cybersecurity tools deployed, suggesting that frequent attacks may be driving interest in more innovative solutions.

Asked what they foresee as the biggest challenge to integrating AI into cybersecurity, 48% of IT decision makers point to a lack of staff with sufficient AI expertise. The ability to ensure data privacy and information security was a close second at 47%—linking back to respondents' concerns about misinformation, surveillance, and privacy violations.

Top AI Areas of Interest in Cybersecurity Among Organizations

Threat detection and prevention emerged as the top areas of interest for applying AI in cybersecurity, followed closely by security automation and threat intelligence, according to respondents.



97% of organizations are using or plan to use a cybersecurity solution that leverages AI.

DIGGING DEEPER

AI Impacts and Challenges

Security Jobs Aren't Threatened by AI

Few leaders think AI will displace cybersecurity professionals:

- 87% expect AI to enhance some or major aspects of their roles.
- 9% say they believe AI will replace significant parts of their roles.
- Only 2% think AI will replace their roles entirely.

Knowledge Gaps Can Challenge AI Adoption

Beyond a lack of AI expertise, respondents anticipated other obstacles to the uptake of AI cybersecurity tools:

- 44% say difficulty understanding or managing potential AI risks could be an adoption challenge.
- 43% say uncertainty or skepticism about the overall role of AI in cybersecurity may also be a barrier.

Preferences Vary Over How to Learn AI Tools

Respondents cited a range of preferred methods for learning about AI tools:

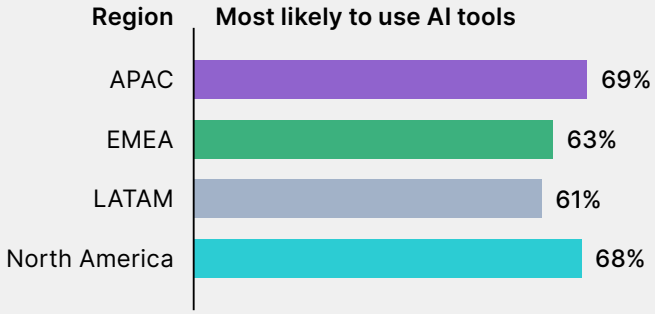
- Vendor training (55%)
- Vendor-agnostic training (49%)
- Hands-on learning on the job (48%)

55% prefer vendor training to learn about AI-enabled cybersecurity solutions.

Regional Highlights

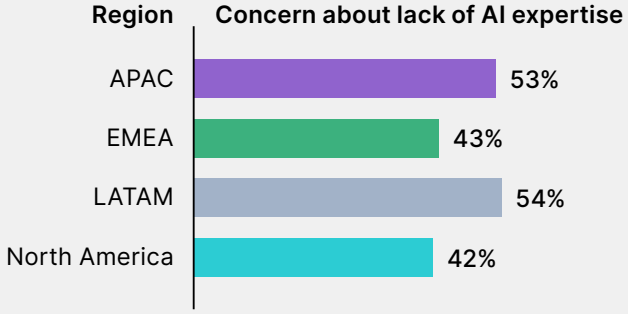
AI cybersecurity tools are most common in APAC and North America

Organizations in Asia Pacific (APAC) and North America are slightly more likely to use AI cybersecurity tools.



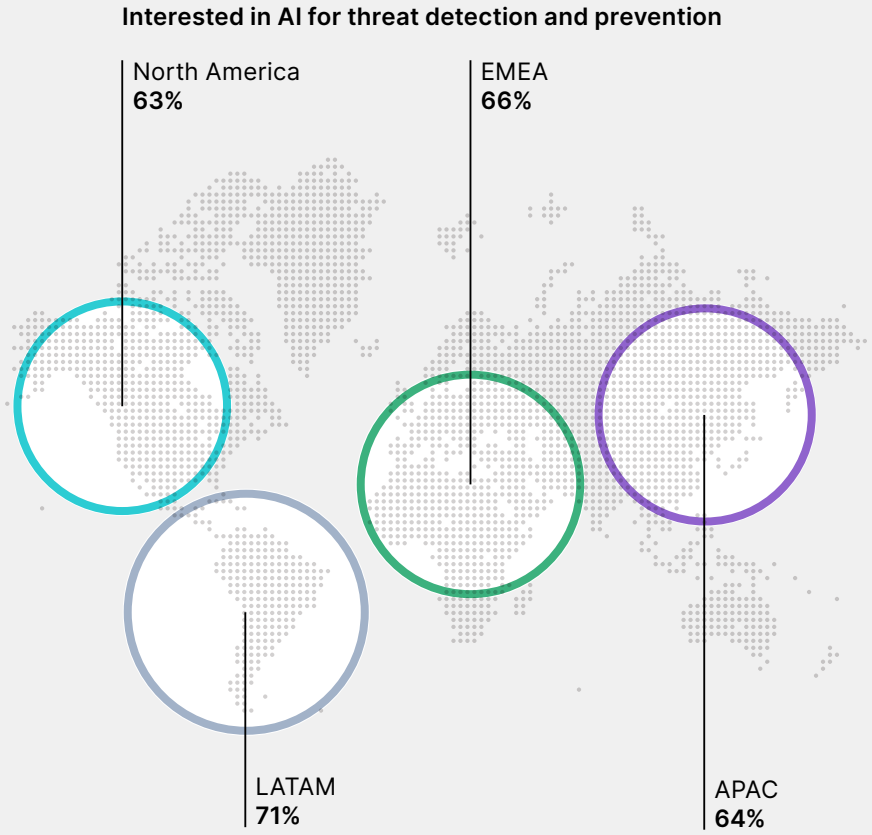
Concerns about AI expertise are higher in some regions

Lack of AI expertise is of greatest concern in Latin America (LATAM) and APAC.



Some regions are more interested in using AI for cybersecurity

Interest of AI for threat detection and prevention is an especially high priority in LATAM.



Taking Action

Strengthen security awareness and training

This year's AI findings correspond with our 2024 Security Awareness and Training Global Research Report, which showed that 62% of leaders were worried that employees would fall for more attacks because of AI. Considering the present findings about AI skills deficits and risks related to misinformation, data privacy, and information security, it seems that organizations believe their people may not be fully prepared to meet the AI moment.

Understand what AI can do for you

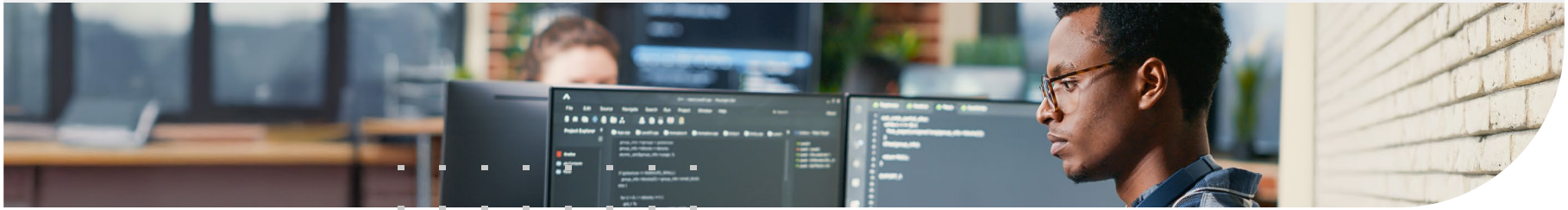
Organizations also need to understand where AI can excel—in essence, serving as a kind of junior analyst to sort quickly through logs to pinpoint the root causes of threats and highlight key insights. This enables skilled personnel, like senior engineers, to focus on critical and timely analysis, make decisions, and oversee responses. Raising awareness and providing training can help address this.

Ask the right questions about AI

Instead of asking if vendors "have AI," organizations need to start asking how they could use AI to support their specific security goals, such as analyzing logs (security information and event management (SIEM)) or autonomously responding to threats (endpoint detection and response (EDR), extended detection and response (XDR), and security orchestration, automation, and response (SOAR)).

Consider SOC-as-a-Service

Since few organizations have the specialized staff needed to run these systems independently, a security operations center (SOC)-as-a-Service (SOCaaS) is also an option. It allows an organization to benefit from AI security and expert guidance, like faster threat response, without the burden of managing the technology in-house.



Fewer than half (**49%**) of all leaders think their board of directors is fully aware of potential risks posed to the organization by using AI.

Boards Lack Cyber Knowledge—Even Though It's a Priority

Even as corporate directors and executives continue to be held accountable for cybersecurity breaches, many board members are seen to be less than fully aware of the potential risks that AI use poses to their organizations.

Fewer than half (49%) of all respondents say they feel their board members are fully aware of AI risks. Somewhat fewer (42%) say board members are moderately aware; 7% say they are slightly aware. Of those with perceived higher AI awareness, 61% oversee organizations that currently use AI cybersecurity tools. Of those with perceived moderate awareness, 36% currently use AI cyber tools. Only 3% of slightly aware board members are using AI solutions.

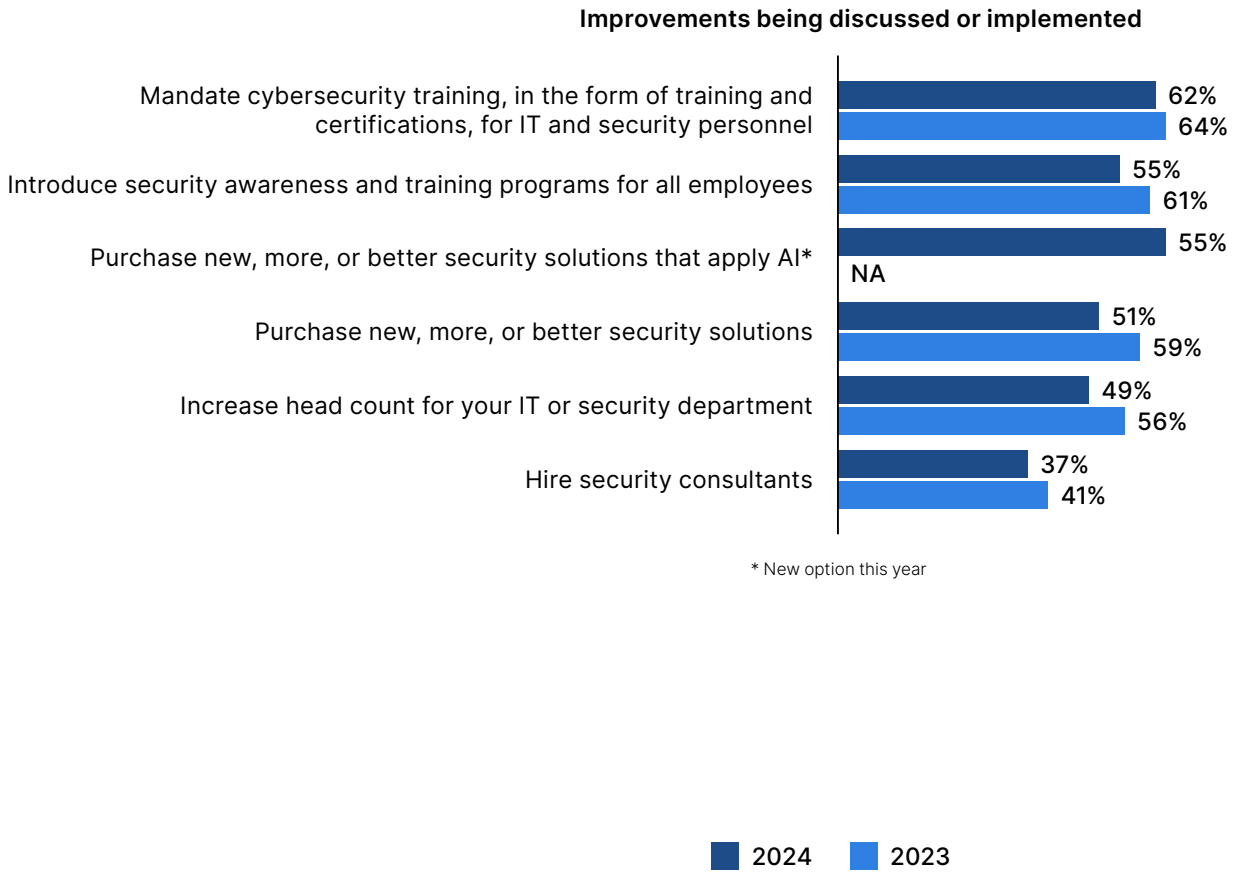
Boards may be playing catch-up on AI, but in general, most are paying greater attention to cybersecurity: More than three-quarters (76%) of respondents say their board put more focus on cybersecurity in 2024, up from 72% in 2023. The vast majority of respondents say cybersecurity is a business (96%) and financial (95%) priority for their organization to some or a great extent.

The increasing board focus on cybersecurity may be partly attributable to the fact that 52% of organizations surveyed say directors or executives have faced fines (33%), jail time (15%), or loss of employment or position (33%) following a cyberattack—on par with the previous year. That 52% jumps to 76% for organizations that experienced five to eight cyberattacks in 2024.

To improve cybersecurity, leaders say their boards have discussed or implemented measures such as: mandatory training or certifications for IT and security staff (62%); security awareness training for all staff (55%—down from 61% in 2023); and purchasing security solutions that use AI (55%).

Top Board-Driven Actions on Cybersecurity

Once again this year, among respondents aware of their boards' focus, a clear majority said mandatory cybersecurity training and certifications for IT and security staff were the top actions discussed or implemented. New and notable is that more than half (55%) say their boards have also discussed or implemented solutions that apply AI.



* New option this year

DIGGING DEEPER

Breaches Still Matter—and Boards Know It

Breaches Remain High and Costly

Most organizations were breached in 2024, and more than half paid a hefty price for it:

- 86% had one or more breaches; 28% had five or more.
- 52% say those breaches cost them more than $1 million.
- Malware, phishing, and web attacks account for 78% of attacks, in line with the previous year (80%).

Recovery Time Continues to Impact Organizations

Recovery times have improved slightly in the wake of cyberattacks:

- 59% of organizations took one month or more to recover from a cyberattack.
- Governments at all levels (federal, state, local) are quickest to recover, with 58% reporting it took less than one month.
- The mean time to recover across all respondents is 2.5 months, a very slight reduction from 2.7 in 2023.

Cybersecurity Has Board Attention

While there is still room for more, boards are paying closer attention to cyber risks:

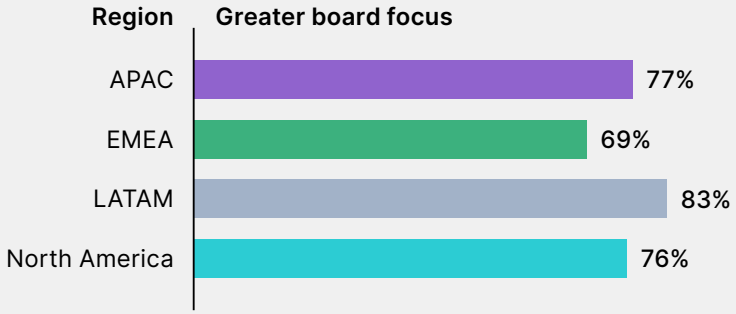
- Only 2% of respondents report less board focus on cybersecurity in 2024.
- Boards of larger organizations focus more on cybersecurity than those of smaller organizations (83% for 5,000+ employees versus 72% for 100–499 employees).
- 96% of boards see cybersecurity as a business priority, and 95% see it as a financial priority.

Only **2%** of respondents reported less board focus on cybersecurity in 2024.

Regional Highlights

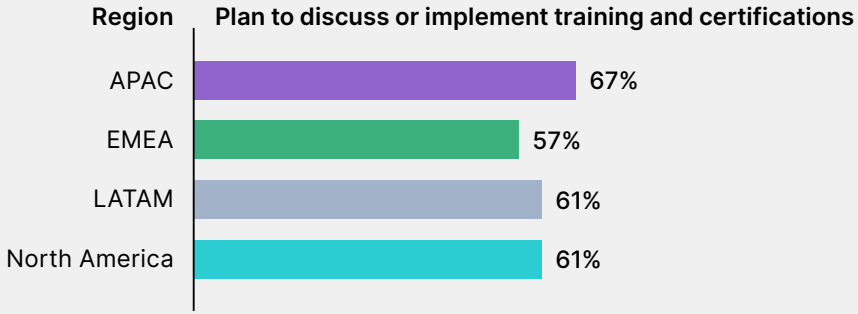
Board attention on cybersecurity rose most in LATAM

Respondents in LATAM were most likely to report a greater board focus on cybersecurity in 2024.



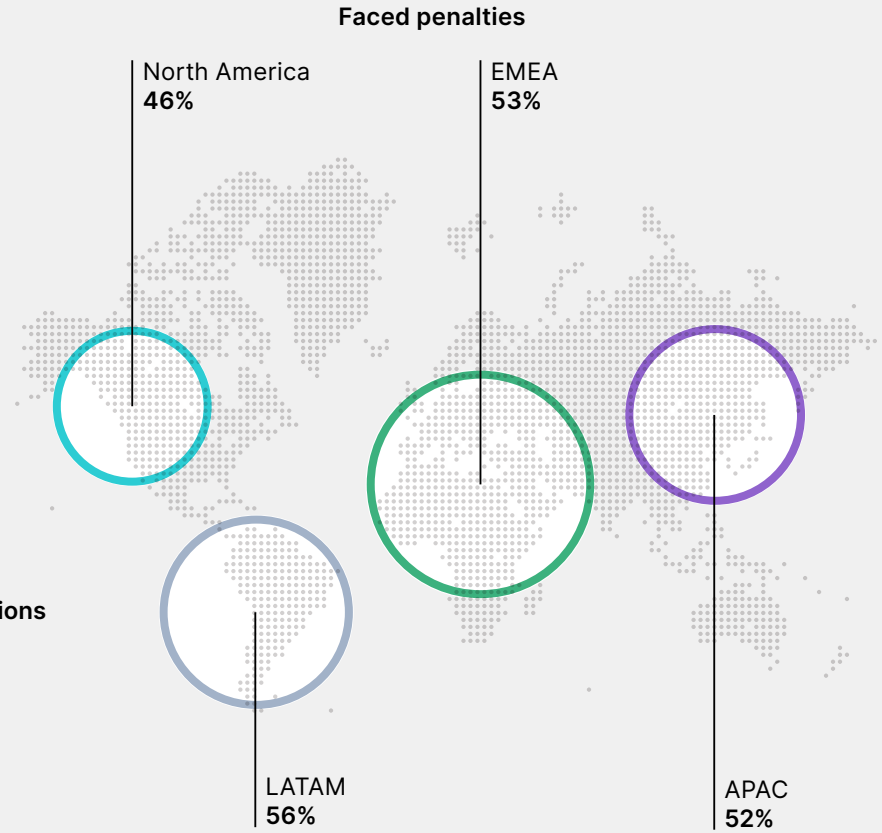
Boards in all regions favor cybersecurity training and certifications

Boards discussed or implemented cybersecurity training and certifications for IT and security staff in all regions, most prominently APAC.



More directors and executives faced penalties in LATAM

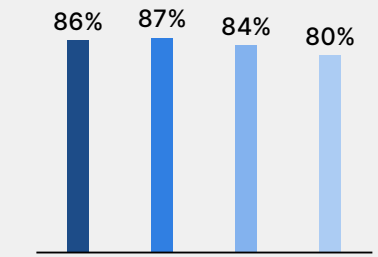
LATAM reported the most board members and executives to be fined, jailed, or lost their position or job because of cyberattacks.



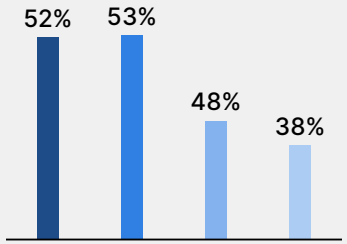
YEAR-OVER-YEAR PERSPECTIVE

Cybersecurity and Corporate Governance

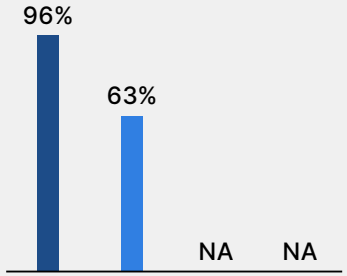
THE IMPACT OF BREACHES



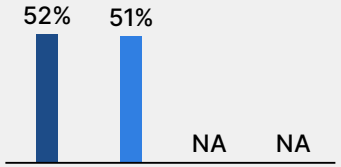
Experienced one or more breaches over the previous 12 months



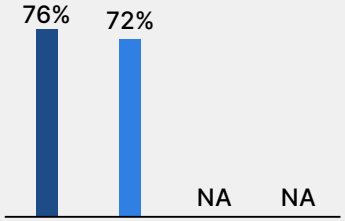
Breaches cost more than $1 million USD



Took more than one month to recover from a cyberattack



Directors or executives penalized with fines, jail time, or loss of employment or position following a breach



Greater board focus on cybersecurity

2024 2023 2022 2021

Taking Action

Educate your board on cybersecurity and AI

Apart from continuing to be a growing priority, not much seems to have changed for boards between 2023 and 2024 with respect to cybersecurity. Given the high stakes associated with breaches and the fact that directors and executives are still held personally liable for security breaches, this lack of change is a sign that more needs to be done--especially considering that boards currently possess a lower awareness of AI risks while AI use continues to grow and AI-driven attacks are expected to increase.

Boards play a key role in setting direction on cyber risk management and resilience. Organizations need to recruit knowledgeable and aware board members, and ensure that boards establish and strengthen committees focused on cybersecurity.

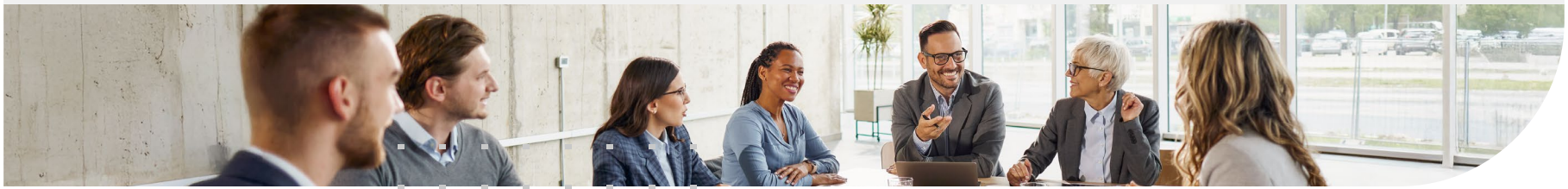
As part of a multi-pronged cybersecurity approach, boards may need to undergo cyber education and be brought up to speed on the risks, challenges, and opportunities presented by AI. Cybersecurity is a fully shared responsibility and boards must do their part.

Develop a cybersecurity risk management plan

Proactive board members could begin their AI awareness process by inquiring about their organization's cyber risk management readiness. One useful question might focus on the organization's mean time to respond (MTTR) to attacks, since slow detection often leads to slow recovery.

Ensure you have the right cyber solutions in place

To shrink a high MTTR, organizations could look for tools that find threats early and enable a quick response. One example is a security orchestration, automation and response (SOAR) platform, which addresses incidents the moment they occur. Others include endpoint detection and response (EDR), network detection and response (NDR) and extended detection response (XDR), which all work together to provide the unified view needed for a rapid response.



56% of IT decision makers say a lack of cybersecurity awareness is the top cause of breaches.

Lack of Cybersecurity Awareness and Training Remains the Top Cause of Breaches

IT leaders attribute cybersecurity breaches to three interrelated factors: lack of employee security awareness (56%), lack of cybersecurity skills and trained IT or security staff (54%), and lack of necessary cybersecurity products (50%).

These figures are similar to last year, with lack of awareness moving into the top position and slight drops related to skills and training and cybersecurity products (both down four percentage points from 2023, where they were at 58% and 54% respectively).

Most respondents (67%) said the cybersecurity skills shortage creates additional risks for their organizations, roughly the same as in 2023 (70%). Data, cloud, and network security are the cybersecurity skills organizations need most.

Largely aligning with the top causes of breaches, IT leaders say their main responses to a cyberattack would be to:

- Expand their internal IT or security team (63%)
- Mandate cybersecurity training in the form of certifications for IT and security personnel (62%)
- Introduce employee awareness and training programs (59%)
- Purchase new security solutions (56%)

Cyberattacks Continue to Target End Users

With malware, phishing, and web attacks once again 'topping the charts' of attack types at 78% (in line with 80% in 2023), bad actors clearly see users as the weak link in organizations' security postures—reinforcing IT leaders' impressions of what causes breaches.

Top 20 attack types

	2024	2023	2022
1. Malware attacks	40%	44%	45%
2. Phishing attacks	32%	36%	36%
3. Web attacks	30%	31%	36%
4. Password attacks	27%	30%	35%
5. Trojan horses	24%	29%	31%
6. Ransomware	24%	26%	28%
7. DoS and DDoS attacks	23%	26%	27%
8. DNS spoofing	19%	20%	22%
9. URL Interpretation	18%	17%	18%
10. Spear-phishing attacks	17%	19%	18%

	2024	2023	2022
11. External USB or physical media	17%	16%	NA
12. SQL injection attacks	16%	16%	16%
13. Whale-phishing attacks	16%	14%	16%
14. Insider threats	14%	14%	18%
15. Drive-by attacks	14%	14%	14%
16. Session hijacking	14%	13%	12%
17. Brute force attacks	13%	15%	15%
18. Coercion, blackmail, or bribery of internal staff	12%	12%	NA
19. Eavesdropping attacks	12%	11%	13%
20. XSS Attacks	12%	11%	12%

DIGGING DEEPER

The Skills Shortage Remains a Liability

Organizations Have Challenges Hiring

While recruitment and hiring remain a challenge, this is less acute than in previous years:

- More than half (52%) of respondents say they struggle to recruit and hire cybersecurity talent—down from 60% in 2021.
- AI is providing some relief, with 80% of respondents saying AI security tools are helping IT and security teams be more effective and efficient.

Key Skills and Types of Experience Remain Elusive

Certain candidates continue to be more difficult to find:

- Candidates with network engineering and security experience are hard to find (58%, down from 62% in 2023).
- Candidates with specific cybersecurity AI experience are a close second (57%).
- AI/machine learning and cloud security are the hardest roles to fill (30%).

Hiring Continues to be Highly Competitive

Organizations struggle to retain cybersecurity staff for a few key reasons:

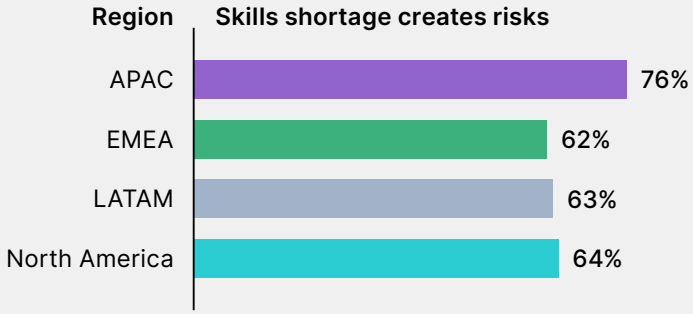
- Some organizations say they lack training and upskilling opportunities (48%).
- Others say they are "outbid" on salary and benefits (42%).
- Very few (13%) organizations say they don't have any challenges around retaining employees.

Roughly a third of respondents say AI/machine learning and cloud security are the hardest roles to fill.

Regional Highlights

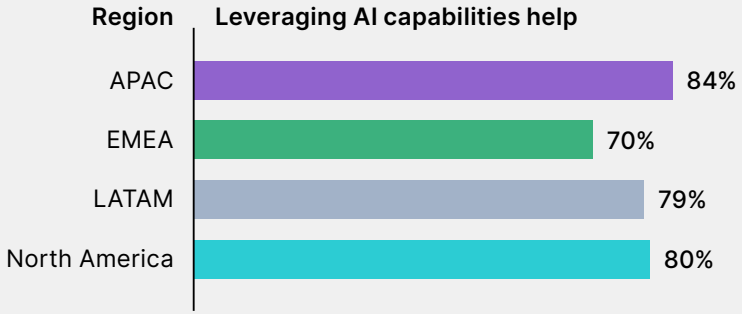
The skills shortage has the biggest impact in APAC

APAC organizations are most likely to agree that the cyber skills shortage creates additional risks for them.



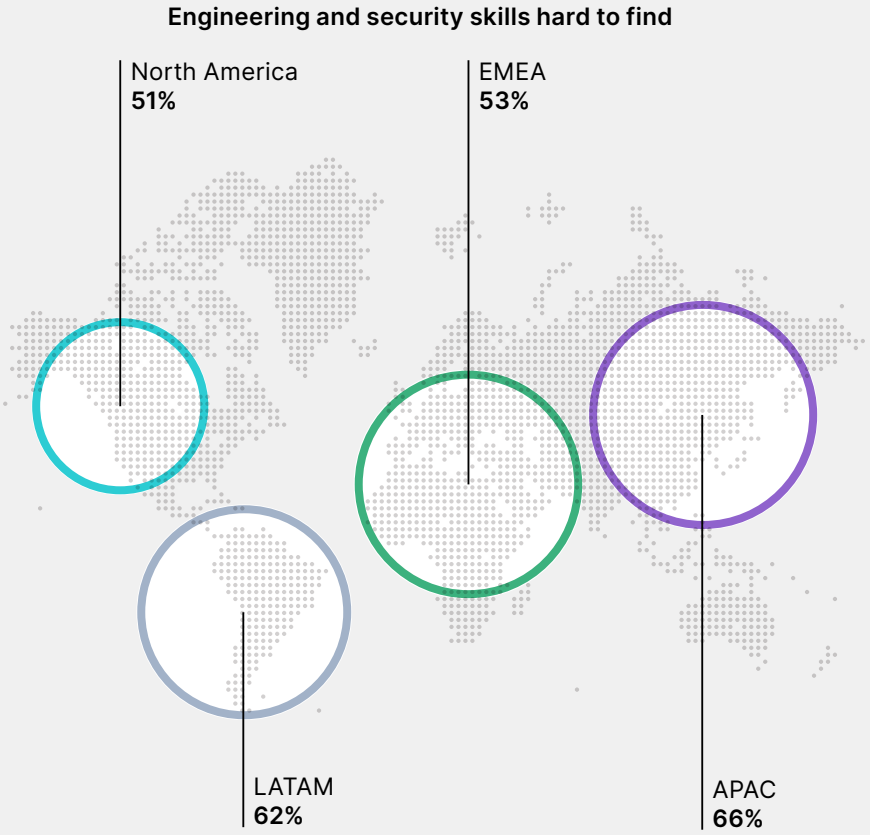
All regions say solutions leveraging AI capabilities are helping

APAC organizations most strongly agree that AI cybersecurity tools boost effectiveness and efficiency.



Network engineering and security experience is scarcest in APAC

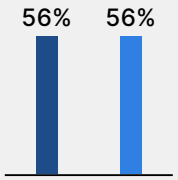
APAC organizations have the most difficulty finding candidates with specific experience in network engineering and security.



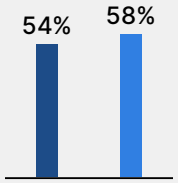
YEAR-OVER-YEAR PERSPECTIVE

Causes and Responses to Cyberattacks

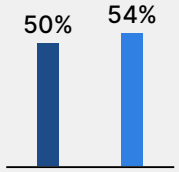
TOP CAUSES OF BREACHES



Lack of employee security awareness

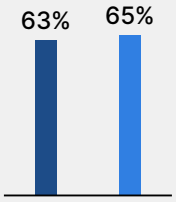


Lack of cybersecurity skills and trained IT or cybersecurity staff

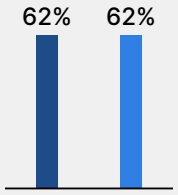


Lack of needed cybersecurity products

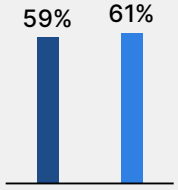
TOP RESPONSES TO CYBERATTACKS



Expand IT or security team



Mandate cybersecurity certifications for IT and security personnel



Introduce security awareness and training programs for all employees

2024 2023

Taking Action

Manage cyber risk proactively

While some types of cyberattacks are more common than others (see page 21), organizations cannot predict which specific attacks they are likely to experience.

Organizations need to treat cybersecurity as a strategic, corporate-wide initiative that includes managing risk proactively rather than taking a purely reactive defense-and-response approach.

Hire based on cyber skills and knowledge

As part of this plan, security leaders should ensure clear communication between hiring managers and HR to ensure that the best individuals are hired to fill vacant or new positions, focusing on fit within the organization and acquired cyber skills and knowledge. When assessing the team, training and certification can help new and existing employees upskill or reskill in growing areas of concern.

Seek industry-recognized training and certification

Security leaders should seek out cybersecurity providers with industry-recognized certification programs and a strong focus on role-based training. The most valuable certifications align with key areas of cybersecurity, and support ongoing skill development across all experience levels.

Keep training and awareness programs up to date

The strategy should also include implementing and continually revising security awareness programs for all employees, and assessing network architecture and vulnerabilities on an ongoing basis to align with the plan and people required to execute the plan.

If organizations want to provide an extra layer of protection against the human errors that their employees might unintentionally make, leveraging AI-powered security tools that can help protect email, browsers, and collaboration tools can significantly reduce the most vulnerable attack surfaces. By automatically neutralizing threats within the applications that employees use daily, security teams can shrink their response times and prevent minor human errors from escalating into major security incidents.

89% of IT decision makers prefer to hire candidates with certifications.

Organizations Want Cybersecurity Personnel with Certifications

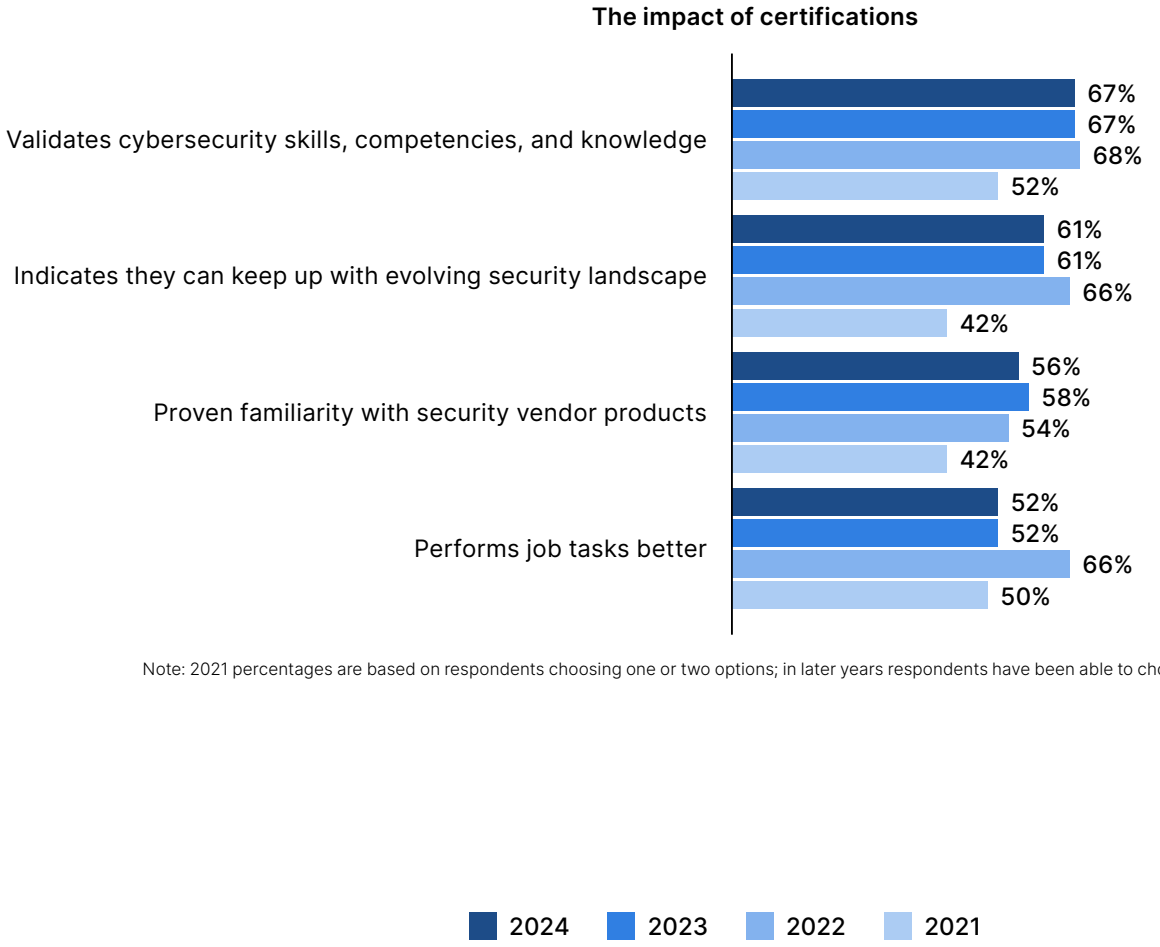
In 2021, the first year of the *Cybersecurity Skills Gap* survey, 81% of respondents said they preferred to hire cybersecurity personnel with certifications. A year later, that figure jumped to 90%—and it has remained essentially the same since.

In 2024, 89% of IT decision makers expressed a preference for certified candidates. A good majority (67%) said they looked for certifications when hiring a team member or direct report because it validates cybersecurity awareness and knowledge. Nearly the same number (61%) said they see certifications as a sign of being able to keep up with the evolving security landscape. More than half (56%) said certifications indicate familiarity with security vendor products.

Despite the advantages and the clear preference for certifications, the percentage of organizations willing to pay for employees to obtain certifications fell sharply in this most recent survey—down to 73% from 89% in 2023. A full quarter (25%) say they would not pay for a certification, up from just 7% in 2023. While it's unclear what has motivated this shift, it seems out of step with the recognition that training and certifications make a difference.

Knowledge and Performance Drive the Preference for Certifications

Looking at the past four years of survey findings, respondents most strongly and consistently prefer certified candidates for the skills, knowledge, and competencies they bring.



Note: 2021 percentages are based on respondents choosing one or two options; in later years respondents have been able to choose more than two.

DIGGING DEEPER

Certifications Have Real Impact

The Prevalence of Certifications is Still High

Most respondents have people on their teams with technology-focused certifications or have certifications themselves:

- 86% have someone on their team with a technology-focused certification.
- 81% have technology-focused certifications themselves (though this is down from 84% in 2023 and continuing a decline from 86% in 2021).

Certifications Bring Observable Benefits

Respondents continue to indicate a range of advantages from certifications for themselves and for others:

- 61% report increased cybersecurity skills and knowledge.
- 55% cite the ability to better perform job tasks.
- 50% note faster career progression or promotion.

Bigger Companies Seem to Put More Value on Certifications

Larger organizations prefer and are slightly more willing to pay for certifications:

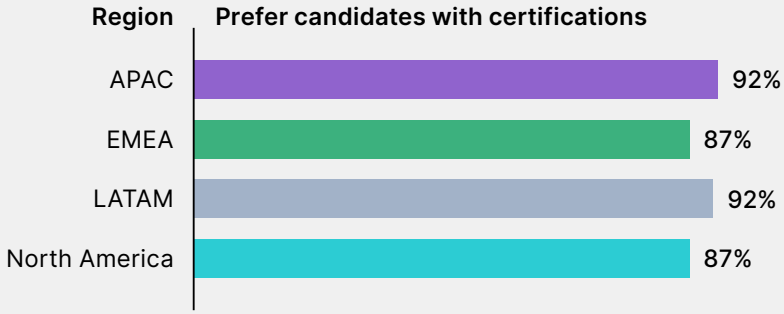
- 77% of organizations with 5,000 or more employees are willing to pay for certifications, versus 72% for smaller organizations.
- Roughly 69% of respondents from organizations with 1,000 or more employees look for certifications—compared to 64% in those with 500 to 999 employees.

86% of respondents say they have someone on their team with a technology-focused certification.

Regional Highlights

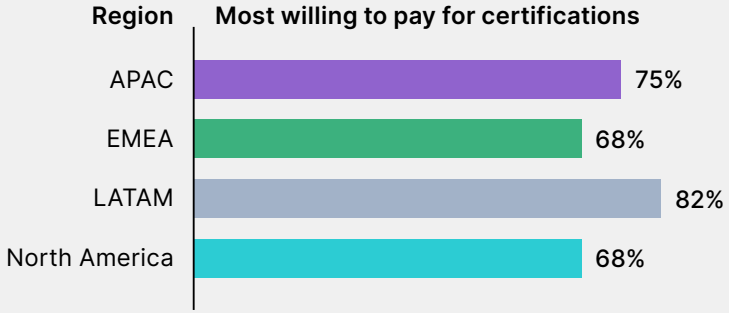
Organizations in all regions prefer candidates with certifications

The preference for technology-focused certifications is highest in APAC and LATAM.



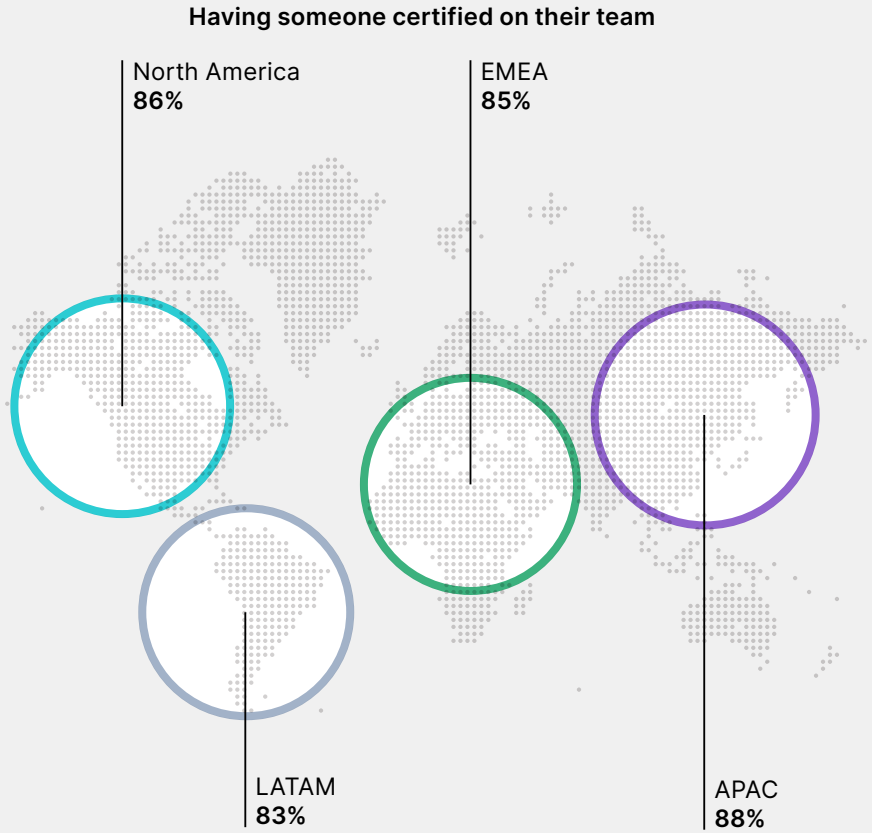
LATAM organizations are most willing to pay for an employee's certification

Willingness to pay for certifications is anywhere from 7–14 percentage points higher in LATAM than in other regions.



Certified team members are common in all regions

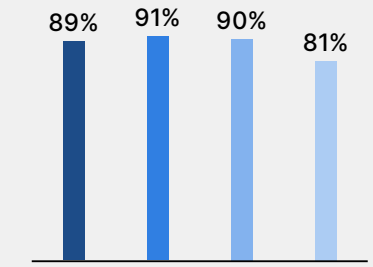
Respondents in APAC are most likely to have someone on their team with a certification.



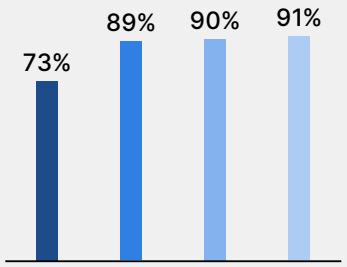
YEAR-OVER-YEAR PERSPECTIVE

Demand for Certifications

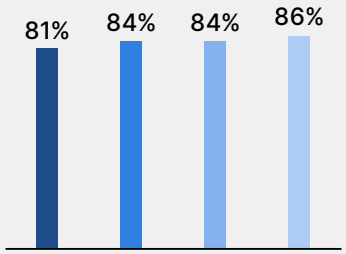
WHY CERTIFICATIONS ARE IMPORTANT



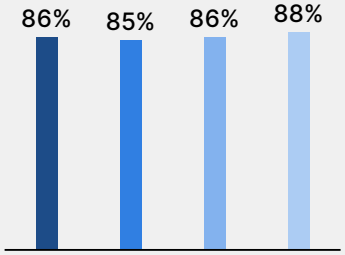
IT decision makers' preference to hire people with technology-focused certifications



IT decision makers' willingness to pay for an employee to get a cybersecurity certification



IT decision makers with certifications



IT decision makers with certified team members

2024 2023 2022 2021

Taking Action

Consider multiple pathways to expertise

Fortinet research shows that organizations need to embrace multiple "pathways to expertise" to overcome the skills gap and fill essential cybersecurity roles. Certifications are one such pathway, providing hands-on experience and industry-recognized credentials.

Most leaders realize this, with 61% citing better cybersecurity skills and knowledge as a top benefit of certifications. Leaders are also more likely to hire candidates who already have a certification.

Prioritize employee skills and knowledge

What is confusing this year is the drop in organizations willing to pay for certifications. More data is needed to understand what is behind this decline. In today's economic climate, one could argue that organizations are concerned about costs. If this is the case, it should be kept in mind that savings from AI and security automation can free up funds to invest in education of employees, providing them with the opportunity to acquire the skills, and knowledge needed to strengthen the security posture of the organization.

Leverage certification for retention

Retention of key employees also plays a part. Organizations need to invest in employees as part of their retention strategy. Nearly half of survey respondents say a lack of training and upskilling opportunities (48%) was their number one retention challenge. IT decision makers seem to recognize this, given their preference for candidates with certifications—which makes the decline in the number of organizations willing to pay for certifications all the more puzzling.

Veterans (**43%**) and veterans' spouses (**41%**) are the most challenging qualified individuals to find.

Potential Talent Pools Are Being Overlooked

While organizations have made some gains tapping into certain underutilized talent pools in the last four years, they still say the skills gap is compromising their cybersecurity. Part of the problem may be how they define "qualified candidates".

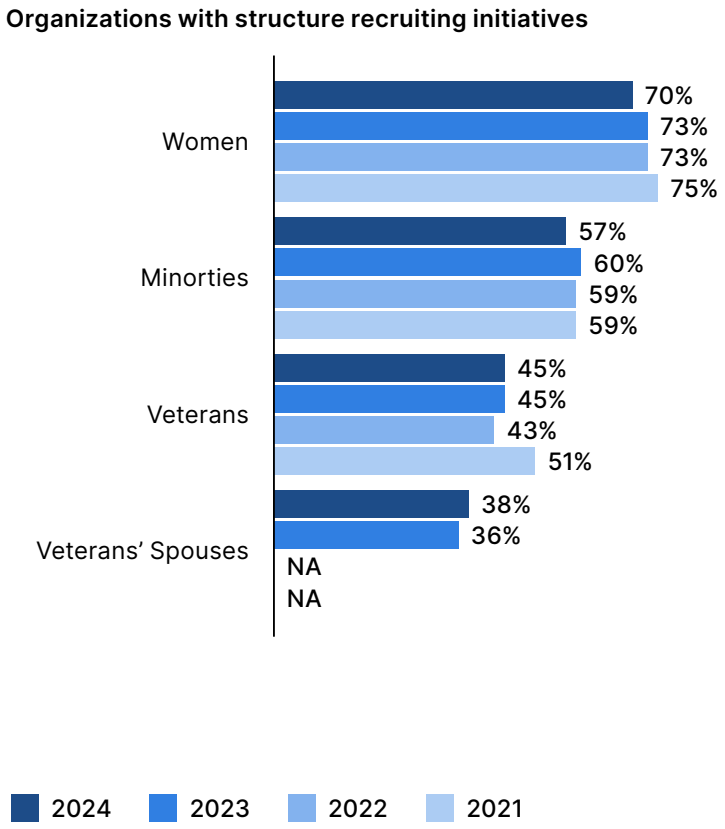
The percentage of organizations reporting difficulty finding qualified women and minority candidates has dropped substantially since our first *Cybersecurity Skills Gap* survey in 2021—down from 30% to 20% in 2024 for women and from 38% to 29% for minority candidates.

That said, those figures have essentially held steady over the last two years, and veterans and veterans' spouses remain considerably harder to recruit at 43% and 41%, respectively. While some of this difficulty may be a supply problem or related to challenges accessing specific talent pools, it may also be attributable to organizations ruling out potential candidates because of their qualifications.

More than half (52%) of organizations consider whether a candidate has a four-year degree when hiring, and a clear majority (65%) consider professional certifications. Allowing for other levels of education or credentials could open the way to more talent, if organizations were willing to invest in on-the-job development after hiring.

Structured Recruiting Initiatives for Key Talent Pools Seem to Be Slowly Declining

Since 2021, the percentage of respondents who say their organization has structured recruiting initiatives for women, minorities, veterans, and veterans' spouses has declined in all cases except veterans' spouses.



DIGGING DEEPER

Employment Levels Reflect Hiring Difficulty

Women Make Up the Biggest Proportion of Non-Traditional IT and Security Hires

Taken as a mean across all organizations surveyed:

- 27% of employees on IT and security teams are women.
- 20% come from minority backgrounds.
- 17% are veterans.
- 15% are veterans' spouses.

Some Organizations Do Consider Alternative Credentials

Respondents said they would consider factors outside of four-year degrees:

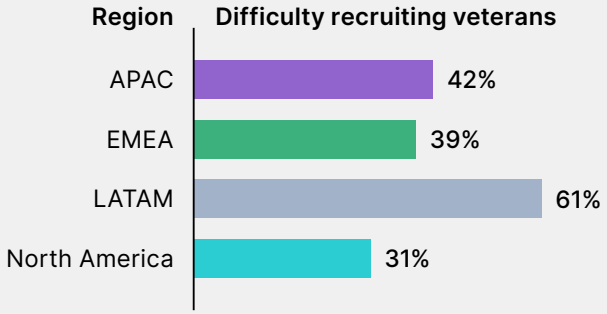
- 43% say they would consider whether a candidate has a diploma.
- 38% say they would consider whether or not a candidate has had vendor training.

Women account for an average of **27%** of the surveyed organizations' IT and security staff.

Regional Highlights

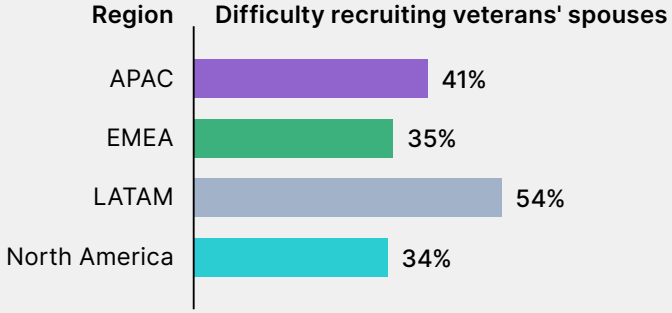
Veterans are harder to recruit in LATAM than in other regions

North America finds it less difficult to recruit veterans.



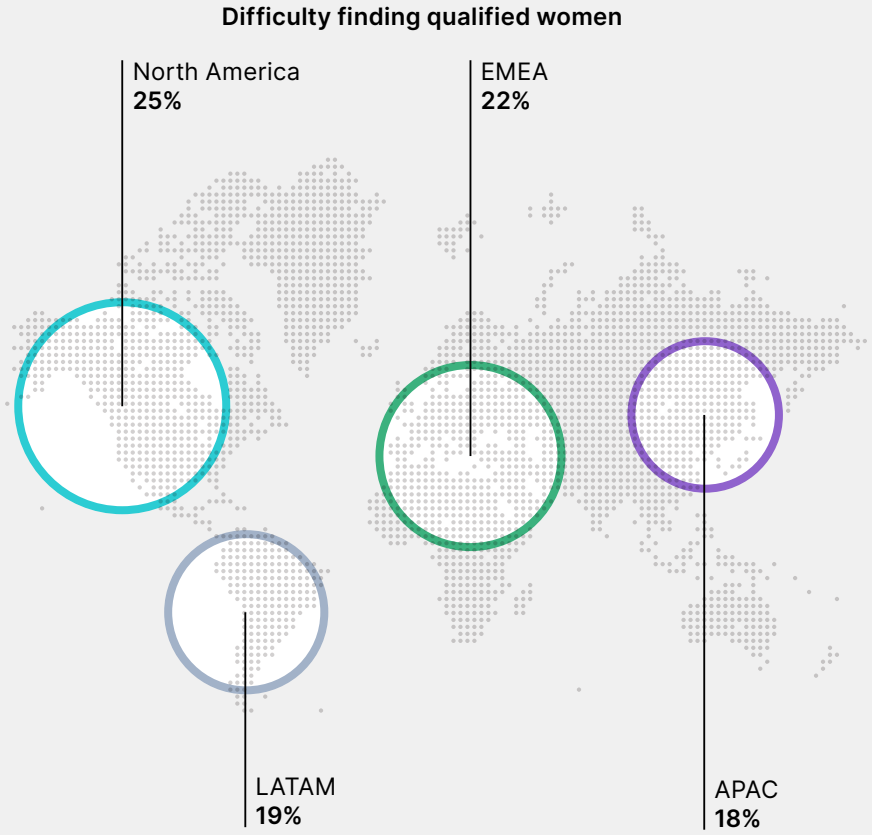
The same is true for veterans' spouses

Organizations in EMEA and North America have less difficulty recruiting veterans' spouses.



Qualified women candidates are hardest to find in North America

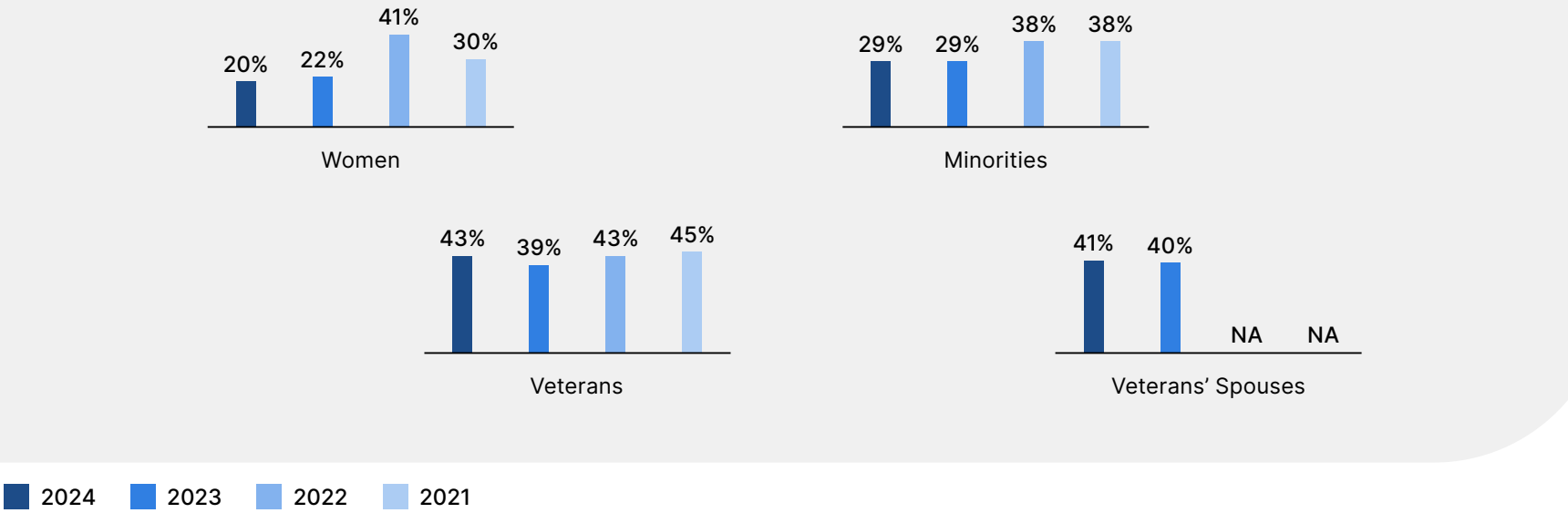
Slightly more organizations in North America and EMEA say it's difficult to find qualified women candidates.



YEAR-OVER-YEAR PERSPECTIVE

Recruitment from Untapped Talent Pools

HARDEST QUALIFIED CANDIDATES TO FIND



Taking Action

Account for both skills and knowledge

Trying to draw from smaller talent pools in a competitive labor market requires flexible and creative strategies. Over-reliance on traditional credentials such as four-year degrees could be limiting employers' access to the talent they need.

As noted in this report, recent Fortinet research shows organizations need to use multiple pathways to find and develop talent, including considering different mixes of credentials and hands-on skill development.

Work closely with HR on job requirements

Cybersecurity leaders should work with HR to ensure the posted qualifications for a position match the organization's skills and knowledge needs, that all potential talent pools are considered, and allow for various training options to fill the role.

Support public-private-partnerships (PPPs) that address the cyber skills gap

On a larger scale, building a talent pool for the global cybersecurity industry that includes all populations will require closer partnerships between industry, academia, and government. Already in the U.S. and other countries, a shift is underway toward two-year cybersecurity programs that are funded by governments to help address the skills gap.

Conclusion

Cybersecurity has become an increasingly strategic concern for organizations around the world, shaped by the rise of AI and the comprehensive array of risks that cyberthreats pose to a business. The need for a strategic approach is pushing cybersecurity past the C-suite all the way up to the board level.

As boards take on more responsibility for cybersecurity, corporate directors are under pressure to understand the issues so they can make informed risk-management decisions. In some cases—especially where AI is concerned—this may require cyber-risk education and training for board members.

AI simultaneously poses risks and has tremendous potential to enhance cybersecurity solutions. Outside of boards of directors, organizations need to ensure that all their people are "AI aware" and that cybersecurity teams have the skills to work with AI tools.

It's also important for teams to appreciate what AI can and can't do—where it can bring efficiencies and ease burdens, and where skilled human beings with expert judgment are still essential.

That need for skilled people means the ongoing global cybersecurity skills shortage remains a problem. Organizations can maximize their opportunities to fill crucial roles by shifting their expectations about the credentials that candidates need to bring—for example, insisting less on four-year degrees—and accessing underutilized pools of talent.

Closing the skills gap also requires investment in training and development. Rather than wait for a 'perfect' candidate, organizations may be better served by hiring people with high potential and good fit, and training them for a specific role. By putting money into training and development, this year's findings also suggest that organizations stand a better chance of retaining the talent they hire. On this point, it can't be stressed enough that the reluctance to pay for certifications that turned up in this year's results may seriously undermine organizations' cybersecurity objectives. Training and certifications remain fundamental to the three-pronged cybersecurity approach alongside general employee awareness and deployment of the right technologies.

Fortinet has embraced that three-pronged approach—awareness, training, and technology—for several years. With this year's survey, we're seeing that approach fit within the larger framework of holistic cyber risk management. As risk management matures, it will empower organizations to proactively protect themselves, their data, and their businesses, no matter how threats and technologies evolve.

About Fortinet

Fortinet (NASDAQ: FTNT) is a driving force in the evolution of cybersecurity and the convergence of networking and security. Our mission is to secure people, devices, and data everywhere, and today we deliver cybersecurity everywhere our customers need it with the largest integrated portfolio of over 50 enterprise-grade products.

Well over half a million customers trust Fortinet's solutions, which are among the most deployed, most patented, and most validated in the industry.

The Fortinet Training Institute, one of the largest and broadest training programs in the industry, is dedicated to making cybersecurity training and new career opportunities available to everyone. Collaboration with esteemed organizations from both the public and private sectors, including Computer Emergency Response Teams ("CERTS"), government entities, and academia, is a fundamental aspect of Fortinet's commitment to enhance cyber resilience globally.

FortiGuard Labs, Fortinet's elite threat intelligence and research organization, develops and utilizes leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence. Learn more at fortinet.com, the Fortinet Blog, and FortiGuard Labs.

FORTINET
Training Institute

www.fortinet.com

September 4, 2025 3:02 pm