FORTINET
Training Institute

2023 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 1,855 IT and cybersecurity decision-makers, conducted by Sapio Research in November 2022. Responses were obtained from 29 locations: Argentina, Australia, Brazil, Canada, Colombia, France, Germany, Hong Kong, India, Indonesia, Israel, Italy, Japan, Malaysia, Mexico, the Netherlands, New Zealand, People's Republic of China, the Philippines, Singapore, South Africa, South Korea, Spain, Sweden, Taiwan, Thailand, United Arab Emirates, United Kingdom, and the United States.

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

Size of Company

100-499 employees **22%**
500-999 employees **24%**
1,000-2,499 employees **23%**
2,500-4,999 employees **16%**
5,000+ employees **15%**

Gender

68% of respondents were male
32% of respondents were female

Total respondents: 1,855

APAC **30%**
EMEA **27%**
North America **22%**
LATAM **22%**

Role Type

13% of respondents held Owner positions
34% of respondents held C-level Executive positions
7% of respondents held Vice President positions
12% of respondents held Head positions
34% of respondents held Director positions

Business Sector

Company Sectors – Top 3

Technology **21%**
Manufacturing **16%**
Financial Services **13%**

Executive Summary

The findings in this 2023 cybersecurity skills gap report clearly show that organizations are fighting an uphill battle against cyberthreat—incurring more breaches, in need of skilled professionals, and continuing to struggle to fill key positions.

Breaches are more frequent and more costly

84% of organizations experienced **one or more breaches** in the past 12 months, up from 80% in 2021.

29% had **five or more intrusions** vs. 19% the previous year.

48% suffered breaches in the past 12 months that **cost more than $1 million** to remediate, up from 38% in 2021.

Unfilled IT positions are a cybersecurity risk

68% of organizations indicate they **face additional risks** because of cybersecurity skills shortages, consistent with 67% in 2021.

56% struggle to recruit and **54% struggle to retain** talent, compared to 60% and 52% in 2021.

Cloud security and security operations are the hardest roles to fill.

Boards of directors are focused on cybersecurity

93% of respondents indicate their **board asks about cybersecurity,** up from 88% in 2021.

In 2022, **83% of boards suggested increasing IT security headcount,** compared to 76% in 2021.

Certifications are sought as proof of cybersecurity knowledge and skills

90% of leaders **prefer to hire people with technology-focused certifications,** up from 81% in 2021. **90% would also pay** for an employee to get a cybersecurity certification.

72% of leaders indicate hiring certified people has **increased security awareness** and knowledge within their organization.

Diverse talent can help close the skills gap but isn't always easy to find

Approximately **40%** have **difficulty finding qualified candidates** who are women, military veterans, or from minority backgrounds.

83% of organizations have **near-term diversity hiring goals,** down from 89% in 2021.

The number of organizations confirming five or more breaches jumped by 53% between 2021 and 2022.

INTRODUCTION

Skilled People are Key to Cybersecurity

In 2022, cybersecurity challenges intensified globally in all sectors, from the exponential growth of new ransomware variants to increased attacks on operational technology (OT) and the rise of Malware-as-a-Service (MaaS). For many organizations, these developments make closing the cybersecurity skills gap within their own IT teams a higher priority than ever before.

While advanced cybersecurity solutions remain essential to meeting the demands of the fast-changing threat landscape, Fortinet's 2023 Cybersecurity Skills Gap Global Research Report finds leaders also looking at the human side of the equation, seeking to understand what skills they need and where to find them.

The focus on building cybersecurity capacity starts at the top, with more boards of directors asking questions about cyber defense and recommending increased IT security headcounts. This likely stems from a recognition of their responsibility for safeguarding the business and, by extension, customers, partners, employees, and the corporate brand.

As this 2023 report shows, organizations are seeking to recruit and retain talent to meet their cybersecurity needs, specifically people with technology-focused certifications as well as those from underrepresented groups, including women, people from minority populations, and military veterans.

What's new in 2023

This edition of the Cybersecurity Skills Gap Global Research Report features year-over-year comparisons and trend analysis based on feedback from security leaders around the world. While many results remained consistent between the last two years, some notable differences are identified throughout the report.

For more on employee cybersecurity awareness, read our companion report: **the 2023 Security Awareness and Training Global Research Brief**, which will publish this spring.

The number of organizations confirming **five or more breaches jumped by 53%** between 2021 and 2022.

Breaches are More Frequent and More Costly

As predicted by Fortinet's FortiGuard Labs, cyberthreats of all kinds became increasingly ubiquitous in 2022. This pervasiveness resulted in more breaches than during the previous year, and at a higher total cost of breaches for many organizations.

A high number of leaders also attribute those breaches, at least in part, to a lack of cybersecurity skills among IT professionals

The majority view seems to be that the threat landscape will only get worse. In the next 12 months, 65% of the survey respondents expect the number of cyberattacks to increase. This prediction aligns with FortiGuard Lab projections, which anticipate the growth of many attack types and cybercrime business models, including the Crime-as-a-Service (CaaS) market.

Despite the rise in breaches, 93% of leaders believe their organization is doing everything it can to deal with increasing attack volumes. This may suggest uncertainty about what additional measures organizations can take and sits somewhat at odds with other findings about increasing board concerns, such as the need for certifications to validate skills and knowledge and gaps in employee cybersecurity awareness.

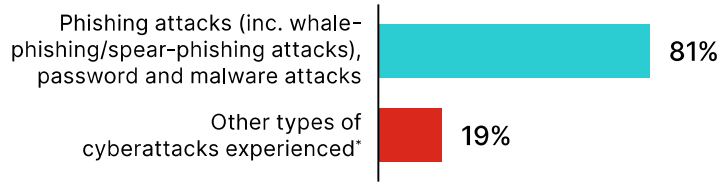
81% of cyberattacks were in the form of phishing, password, and malware attacks.

Phishing is the most common attack method

In 2022, respondents reported that phishing, malware, and password attacks together formed the bulk (81%) of attack types encountered by surveyed organizations in 2022. Notably, these three attacks can target not only systems but also individual users directly. Phishing schemes are especially insidious as they often deliver the other attack types: malware and social engineering that can lead to password and web attacks.

Organizations in North America saw significantly more phishing attacks than their counterparts in Latin America, while Latin America faced significantly more password attacks than peers in Europe, the Middle East, and Africa.

What types of cyberattacks did your organization experience?



*Refers to Web Attacks, Trojan Horse Attacks, Ransomware Attacks, DoS and DDoS Attacks, DNS Spoofing Attacks, Insider Threats, URL Interpretation, SQL Injection Attacks, Brute Force Attacks, Drive-by Attacks, Eavesdropping Attacks, Session Hijacking Attacks, Cross-site Scripting (XSS) Attacks, Man-in-the-Middle (MITM) Attacks, Birthday Attacks.

**Asked only to those whose organization had experienced a cyberattack in the past 12 months.

Digging Deeper

More organizations were breached last year than in 2021

84% of respondents indicate their organization experienced one or more breaches in the past 12 months, up from 80% the year before.

- 55% had one to four breaches.
- 29% had five or more breaches.
- 7% had nine or more, more than double the previous year (3%).

There was a notable increase in cost of breaches exceeding $1 million

Nearly half (48%) of organizations that suffered at least one breach in the past 12 months indicate that it cost more than $1 million to remediate, up from 38% in 2021.

- 64% of North American organizations report a total cost of breaches above $1 million, the most of any region.
- 31% of Latin American organizations report a total cost of breaches above $1 million, the fewest of any region.

64% of North American organizations report a total cost of breaches above $1 million, the most of any region.

Most leaders believe attacks will increase in the future

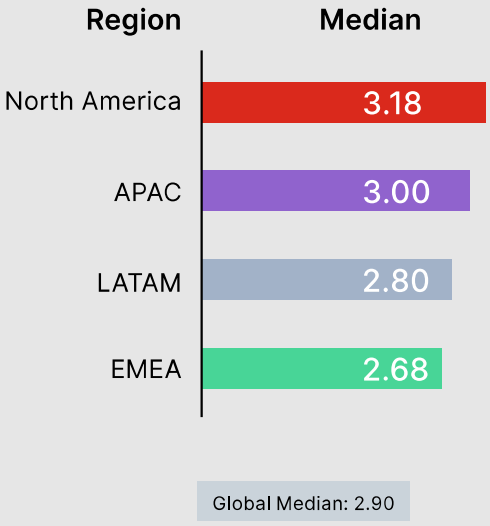
While most respondents (65%) expect cyberattacks to increase over the next 12 months, a surprising 19% indicate they expect no increase at all. Given analyst predictions to the contrary, these organizations could be vulnerable, as they likely won't prioritize security preparation for their networks, IT recruitment, or cyber-skills development for staff.

- North American respondents expect a 25% increase in attacks over the next year.
- Respondents in Europe, the Middle East, and Africa expect a slightly lower increase at 17%.

Regional Highlights

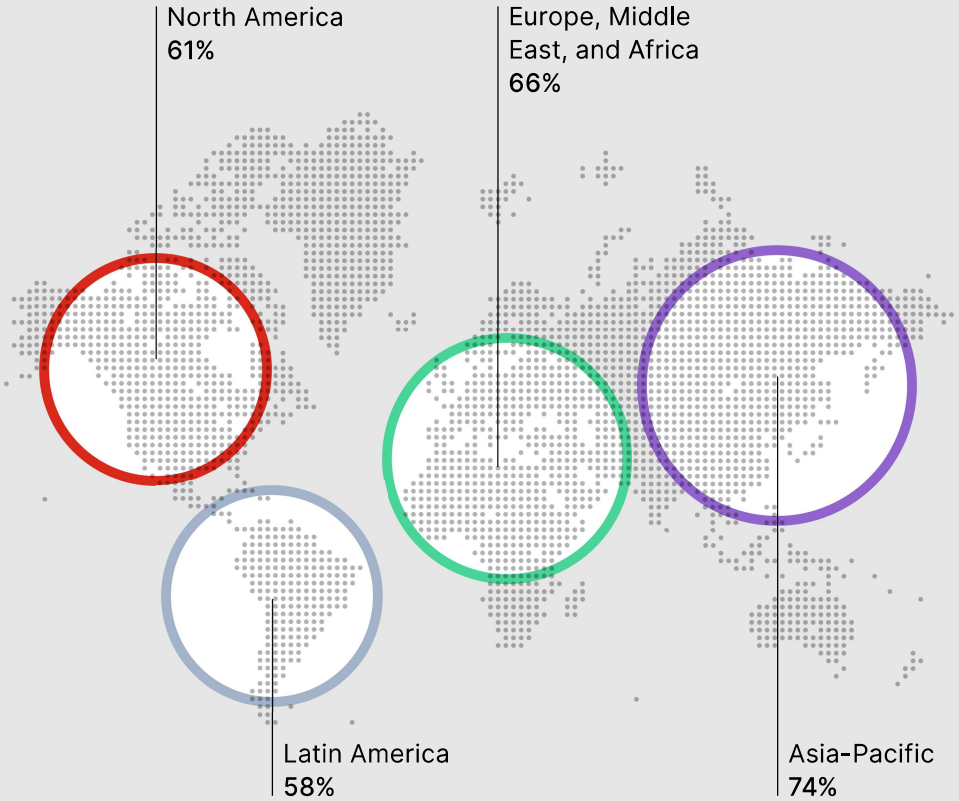
North American organizations report the most breaches

On average, respondents in North America indicate they had the most breaches, while those in Europe, the Middle East, and Africa experienced the fewest.



Asia-Pacific organizations are most likely to expect attacks to increase

Considerably more respondents in the Asia-Pacific region believe cyberattacks will increase over the next 12 months.



Boards of Directors are Focused on Cybersecurity

As cyberthreats and breaches increase, IT security continues to gain prominence at the governance level, with corporate boards asking direct questions about how organizations are protecting themselves.

In the past couple of years, analysts such as McKinsey and publications including the *Harvard Business Review* have spotlighted the role boards can play in helping organizations strengthen their security posture. The growing enterprise attack surface and diversification of threats have made this of paramount importance, given board responsibilities for overseeing corporate risk and reputation management.

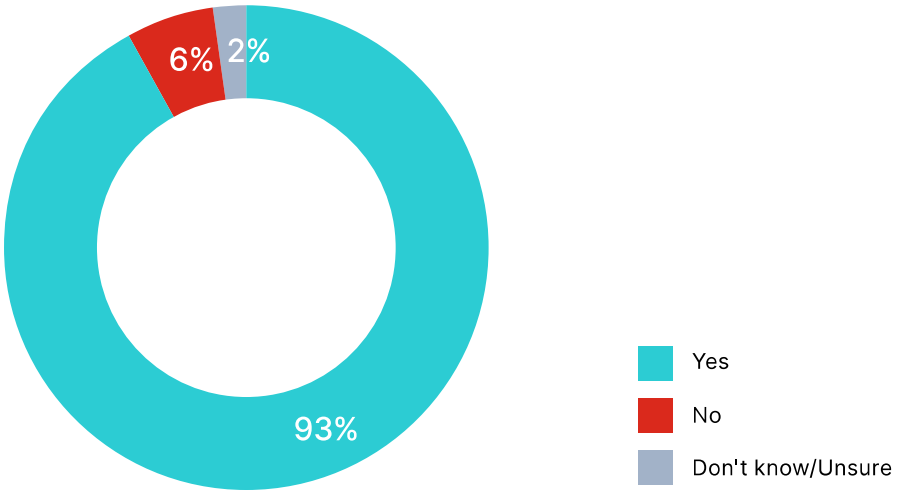
As a result, nearly all surveyed leaders (93%) indicate their boards are raising cybersecurity questions, and most boards (83%) are advocating for hiring more IT security staff.

83% of boards recommend increasing IT security headcount.

Board concerns grow with organization size

While most boards (93%) are asking questions about cybersecurity, that scrutiny is greatest (96%) in organizations with 1,000 to 2,499 employees.

Is your board of directors asking questions about how your organization is protecting itself against the increase in cyberattacks?



*Asked only those whose board whose organization reports to or has a direct line of communications to a board of directors.

Digging Deeper

Board concerns about cyberthreats are growing

Nearly all leaders (91%) surveyed either report to or have a direct line of communication with a board of directors.

- 93% indicate that their board asks how the organization is protecting against increasing cyberattacks, up from 88% in 2021.
- 96% of boards that govern organizations with 1,000 to 2,499 employees ask about cybersecurity.

Staffing up to strengthen security is a top board priority

Most boards recommend hiring IT and cybersecurity staff.

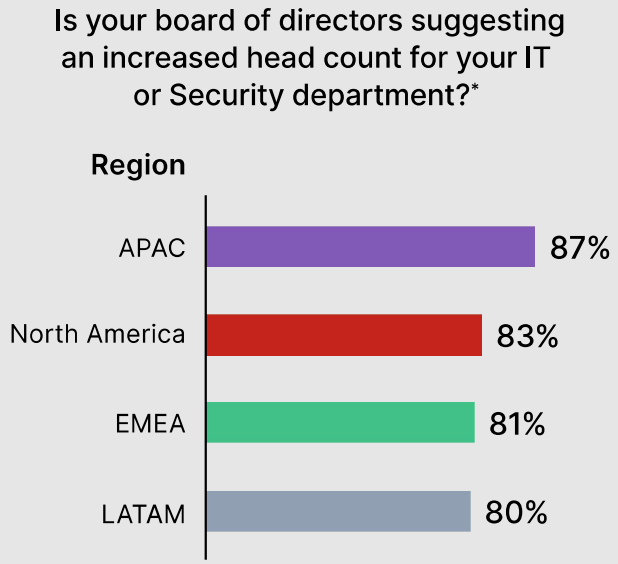
- 83% of leaders indicate that their board recommended increasing IT and cybersecurity headcount in 2022, up from 76% in 2021.
- 85% of boards that govern organizations with 5,000+ employees recommended increasing IT security headcount.

93% of boards are asking how the organization is protecting against increasing cybersecurity attacks.

Regional Highlights

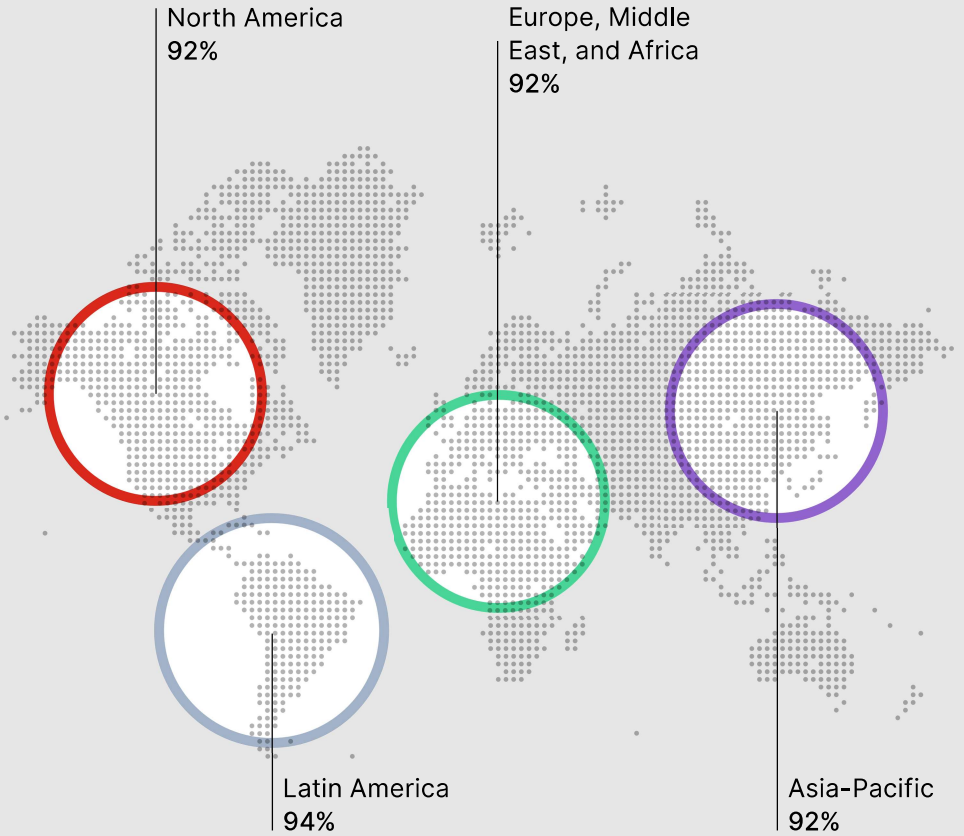
Boards in all regions are concerned about cybersecurity

The interest to protect organizations from cyberthreats is consistently high worldwide.



Boards in all regions advocate hiring more IT security staff

Those in the Asia-Pacific region were most inclined to push for adding cybersecurity headcount in 2022.



*Asked only those whose board board of directors is asking questions about how their organization is protecting itself against the increase in cyberattacks.

Certifications are Sought as Proof of Cybersecurity Knowledge and Skills

Most leaders recognize the value of specialized technical knowledge and skills. Eighty-two percent (82%) of respondents indicate their organization would benefit from cybersecurity certifications, and 90% indicate they would pay for an employee to obtain a cybersecurity certification.

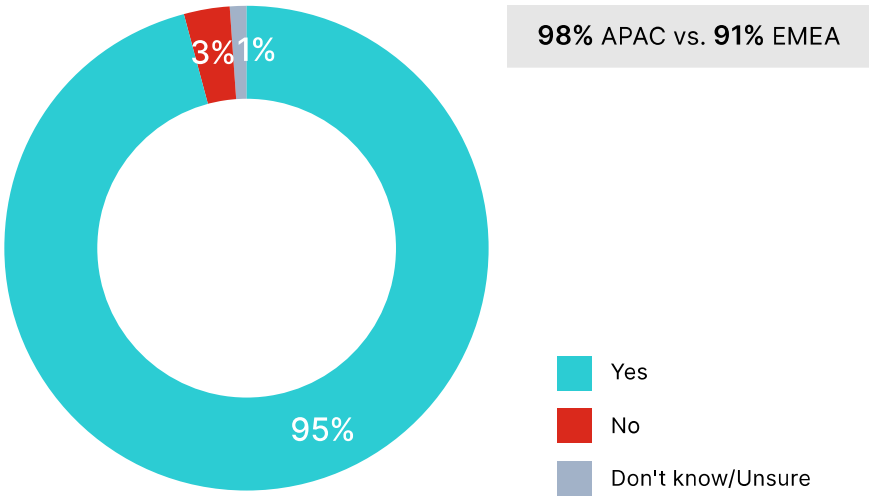
The need for certified professionals may be rooted in real-world experience, as most leaders have either a technology certification themselves or work with someone on their team who does, enabling them to better understand the value of obtaining certifications. Another hypothesis is that with the increasing threat landscape, leaders are leaving less to chance, and want validation that the professionals they are retaining or hiring have the required cybersecurity skills.

90% of leaders prefer to hire individuals with technology-focused certifications.

Certifications deliver real benefits

Leaders who have a technology certification themselves, or have someone on their team who does, indicate that being certified has had a positive impact on their role or their team's role.

Do you feel that holding technology-focused certifications has had a positive impact on you or your team's role?



98% APAC vs. **91%** EMEA

*Only asked to those who personally have a technology-focused certification and/or their team has.

Digging Deeper

More leaders prefer to hire employees with technology-focused certifications

Most respondents (90%) indicate they prefer to hire people with certifications, up from 81% the year before. Similarly, 90% would be willing to pay for employees to get certified.

- 84% have a technology-focused certification themselves.
- 86% have someone with a certification on their team.
- 73% indicate it continues to be hard to find people with technology-focused certifications, down from 78% in 2021.

Certifications benefit organizations and individuals alike

Nearly all leaders (95%) with certifications themselves or who have a certified employee on their team have experienced positive results.

- 72% indicate increased cybersecurity knowledge.
- 62% indicate better performance of duties.
- 55% indicate that certification has sped up their career growth compared to 34% in 2021.
- 47% indicate higher salaries, up from 29% in 2021.

Certifications rank highly alongside security awareness and training, and security solutions

The close ranking of all three options from respondents demonstrates that a three-pronged approach may be the best line of defense against cyberattacks.

- 82% indicate that their organization would benefit from cybersecurity training in the form of certifications.
- 75% indicate that their organization would benefit from security awareness and training for all employees.
- 71% indicate that their organization would benefit from new, better, or additional security solutions.

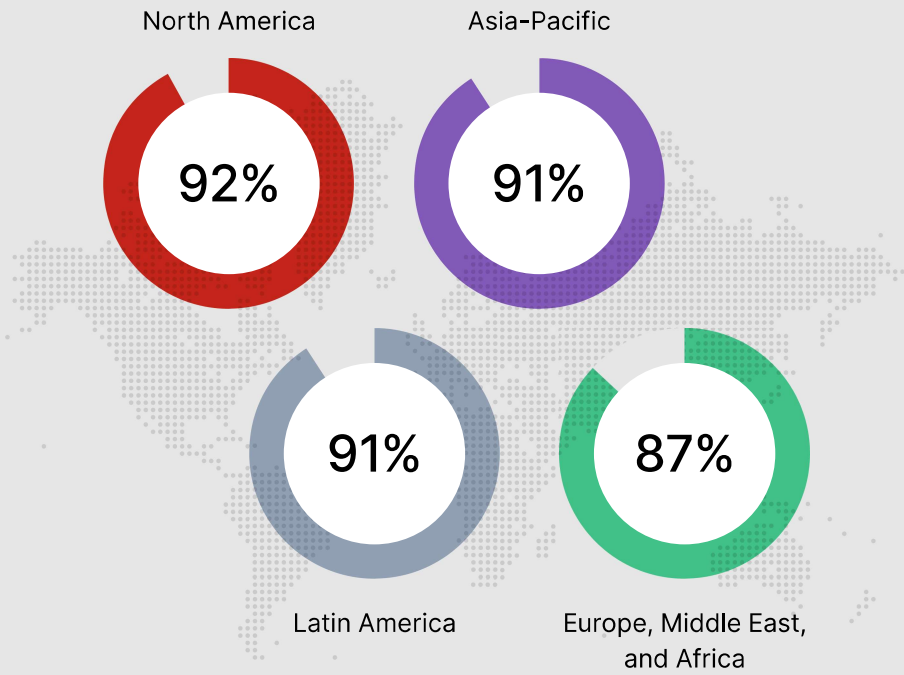
90% of leaders would be willing to pay for employees to get certified.

Regional Highlights

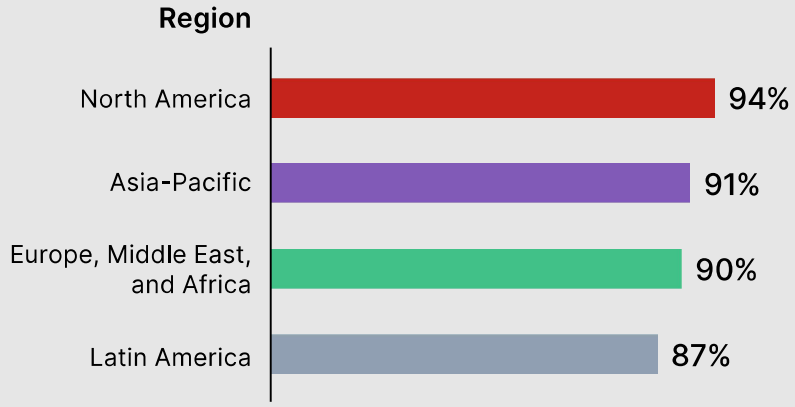
Organizations worldwide value certification

North American companies had the highest number of respondents who prefer to hire people with technology-focused certifications and are willing to pay for it.

Prefer to hire certified personnel



Willing to pay for employees to obtain certification



Unfilled IT Positions are a Cybersecurity Risk

More than half of leaders indicate they struggle to recruit and retain cybersecurity talent, creating skills shortages that pose additional cyber risks for their organizations.

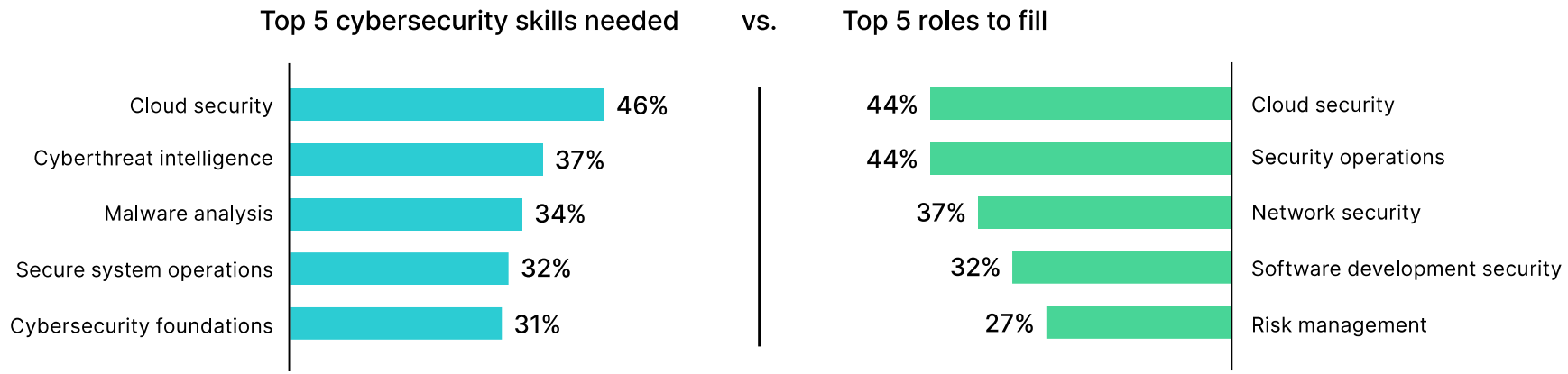
Recruitment and retention are essentially equivalent challenges, with skills needed most in the areas of cloud security, cyberthreat intelligence, and malware analysis. Specific roles that are proving hard to fill include cloud security, security operations, and network security.

Given the well-publicized burdens that cybersecurity teams are currently under to keep up with thousands of daily alerts, manage disparate tools, and protect a network perimeter that is increasingly dispersed due to cloud technologies and hybrid work models, these skills shortages are significant.

68% of organizations indicate they face additional risks because of cybersecurity skills shortages.

Cloud cybersecurity skills are needed most.

Cloud security tops the list of the most needed cybersecurity skills and hardest-to-fill roles for organizations.



Digging Deeper

Cybersecurity shortages increase risk

Sixty-eight percent (68%) of leaders agree that cybersecurity skills shortages create additional cyber risks for their organization, similar to 67% in 2021.

- 28% strongly agree with that statement.
- Only 7% strongly disagree with that statement.

Recruitment and retention are equally difficult

More than half (56%) of respondents indicate their organizations struggle to recruit cybersecurity talent, down slightly from 60% in 2021.

The majority (54%) indicate retention is also a challenge, up slightly from 52% last year.

- 44% indicate both cloud security and security operations roles are hardest to fill.
- 37% indicate network security roles are hardest to fill.
- 32% Indicate software development roles are hardest to fill.

Cloud security skills are needed the most in nearly half of all organizations

Leaders identified the following skills as highly needed by their organizations.

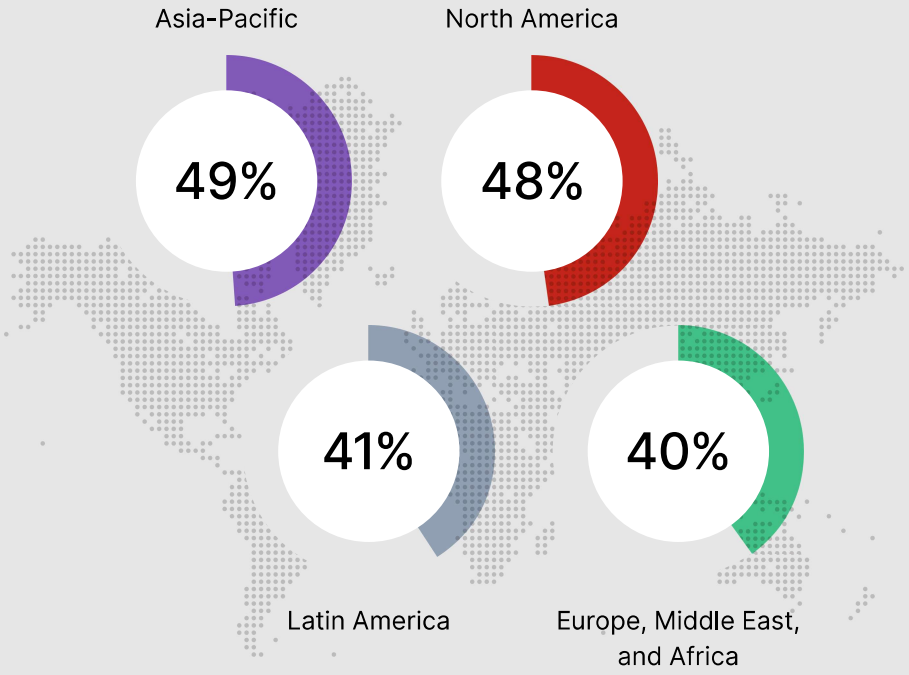
- 46% report the need for cloud security skills.
- 37% indicate cyberthreat intelligence skills are most needed.
- 34% indicate malware analysis skills are most needed.

46% report the need for cloud security skills.

Regional Highlights

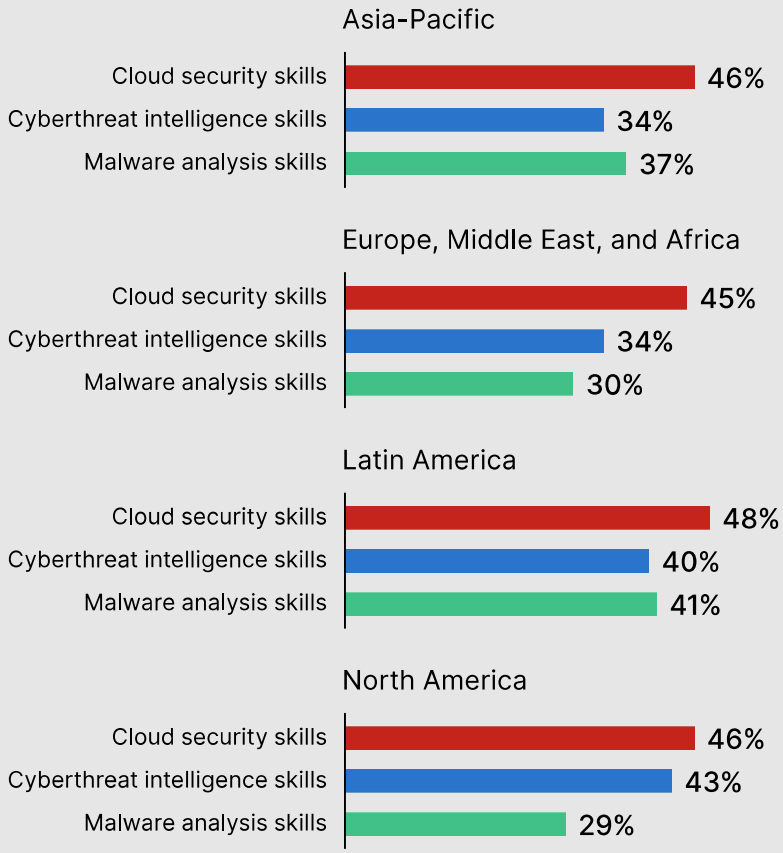
Some regions find it harder to fill cloud security roles

Organizations in the Asia-Pacific and North America regions face greater challenges filling cloud security roles compared to their counterparts in Latin America and Europe, the Middle East, and Africa.



Different regions require different skills

While organizations in all regions indicate they need cloud security skills, those in North America are much more likely to also need cyberthreat intelligence skills, while those in Latin America mostly need malware analysis skills.



Diverse Talent Can Help Meet Skills Needs but Isn't Always Easy to Find

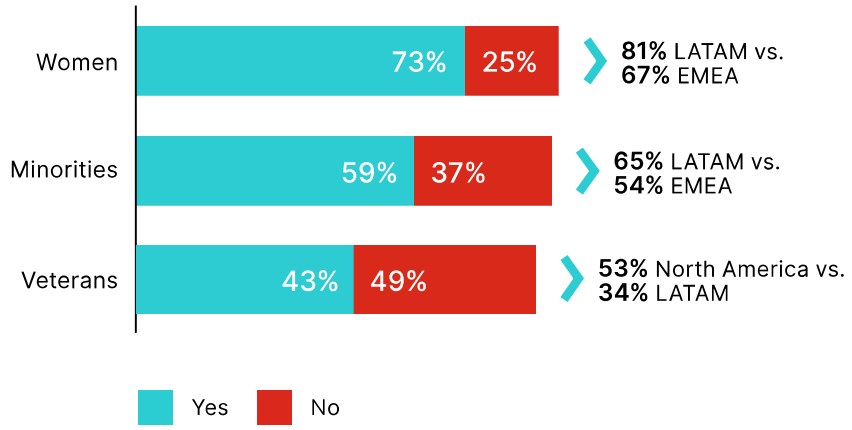
Most organizations (83%) have diversity goals for hiring over the next two-to-three years. Drawing from historically overlooked sources of talent can help fill skill gaps by expanding the overall pool of potential candidates. However, it remains challenging to find appropriately qualified individuals in some cases.

Organizations are constantly seeking out cybersecurity talent from various sources, in particular women, minority groups, and military veterans. This last group is often considered to already have the right training, orientation, and discipline to work in a cybersecurity context.

Of the three talent sources, finding and hiring qualified women is seen as a top challenge by most IT decision makers, considerably harder than hiring from minority and veteran populations.

Roughly 40% of organizations indicate they have difficulty finding qualified candidates who are women, military veterans, or from minority backgrounds.

Do you have any structured or formal recruiting initiatives in place that specifically target the following populations?



More recruitment initiatives target women.

To attract diverse talent, many organizations maintain recruiting initiatives aimed at women (73%) and candidates from minority populations (59%). However, between 2021 and 2022, similar initiatives for veterans fell from 51% to 43%.

Digging Deeper

Most organizations have diversity goals but have difficulty hiring

Eighty-three percent (83%) of organizations surveyed have near-term diversity hiring goals, down slightly from 89% in 2021.

- 69% indicate hiring women is a top challenge, holding steady with 70% in 2021.
- 56% indicate hiring people from minority backgrounds is a top challenge, down from 61% in 2021.
- 43% indicate hiring veterans is a top challenge, down from 53% in 2021.

Part of the challenge is finding qualified, diverse candidates

Respondents indicate recruiting qualified candidates from all three underrepresented groups is equally challenging.

The majority (54%) indicate retention is also a challenge, up slightly from 52% last year.

- 43% indicate difficulty recruiting qualified veterans, a slight drop from 45% in 2021.
- 41% indicate difficulty recruiting qualified women candidates, up significantly from 30% last year.
- 38% indicate difficulty recruiting qualified individuals from minority backgrounds, unchanged from last year.

Despite the challenges, diversity in hiring is happening

Many organizations hired from all three groups, especially women.

- 89% of respondents actively hired women, about the same as last year (88%).
- 68% hired individuals from minority populations, similar to 2021 (67%).
- 47% hired military veterans, a drop from 53% the previous year.

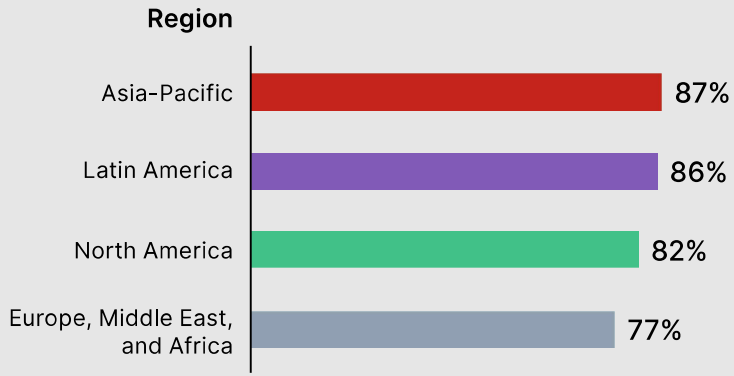
83% of organizations surveyed have near-term diversity hiring goals, down slightly from 89% in 2021.

Regional Highlights

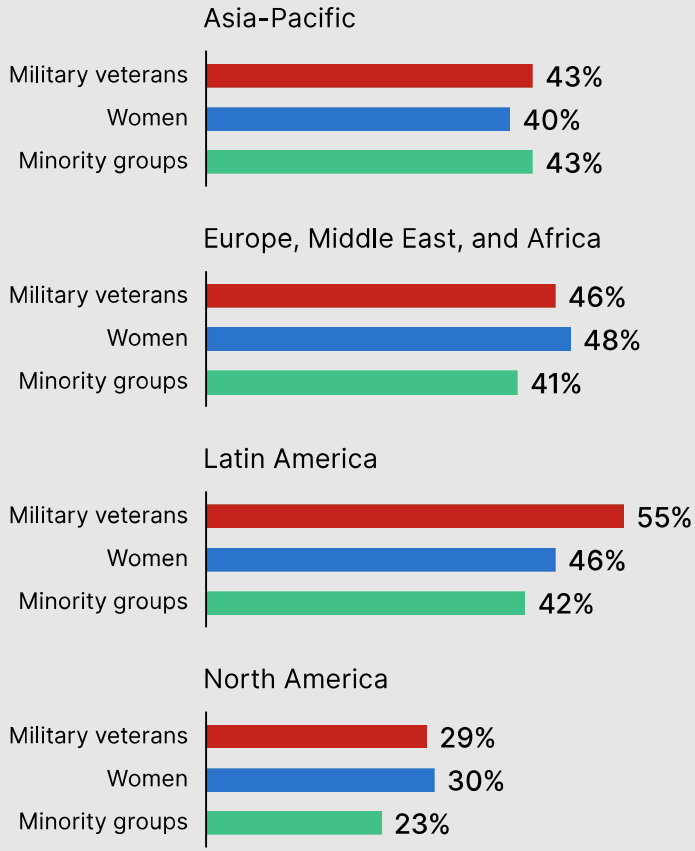
Across the regions, organizations encounter different HR challenges

Companies in the Asia-Pacific region and Latin America are most likely to have diversity hiring goals for the next two-to-three years. Region by region, hiring from underrepresented groups is harder.

Diversity hiring goals by region



Challenges hiring from different groups



Conclusion

The evolving threat landscape and rising incidence of breaches make it imperative that organizations continue building their cybersecurity defense to protect their networks, systems, data, customers, partners, and employees. When considering their cybersecurity strategies, leaders need to look at three factors:

- **Advanced solutions** to deal with real-time threats in complex, distributed IT environments
- **Expert teams** who have the knowledge and skills to manage cybersecurity effectively
- **A cyber-aware culture** for every individual in their organization

Greater interest by corporate boards

Corporate boards are paying closer attention to cyber risk and the associated human factors, creating more conversations at the board level about what is being done to mitigate risk. Specific conversations about increasing the size of IT security teams are pushing organizations to pay more attention. This increase in attention at the board level will likely drive organizations to double down on efforts to recruit and retain qualified employees and develop a hiring strategy for required and hard-to-find cybersecurity skills, especially with growing recognition that unmet skills create additional risk for many organizations. Leaders needing to demonstrate to their boards that they are aware of the current and future state of the threat landscape will want to get ahead of these ongoing conversations.

48% of organizations that suffered at least one breach in the past 12 months indicate that it cost more than $1 million to remediate, up from 38% in 2021.

Certifications take center stage

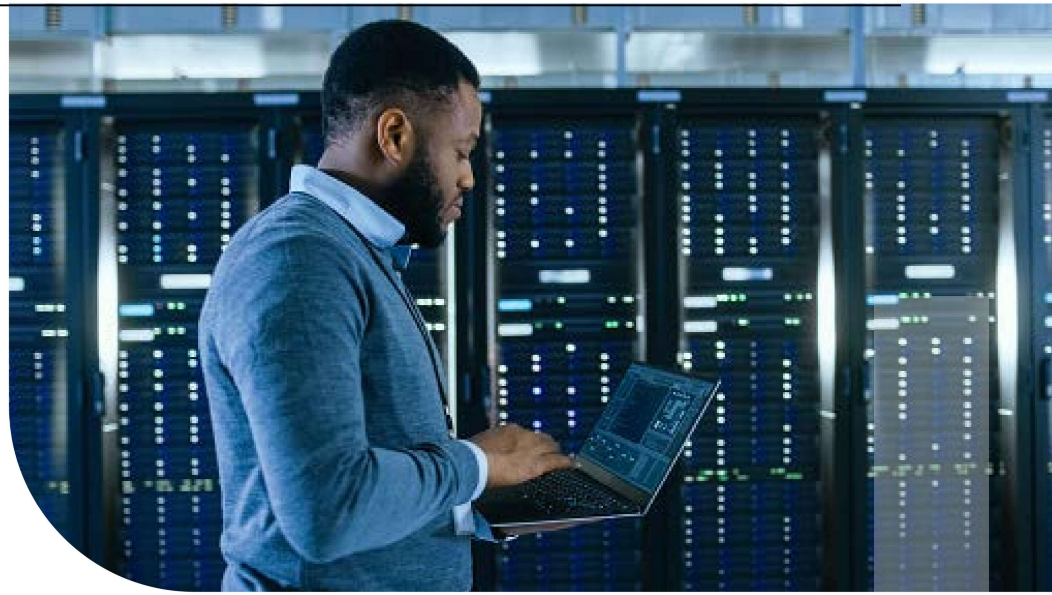
Whether hiring new employees or seeking to boost the knowledge of existing IT security staff, leaders are turning more and more to certifications to validate individual skills. Well-designed certification programs aim to establish not only technical competencies but also a deeper understanding of how to apply those competencies in the context of a given role.

Investing in people often strengthens employee commitment. Fortinet feels that by investing in and developing their existing IT security workforce, organizations can reduce issues of talent retention. By encouraging and supporting employees to obtain or renew their certifications, organizations can increase employee loyalty, increase retention, and ensure individuals' skills stay up to date.

Seeking talent in new places

Expanding the talent pool to draw from more diverse groups will continue to be critical so that organizations can meet their staffing needs. In 2021, it was estimated that women made up just a quarter of the global cybersecurity workforce.[3] While minority populations vary by country and region, it seems generally true that these groups are underrepresented in the cybersecurity field. In the U.S. for example, only 9% of cybersecurity experts are Black, 8% are Asian, and 4% are Hispanic.[4]

Military veterans often have the unique advantage of already having a defense mentality and are well trained to learn new skills and transition between roles. The industry has much to gain by attracting individuals from this group and building on their existing training and skills—both technical and soft skills.



Corporate culture counts

Outside of cybersecurity technologies and specialists, leaders have one other powerful tool to protect themselves: a strong, internal cybersecurity culture. Leaders can cultivate a strong culture by increasing employee awareness of the need for good cybersecurity hygiene. For more on employee cybersecurity awareness, read our companion report: the 2023 Security Awareness and Training Global Research Brief, which will publish this spring.

The good news is that progress continues in the fight against cybercrime, and organizations that are committed to strengthening their security posture are not alone. From the World Economic Forum Partnership Against Cybercrime (PAC) to the NATO Industry Cyber Partnership and MITRE Engenuity Center for Threat-Informed Defense, many governing bodies are engaged in protecting businesses from cyber threat. We at Fortinet are proud to be an active contributor to many of these efforts.

[3] Tayo Bero, "Cybersecurity is a red-hot career choice – why aren't more women working in this space?" The Globe and Mail, Aug. 24, 2022.
[4] Ben Allen, "Minorities and the Cybersecurity Skills Gap," Forbes, Sept. 30, 2022.

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 you 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. 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 www.fortinet.com, the Fortinet Blog, and FortiGuard Labs.

FORTINET
Training Institute

www.fortinet.com

March 2023