FORTINET
Training Institute

2024 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 1850 IT and cybersecurity decision-makers conducted by Sapio Research in January 2024. The survey and interviews were conducted in the following 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.

Size of Company

100-499 employees **24%**
500-999 employees **23%**
1,000-2,499 employees **21%**
2,500-4,999 employees **17%**
5,000+ employees **14%**

Role Type

13% 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

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

Top Three Business Sectors:

Technology **21%**
Manufacturing **15%**
Financial Services **13%**

Total respondents: 1,850

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

Executive Summary

When it comes to cybersecurity in 2024, the stakes are high for organizations. Breaches continue to take a financial toll—and senior leaders are penalized when they happen. In response, organizations are focusing on a three-pronged approach to cybersecurity that combines training, awareness, and technology.

Corporate leaders are being held accountable

51% of respondents say that directors or executives have faced fines, jail time, loss of position, or loss of employment following a cyberattack.

To improve cybersecurity, boards have discussed or implemented the following measures:

- Mandatory training or certifications for IT/ security staff **(64%)**
- Security awareness training for all staff **(61%)**
- Purchasing security solutions **(59%)**

72% of respondents say their boards were more focused on cybersecurity in 2023 than the year before.

Breaches consume precious time and money

87% of respondents report having experienced one or more security breaches in 2023.

63% of respondents say it took longer than a month to recover from a cyberattack.

53% of respondents say breaches cost them more than $1 million in lost revenue, fines, and other expenses. This is up from 48% in 2022 and 38% in 2021.

Cybersecurity depends on three key factors

IT leaders say that the top three causes of breaches are:

- An IT/security staff that lacks the necessary skills and training **(58%)**
- A lack of organizational or employee security awareness **(56%)**
- A lack of cybersecurity products **(54%)**

70% of respondents agree that the cybersecurity skills shortage creates additional risks for their organizations.

62% of IT decision-makers say that the greatest challenge is finding candidates with specific experience in network engineering and security.

Candidates with certifications stand out

91% of respondents prefer to hire candidates with certifications.

89% of respondents would pay for an employee to obtain a cybersecurity certification.

72% of respondents say it is difficult to find candidates with technology-focused certifications—down slightly from 2022 (73%) and down from 78% in 2021.

Organizations may be overlooking candidates from underrepresented backgrounds

83% of companies have set diversity hiring goals for the next few years.

71% require four-year degrees and **66%** hire only candidates with traditional training backgrounds.

Despite ongoing targets, diversity hiring varies from year to year:

- Active hires of women are down to **85%** from 89% in 2022 and 88% in 2021.
- Active hires from minority groups is unchanged at **68%** and up slightly from 67% in 2021.
- Active hires of veterans are up slightly to **49%** from 47% in 2022, but down from 53% in 2021.

INTRODUCTION

Cybersecurity Requires an All-Hands-On-Deck Approach

Last year's Cybersecurity Skills Gap Report indicated that boards of directors were taking more interest in cybersecurity. The 2024 report includes new questions, designed to dig deeper, that reveal why this is the case and highlight companies' increasingly holistic approach to fighting cyberthreats.

When writing this report, we looked at cybersecurity skills challenges through five lenses: business leaders' priorities, the threat landscape, cybersecurity strategies, the value of certifications, and hiring from diverse talent pools.

What we found is that the increasing frequency of costly cyberattacks, combined with the potential of severe personal consequences for board members and directors, is resulting in an urgent push to strengthen cyber defenses that is coming from the top, down.

This year's report includes comparative statistics, for some questions, that go back to 2021 and digs deeper into key topics to create a fuller picture of the state of the skills gap today. It also includes additional details related to the board-level view of cybersecurity and new data about the effects of breaches and details about how organizations plan to respond to those effects.

It's clear that some persistent challenges remain to be solved. The cybersecurity skills gap is still taking a toll on the industry. In addition, the recruitment and retention of employees with the required skill set remains difficult for most respondents. This may be due, in part, to their continued under-utilization of nontraditional talent pools and requirements for "traditional" credentials.

The overarching takeaway is that effective cybersecurity requires a three-pronged approach:

1. **Help IT and security teams** obtain vital cybersecurity skills by investing in the training and certifications required to achieve this goal.
2. **Cultivate a cyber-aware frontline staff** who can contribute to security as a first line of defense.
3. **Obtain and use effective cybersecurity solutions**, to ensure a strong security posture.

51% of organizations say senior leaders have faced fines, jail time, loss of position, or loss of employment following a cyberattack.

Corporate Leaders Are Being Held Accountable

Today, boards of directors are taking more interest in cybersecurity, and their interest may be personally motivated. Just over half (51%) of respondents say directors or executives have faced fines, jail time, loss of position, or loss of employment following a cyberattack.

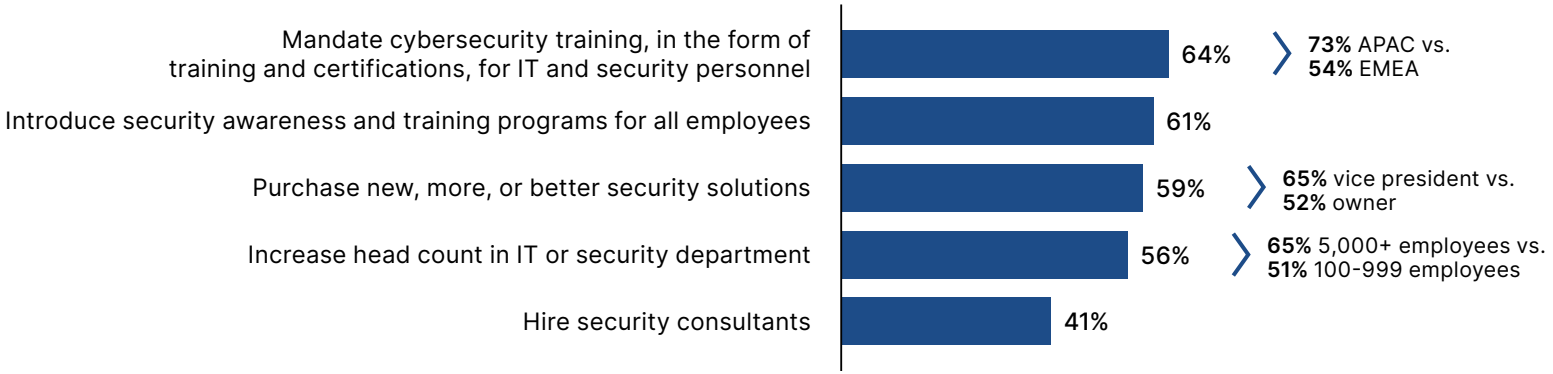
Given those stakes, it's not surprising that nearly three-quarters (72%) of respondents say their boards were more focused on cybersecurity in 2023 than in the previous year. Improvements discussed or implemented by boards include mandatory cybersecurity training or certifications for IT and security personnel (64%); security awareness training for all employees (61%); and the purchasing of new, more, or better security solutions (59%).

These improvements align with IT leaders' views that a lack of skills and trained staff, as well as insufficient awareness and products, are the main causes of security breaches. See page 17 for more information.

Boards' cybersecurity priorities: training, awareness, and solutions

Board members seem to recognize that knowledge, skills, and awareness are vital first lines of a sound cyber defense, and that technology is essential to backing them up.

Improvements being discussed or implemented



DIGGING DEEPER

Boards See Cybersecurity as a Business Imperative

Boards are taking action on cybersecurity

In the previous year, 93% of respondents said their board members were asking about cyber defenses. This year's survey digs deeper into which aspects of cybersecurity boards are focused on.

- 97% of respondents say their board considers cybersecurity to be a business priority.
- 56% say their board has discussed or implemented increasing IT/security headcount.

Leaders face penalties in organizations of all sizes

The risk of penalties for board members or executives is about the same across all organizations.

- At the highest end, 59% of organizations with 2,500–4,999 employees report leaders in their organizations faced penalties following cyberattacks.
- 48% of small organizations (100–999 employees) and 48% of very large organizations (more than 5,000 employees) report that their leaders also faced penalties.

Fines are the most common penalty for leaders

Most board members and company executives who were held accountable received financial penalties after a cyberattack, though other serious consequences were meted out as well.

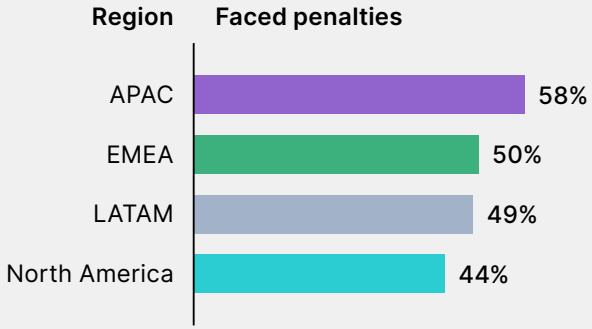
- 34% received fines.
- 33% lost their position or their job.
- 16% faced prison sentences.

97% of respondents say their board sees cybersecurity as a business priority.

Regional Highlights

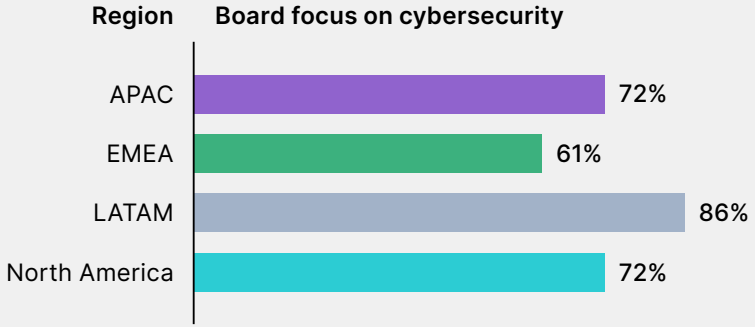
Asia-Pacific leaders most likely to face penalties

Executives and board members in the Asia-Pacific (APAC) region are most likely to face fines, jail time, loss of position, or loss of employment after a cyberattack.



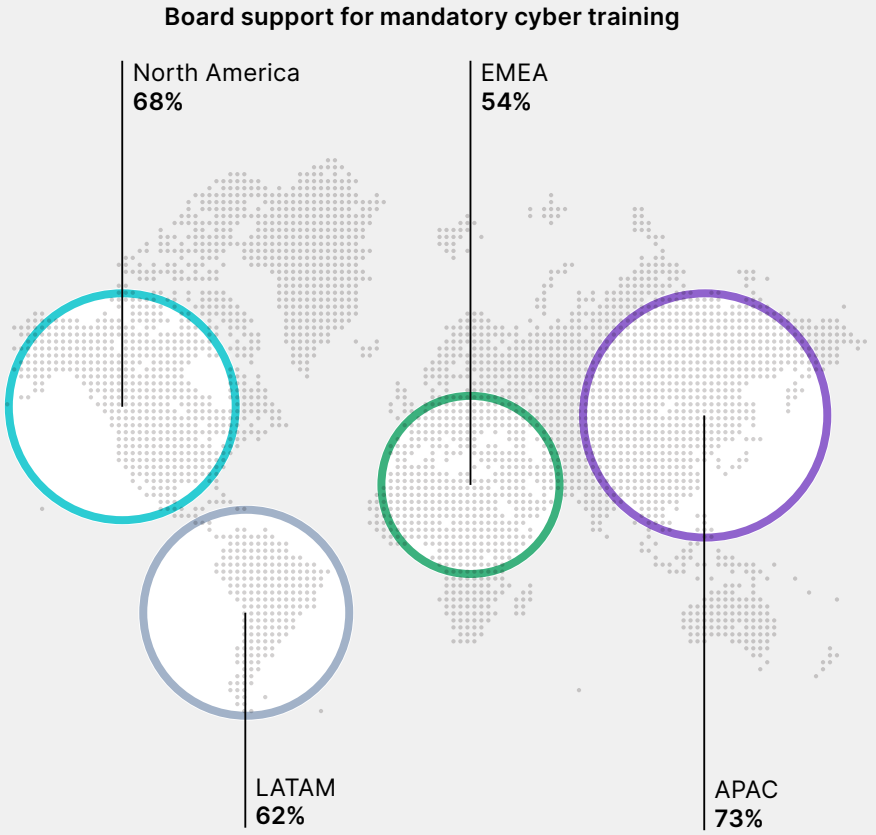
Increased board focus on cybersecurity highest in Latin America

Boards in Latin America (LATAM) are most focused on cybersecurity compared to the previous year, boards in Europe, Middle East, and Africa (EMEA) are the least.



APAC boards most likely to support mandatory cybersecurity training

Board support for mandatory cyber training for IT and security personnel was highest in APAC and lowest in EMEA.



53% of respondents say breaches cost their organizations over **$1 million** in 2023.

Breaches Consume Precious Time and Money

The vast majority (87%) of organizations say they have experienced one or more security breaches in 2023, with more than half (53%) reporting over $1 million in lost revenues, fines, and other expenses—up from 48% in 2022 and 38% in 2021.

A smaller percentage of organizations report experiencing no breaches at all—just 13% in 2023 compared to 15% the year before and 20% in 2021. At the same time, breaches seem more likely to take a financial toll. Only 17% of this year's respondents say cyberattacks have not cost their organization any money, down from 21% in 2022 and 36% in 2021.

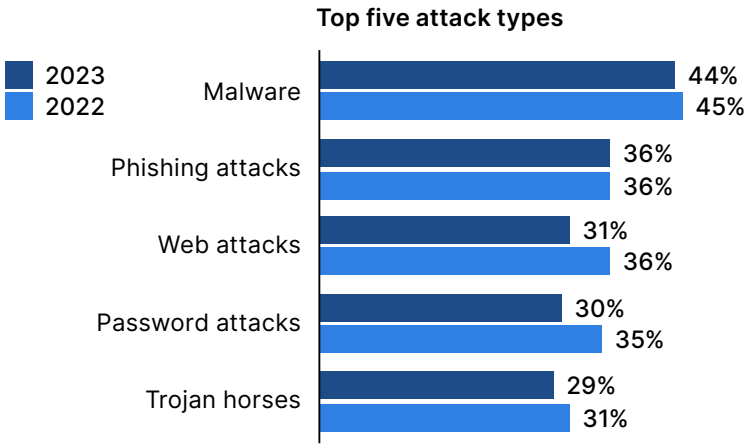
The breaches that respondents reported were the result of many different types of attacks. Malware, phishing, and web attacks combined account for 80% of all attacks throughout the year. Many of the most frequently used attack types target individual users directly, underscoring the importance of general security awareness.

One or more cybersecurity breaches

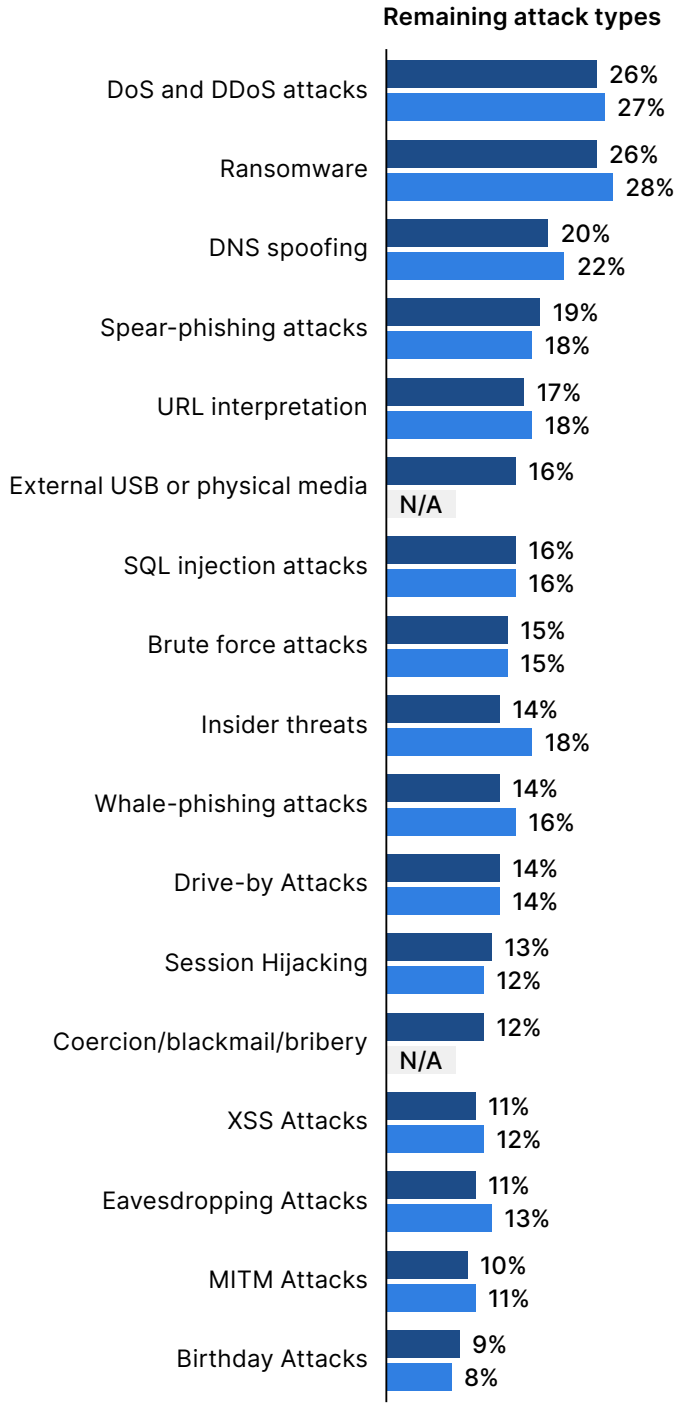
Malware, phishing, and web attacks combined account for **80%** of all attacks throughout the year.

A Familiar Threat Landscape

The top five most commonly experienced attacks in 2023 are the same as those in the previous year: malware, phishing attacks, web attacks, password attacks, and trojan horse attacks.



The graphic on the right depicts the remainder of the attacks included in this year's survey. New attack types added to this report for survey analysis were: external USB or physical media attacks (16%) and coercion and blackmail or bribery of internal staff (12%).



DIGGING DEEPER

Recovering From an Attack Is Difficult

Recovery can be time-consuming

Respondents' average time to recover was nearly three (2.7) months.

- The majority (63%) of organizations needed more than one month to recover from a cyberattack.
- 35% took one to three months to recover.
- For nearly a third (28%), recovery took four months or longer.

Companies expect attacks to increase in number and frequency

Given the intensification and mounting consequences of attacks, most respondents expect things to get worse before they get better.

- 80% expect cyberattacks to increase over the next year (up from 65% in 2022).
- When asked how much they thought attacks would increase, on average, respondents say they expect an increase of 19.3% in the next 12 months. This is roughly on par with 2022, when the average was 20%.

Size and scale seem to attract attacks

Companies of a certain size and those in certain industries tend to report experiencing multiple cyberattacks.

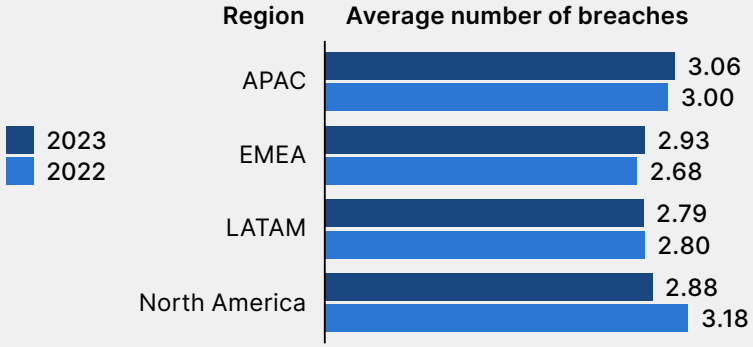
- 36% of companies with 1,000–2,499 employees reported five or more attacks in the past 12 months—up from 35% in 2022.
- 34% of companies with 2,500–4,999 employees reported five or more attacks—down from 38% in 2022.
- Oil and gas companies experienced the highest occurrence of multiple attacks of any industry, with 56% citing five or more—up from 34% in 2022.

On average, recovery from a cyberattack takes **2.7 months**.

Regional Highlights

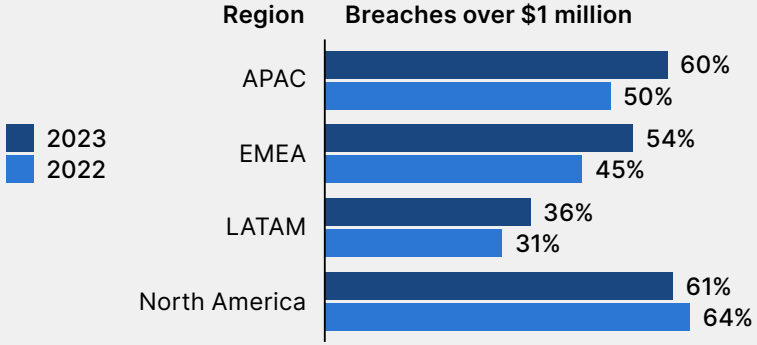
Breaches are equally common worldwide

While APAC's average is slightly higher and LATAM's is slightly lower, all regions report a similar average number of breaches.



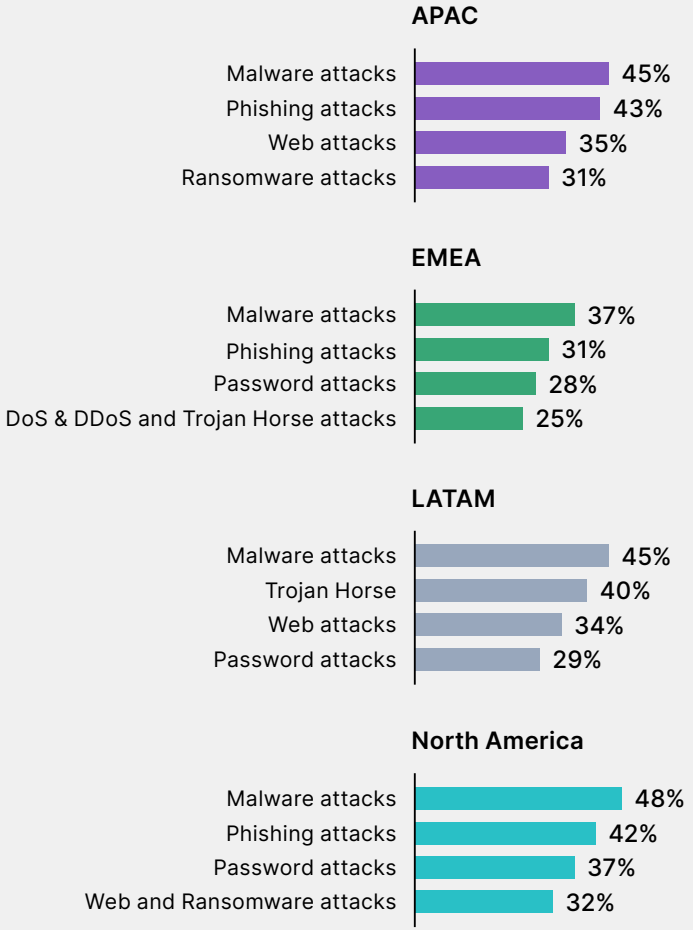
North America and APAC had more costly attacks

North America and APAC continued to report the most financially damaging attacks, costing over $1 million in 2023. Except for North America, all regions saw an increase in more costly attacks compared to 2022.



Top attack types differ slightly by region

Malware attacks were the most common attack type across all regions. Password attacks were more common in North America than in any other region. Respondents in APAC experienced a higher percentage of phishing and web attacks than other regions.



58% of IT decision-makers say that the top cause of security breaches is IT/security staff with a lack of cybersecurity skills and training.

Cybersecurity Depends on Three Key Factors

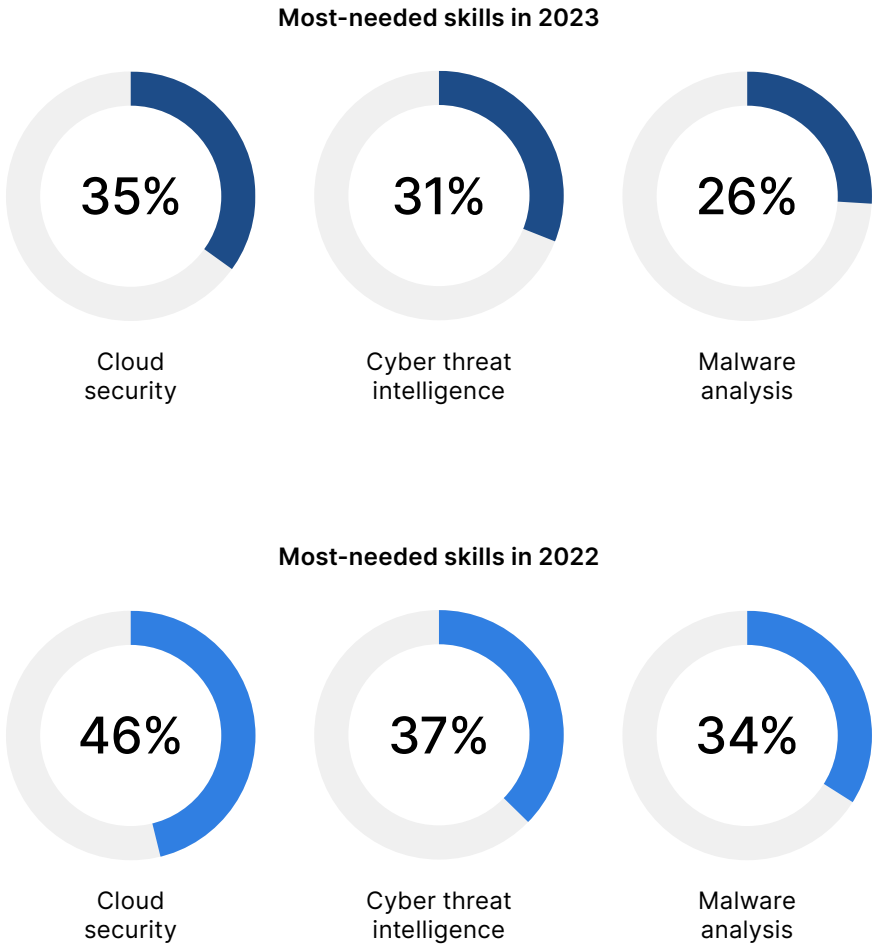
As the saying goes, knowledge is power. Conversely, a lack of knowledge would be considered a weakness or, in the case of cybersecurity, a major liability. Well over half (58%) of respondents say insufficient skills and a lack of properly trained IT/security staff are the prime causes of breaches. Additionally, 56% point to a lack of organizational or employee security awareness, and 54% blame a lack of essential cybersecurity products.

Given that technical skills, staff, and security solutions are viewed as key factors, it makes sense that 65% of IT leaders say they plan to grow their IT/security teams in response to experiencing a cyberattack.

Nearly as many (62%) say they will mandate cybersecurity training in the form of certifications for IT and security personnel. Almost as many (61%) say they will introduce security awareness and training programs for all employees, and a majority (59%) also say they plan to purchase more, newer, or better security solutions.

In-demand skills hold relatively steady

Between 2022 and 2023, the top three in-demand cybersecurity skills remained the same across all participating organizations. While there is no clear cause for the shift in percentages, note that new skills were added to the 2023 list, which were not present in the previous survey.



DIGGING DEEPER

People Are Essential to Cybersecurity

Skills shortages are a liability

70% of respondents agree that the cybersecurity skills shortage creates additional risks for their organizations, up slightly from 68% in 2022 and 67% in 2021.

- 62% of respondents say it's difficult to find candidates with network engineering and security experience.
- The most difficult roles to fill continue to be security operations and cloud security (43%)—just down slightly from 44% for both in 2022.

Recruitment challenges are seen as a supply problem

Organizations are finding it easier to recruit, though challenges remain.

- 54% of organizations say they struggle to recruit cybersecurity talent. These numbers are down slightly from 56% in 2022 and 60% in 2021, but recruiting candidates with cybersecurity expertise remains an issue for more than half of respondents.
- 51% of respondents say the talent pools for the required skill sets are generally lean.

Employees want to learn and grow

Retention pressures may be easing slightly because employees highly value training and upskilling.

- Slightly fewer organizations (50%) say they are struggling to retain cybersecurity talent compared to 2022 (54%) and 2021 (52%).
- The greatest challenge to retention comes from organizations' inability to offer sufficient training and upskilling opportunities (50%).
- Salary/benefits (41%) and remote/hybrid work arrangements (38%) are lesser concerns.

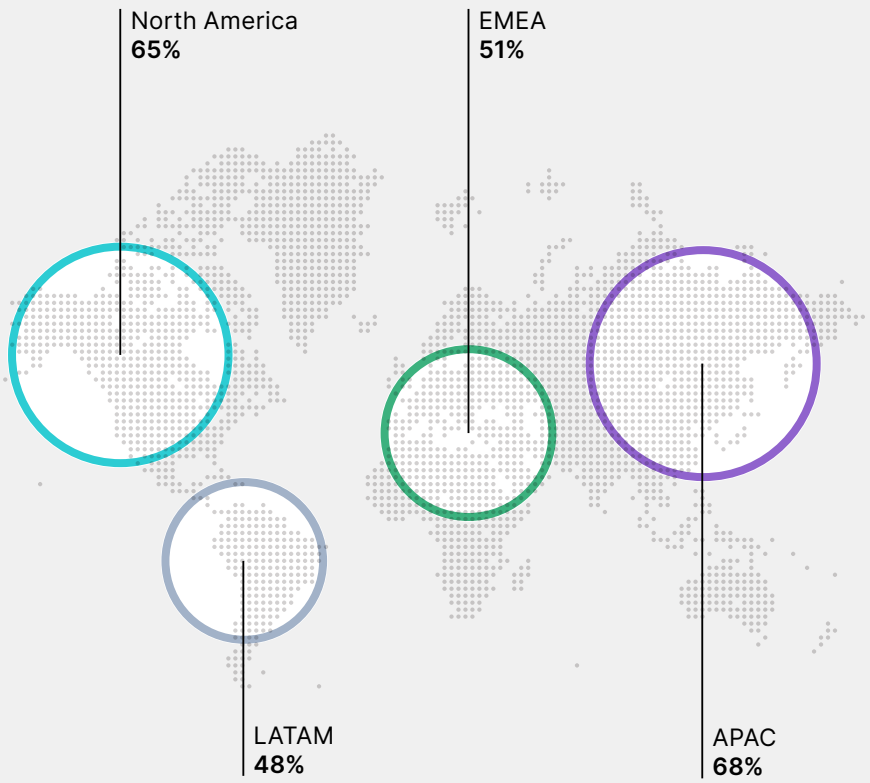
50% of respondents say a lack of training and upskilling opportunities is the biggest retention challenge.

Regional Highlights

The link between breaches and skills is strongest in APAC

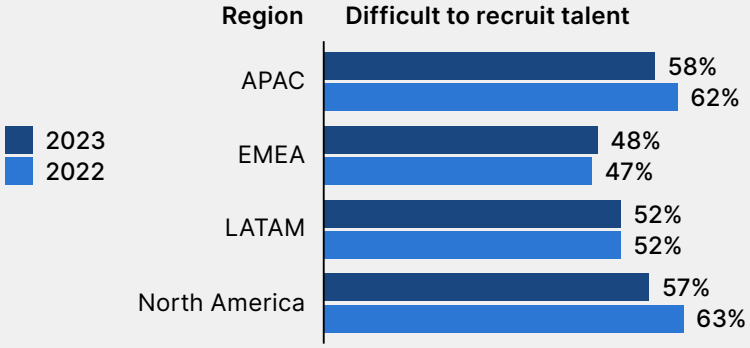
68% of companies in APAC attribute breaches to a lack of cybersecurity skills and training, compared to just 48% in LATAM.

Attribute breaches to lack of skills and training



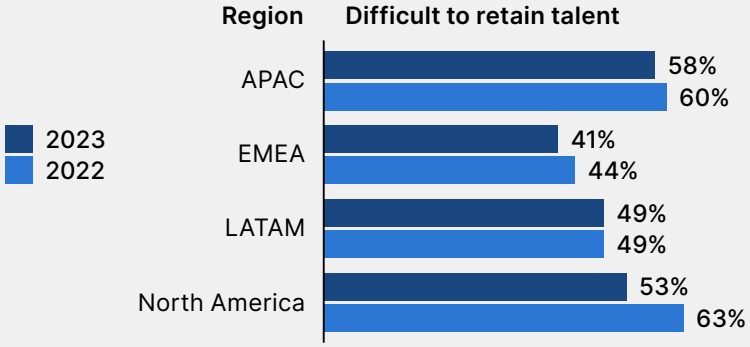
APAC and North America struggle the most with recruitment

This remains the same as in 2022, though at slightly higher percentages.



APAC companies report more difficulty with retention

Organizations in North America indicate a significant decrease in difficulty retaining talent compared to 2022. EMEA had a slight decrease, while LATAM stayed the same.



91% of leaders prefer to hire candidates with certifications.

Candidates With Certifications Stand Out

IT leaders widely regard certifications as badges of cybersecurity know-how. Nearly all (91%) prefer to hire candidates with certifications—a figure that is in line with 2022 and up 10% from 2021. The majority (67%) of respondents prefer team members or direct reports to have certifications because they believe that these credentials validate cybersecurity awareness and knowledge.

While demand is high, 72% of respondents say it's difficult to find individuals with technology-focused certifications. This percentage is similar to 2022 (73%) but down from 78% in 2021, suggesting that the search for certified talent may be getting slightly easier.

Eighty-nine percent (89%) of IT leaders say they would pay for an employee to obtain a cybersecurity certification. This high rate of "yes" responses has held relatively stable (90% in 2022 and 91% in 2021) for the past three years.

Certifications make a measurable difference

Those who have a certification or work with someone who holds a certification notice clear benefits. Increased skills and knowledge top the list of those benefits.

The impact of certifications

DIGGING DEEPER

Certifications Foster Trust

IT leaders know firsthand the value of certifications

84% of respondents have a certification themselves. This is the same as in 2022 and close to 2021 (86%).

- 85% have a team member with a certification, down just one percent from last year and only slightly below 2021 (88%).
- The relative stability of the percentage related to certifications over three years may indicate that people and organizations are seeing the importance of certifications.

Certifications boost awareness and knowledge

67% of respondents say certifications validate cybersecurity awareness and knowledge—similar to 2022 (68%).

- 58% say certifications indicate familiarity with security vendor products—up from 54% in 2022.
- Only 1% say having a certification had no impact on their job.

Certifications improve security posture

61% of respondents say certified individuals are better able to keep up with the evolving security landscape. This is down slightly from 66% in 2022 but up from 42% in 2021.

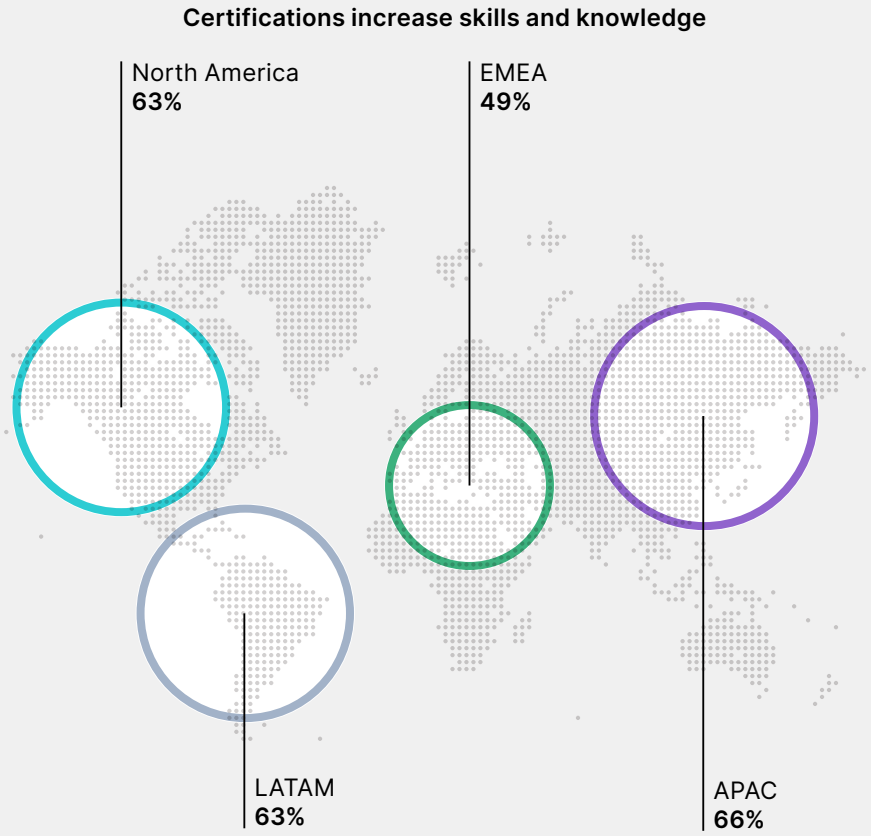
- 70% of those who hold this view say their organization faced nine or more cyberattacks in the past year; 59% faced one to four.
- These correlations may suggest that those who have had to fend off a cyberattack, value certifications.

61% believe certifications improve an individual's ability to keep up with the evolving security landscape.

Regional Highlights

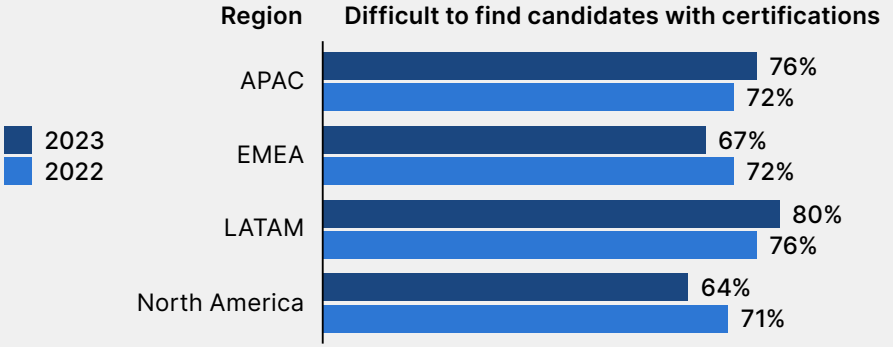
APAC organizations have high confidence in certifications

Respondents in APAC were most likely to say certifications increase skills and knowledge.



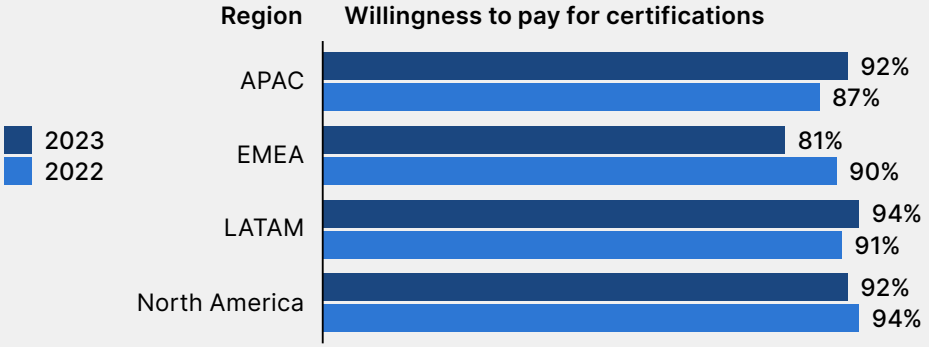
Certified professionals are most difficult to find in LATAM

Finding certified candidates has become more difficult for companies in LATAM and APAC, and easier for those in North America and EMEA.



Organizations worldwide pay for certifications for employees

Willingness to pay for an employee increased in APAC and LATAM, but decreased in North America and EMEA.

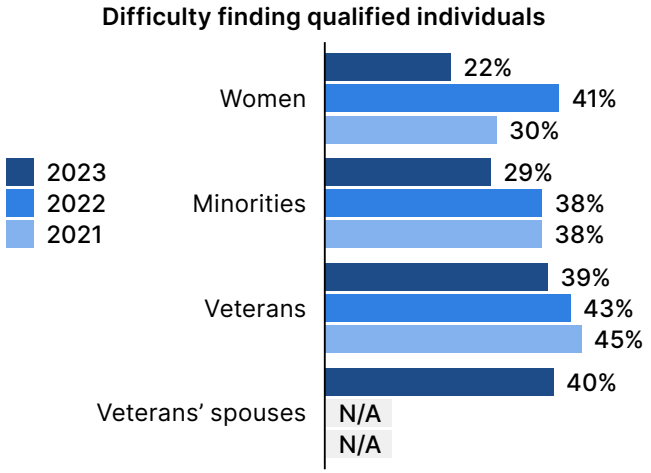


83% of companies have diversity goals for hiring in the next two to three years.

Organizations May Be Overlooking Candidates from Underrepresented Backgrounds

With the global cybersecurity skills shortage persisting, and equity and inclusion becoming increasingly entrenched as pillars of corporate responsibility, diversity hiring continues to be a declared goal for many organizations.

Most (83%) companies report that they have diversity hiring goals slated for the next few years—in line with 2022, though down somewhat from 89% in 2021. Women and minority groups are the top targets at 76% and 64%, respectively. This may be because qualified women and minority candidates are easier to find, though respondents say it has become less difficult to find candidates from all groups.[1] Veterans and their spouses are the groups that follow at 49% and 41%, respectively.



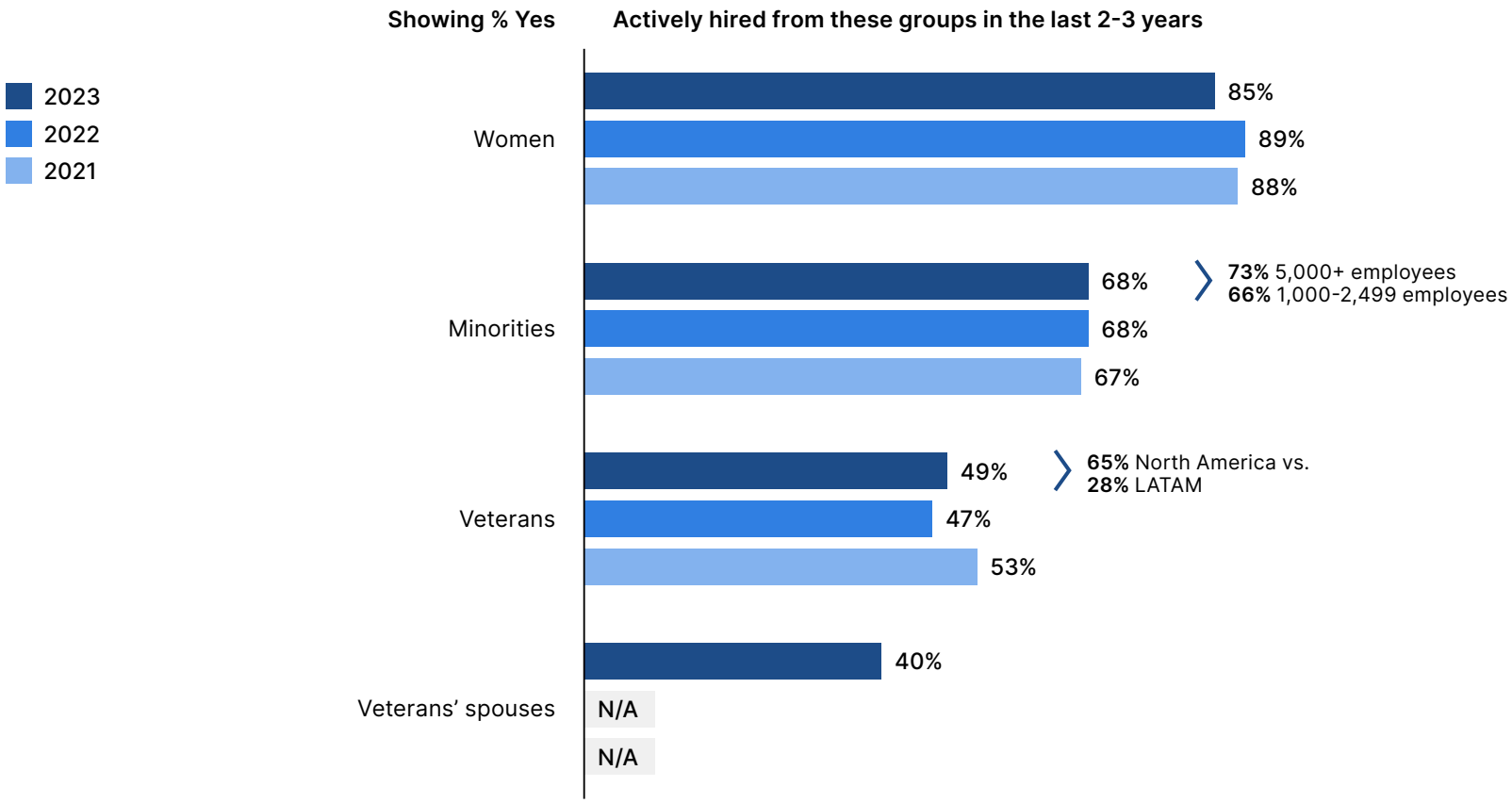
While qualified women (51%) candidates have become easier to find, fewer organizations have actively hired women in the past two to three years: 85% in 2023 compared to 89% in 2022. Active hiring from minority groups has held relatively stable and veteran hires are up slightly in 2023. Forty percent (40%) of organizations report hiring veterans' spouses.

Organizations could potentially find it easier to identify and hire diverse employees if they changed certain prerequisites. Seventy-one (71%) of respondents say they require four-year degrees, instead of considering qualifications from nontraditional backgrounds, such as boot camps, professional certifications, and self-learning. If organizations changed their minimum requirements this, combined with apprenticeships or train-to-hire programs—which 80% of respondents already offer—could help grow their talent pool.

[1] This is true for all groups except veterans' spouses, which was not previously tracked.

Active Hiring Varies

Active hiring of women is slightly lower in 2023 than in the previous year, while the hiring of veterans is up slightly, though down from 2021.



DIGGING DEEPER

Targeted Recruitment Programs Tend to Yield More Hires

More organizations have programs targeting women

Women continue to be the top focus of structured diversity recruiting initiatives.

- 73% of IT decision makers have structured recruiting initiatives targeting women.
- This proportion has held relatively stable over the past few years—73% in 2022 and 75% in 2021.

Minority candidates remain a significant target

The targeted recruitment of minority candidates has been stable since 2021.

- 60% of organizations report structured recruiting initiatives for minority candidates.
- This is nearly unchanged from 59% in prior years.

Veterans and their spouses continue to be underutilized

Veterans often have a strong foundation of security skills accumulated from working in highly disciplined and secure contexts. These skills could translate to cybersecurity.

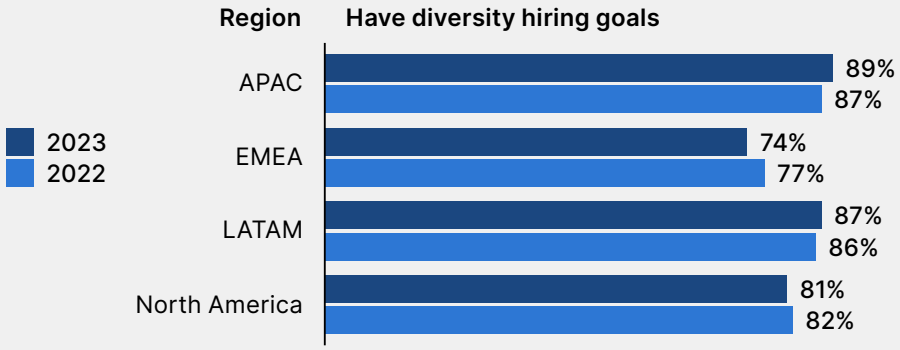
- Fewer than half (45%) of respondents have recruitment initiatives targeting veterans. This is up slightly from 2022 (43%) but down from 2021 (51%).
- Even fewer organizations (36%) have structured programs targeting veterans' spouses.

More organizations (73%) have structured programs targeting women and more (85%) report actively hiring women, suggesting a correlation between programs and outcomes.

Regional Highlights

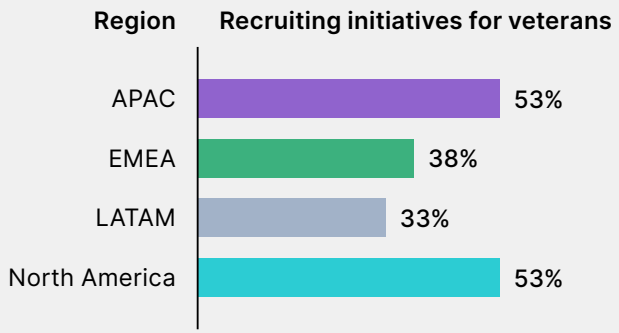
APAC leads in diversity hiring goals

Companies in APAC continue to be most likely to have diversity hiring goals for the next two to three years. Companies in EMEA remain least likely.



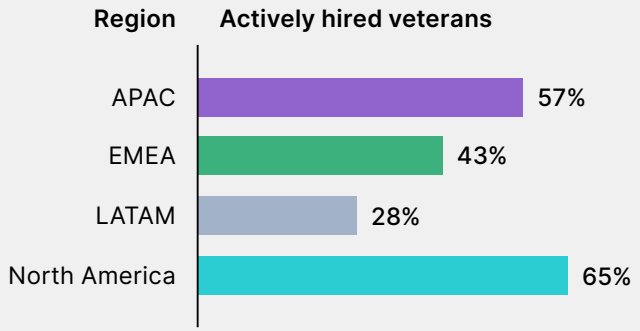
Veterans are most sought after in North America and APAC

Companies in North America and APAC are most likely to have structured recruiting initiatives for veterans.



Veterans are hired more often in North America and APAC

This goes hand-in-hand with the prevalence of recruiting initiatives.



Conclusion

In 2023, cybersecurity was clearly an enterprise-wide issue for many organizations, with implications from the board level to the front lines. The results of this survey show that participants are embracing a threefold response to cybersecurity that combines training, awareness, and technology. This response provides a comprehensive strategy for facing current and emerging threats.

Investing in training and certification for dedicated IT and security staff and raising awareness of cybersecurity best practices among all employees go a long way toward strengthening an organization's security posture. This will be especially important as new threats develop and technologies, such as AI, make attacks more precise and sophisticated on a larger scale.

Better trained, more knowledgeable, and highly skilled IT/security professionals are essential to protecting executives and board members from being penalized for breaches. A security-aware staff provides critical frontline defenses. The more that corporate leaders are held accountable, the more cybersecurity will be seen as "everyone's responsibility".

Investing in certifications, ensuring certifications remain current, and recruiting from diverse and nontraditional talent pools will help close skills gaps. Organizations may be restricting their access to skilled, ready-to-develop cybersecurity talent by being too rigid in their requirement of foundational credentials. By expanding their recruitment pools to include candidates whose credentials fall outside of the traditional four-year degrees or training and development backgrounds, organizations could unlock new possibilities, especially if they are also willing to pay for certifications and training.

At the end of the day—and as most survey respondents seem to recognize—capable human resources need the right cybersecurity tools and skill sets to combat threats and contend with the speed and volume of today's attacks. Rounding out skills, knowledge, and certifications with advanced technologies, remains key.

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 all populations. Collaboration with high-profile, well-respected organizations from both the public and private sectors, including 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, Fortinet Training Institute and FortiGuard Labs.

FORTINET
Training Institute

www.fortinet.com

June 20, 2024 11:43 am