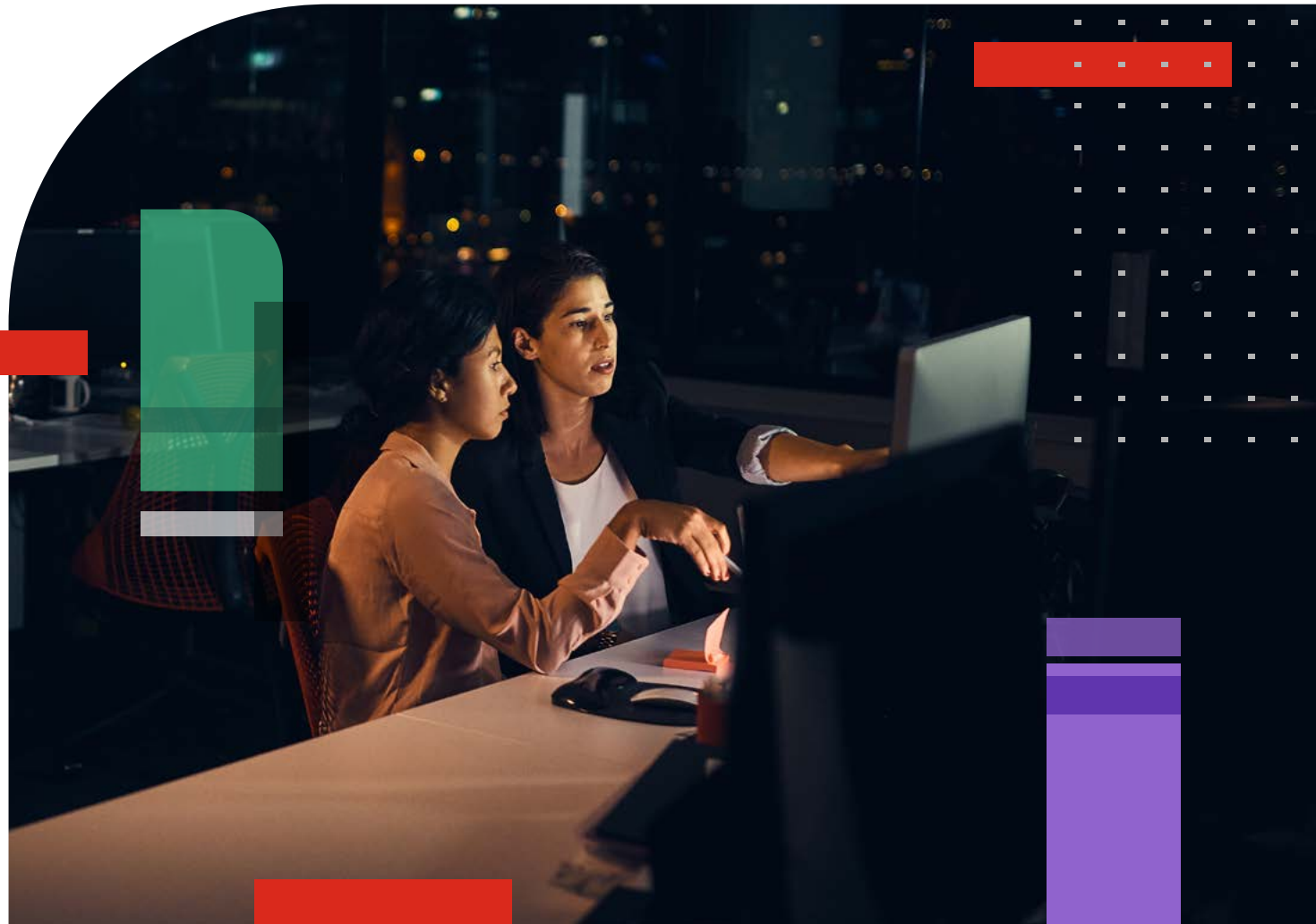
FORTINET
Training Institute

2023 Security Awareness and Training

Global Research Brief



Contents

03 Methodology

04 Introduction: Focusing on the Human Element of Cybersecurity

05 Executive Summary

07 Employees Can Be Your Weakest Point or Your Most Powerful Defense

09 Employees Lack Cybersecurity Awareness, Even with Current Training

11 Cybersecurity Is a Growing Priority for Boards of Directors

13 Conclusion

14 About Fortinet

Methodology

The findings of this report are based on an online interview and an email survey of 1,855 IT and cybersecurity decision makers conducted by Sapio Research in November 2022. Responses were collected 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 – **25%**
500-999 employees – **23%**
1,000-2,499 employees – **23%**
2,500-4,999 employees – **15%**
5,000+ employees – **14%**

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
21% Technology
16% Manufacturing
13% Financial Services

INTRODUCTION

Focusing on the Human Element of Cybersecurity

As cyberattacks intensify, more and more organizations recognize the need to have a strong security culture for all employees. This cyber-aware workforce is a necessary addition to a skilled and knowledgeable security team and the use of advanced cybersecurity solutions. Employees who know how to practice good cyber hygiene are increasingly seen as a crucial line of defense.

Bolstering cyber defenses will be important in 2023, as organizations face an ever-evolving threat landscape. Fortinet's FortiGuard Labs predicts "explosive" growth in Cybercrime-as-a-Service (CaaS); use of machine learning to launder money; cybercrime exploits in augmented, virtual, and mixed reality environments; and data-erasing wiper malware.

This prediction underscores the critical nature of employee cyber-security awareness and training—which is why Fortinet is giving these topics their own focus in this *2023 Security Awareness and Training Global Research Brief*. The following pages highlight some of the top concerns and actions being taken by leaders around the world, based on survey findings from the annual Fortinet Cybersecurity Skills Gap Global Research Report.

Executive Summary

Employees can be your weakest point or your most powerful defense.

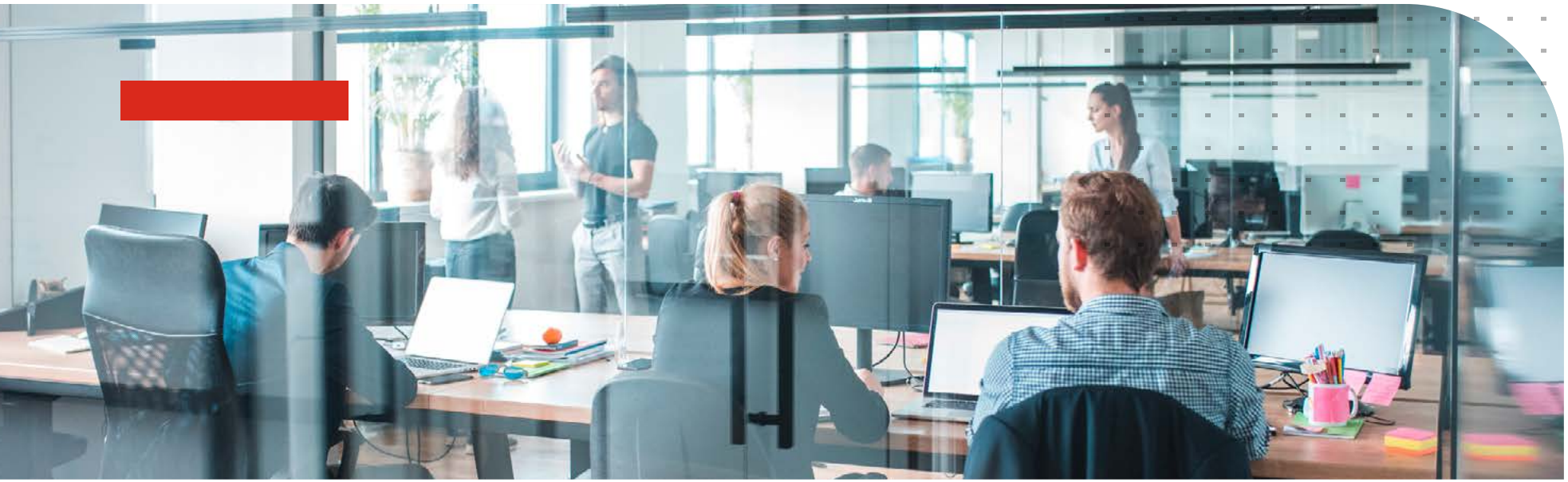
81% of surveyed organizations faced **malware**, **phishing**, **and password attacks** last year—many of which directly targeted users.

Employees lack cybersecurity awareness even with current training.

56% of leaders believe their **employees lack knowledge** when it comes to cybersecurity awareness.

Cybersecurity is a growing priority for corporate boards.

93% of boards of directors are questioning their **organizations' cyber defenses**.



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

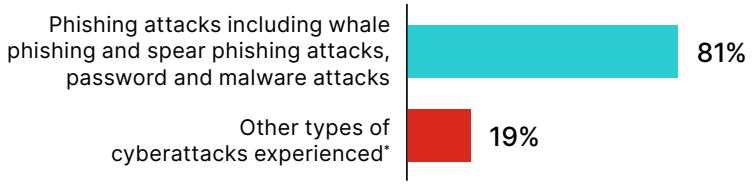
Employees Can Be Your Weakest Point or Your Most Powerful Defense

Nearly all organizations surveyed had experienced at least one cybersecurity breach in the past 12 months. Almost a third had experienced five or more. A common characteristic of many of the cyberattacks that occurred in 2022, was that they targeted users directly, such as phishing schemes, or capitalized on weak cyber hygiene to compromise passwords and credentials.

While malware was the most common type of attack used in the past 12 months, phishing might be the most insidious, often housing other kinds of attacks in the guise of friendly emails, text messages, and web links. Other reported types of attacks targeting employees included password attacks, spear phishing, and whale phishing (also referred to as whaling).

With the cost of breaches exceeding $1 million for close to half of responding organizations, equipping employees to recognize, avoid, and report cyber threats seems key.

Most common attacks reported by organizations



*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.

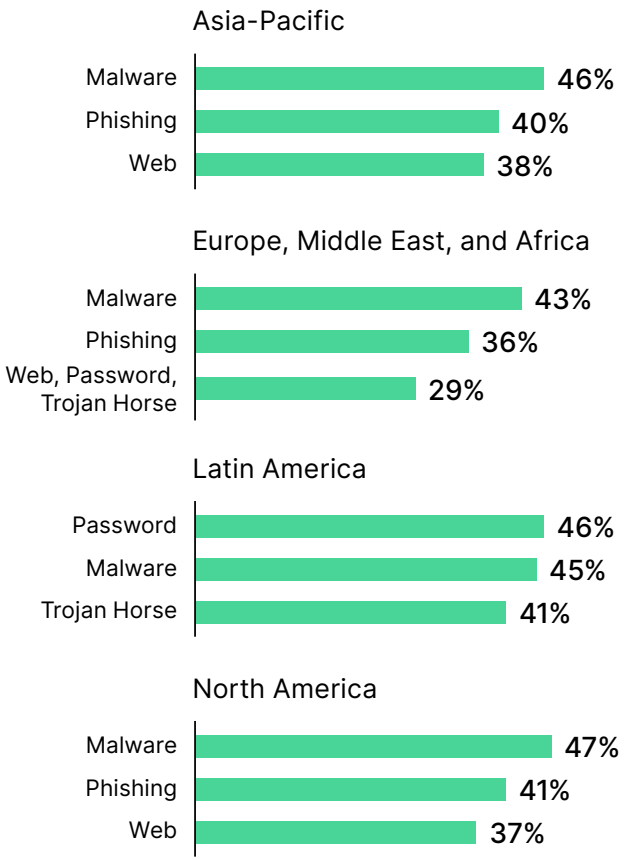
Digging Deeper

- **84%** of organizations surveyed experienced **at least one cybersecurity breach** in the past 12 months, up from 80% the year before.
- **29% had five or more**, up from 19%.
- And **7% had more than 9**, up from just 3%.
- **65%** of leaders expect an **average 20% increase in cyberattacks** over the next 12 months.

Regional Highlights

The most common attacks vary by region.

Organizations in each world region have a slightly different attack profile.



Different industries face different volumes of malware attacks.

FortiGuard Labs 2022 research shows attack volumes vary by industry and region. For this research, FortiGuard Labs separated Europe and Middle East from Africa.

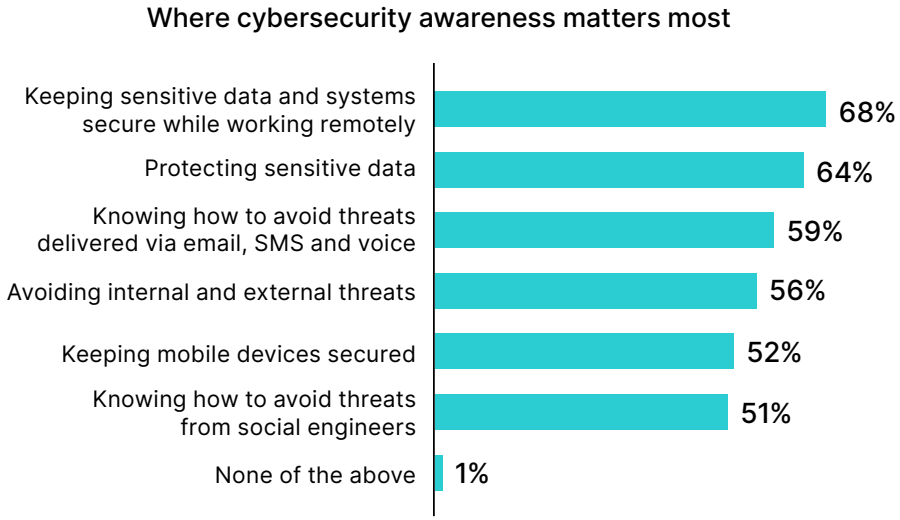
Industry		
Financial services		
	Regional high	Europe and Middle East (**63.1%**)
	Regional low	Latin America (**1.8%**)
Healthcare		
	Regional high	Asia Pacific (**62%**)
	Regional low	Africa (**2.6%**)
Managed security services		
	Regional high	Europe and Middle East (**46.6%**)
	Regional low	Asia Pacific (**1.8%**)
Retail and hospitality		
	Regional high	Asia Pacific (**38.8%**)
	Regional low	Africa (**8.6%**)
Oil and gas		
	Regional high	Europe and Middle East (**49.1%**)
	Regional low	Asia Pacific (**18.9%**)

Employees Lack Cybersecurity Awareness, Even with Current Training

Eighty-five percent of leaders say their organization has a security awareness and training program, yet more than half believe their employees still lack cybersecurity knowledge.

This disconnect seems to suggest the training programs in place are not as effective as they could be, that cyber hygiene practices are applied inconsistently, or that training is not reinforced sufficiently, which analysts consider to be key to building an effective cybersecurity culture.

Leaders say that protecting sensitive data and systems when working remotely is the most important aspect of cybersecurity awareness for employees, followed closely by protecting sensitive data in general.



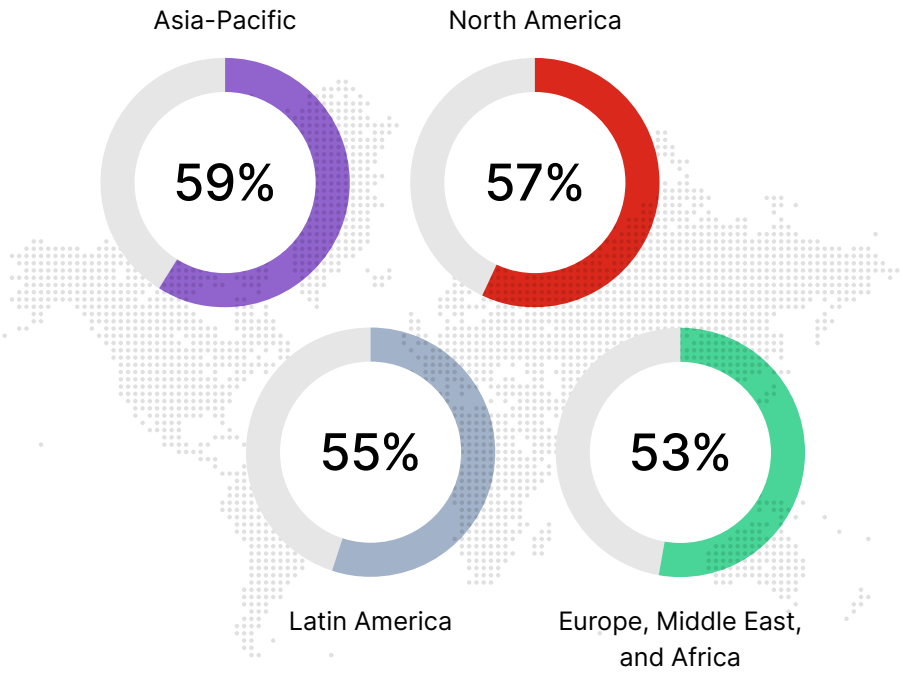
Digging Deeper

- **56%** of leaders believe their **employees lack knowledge** when it comes to cybersecurity awareness, up from 52% in 2021. That's despite **85%** having a **security awareness and training program** in place.
- **73%** of organizations **without a training program** are looking for one, an increase from 66% in 2021.
- **93%** of leaders believe greater employee cybersecurity awareness would help **reduce cyberattacks**.
- **59%** of leaders say it's reasonable for employees to **spend one to three hours per year in cybersecurity training**.
- **68%** of leaders say it's most important for employees to know **how to keep sensitive data and systems secure while working remotely**.

Regional Highlights

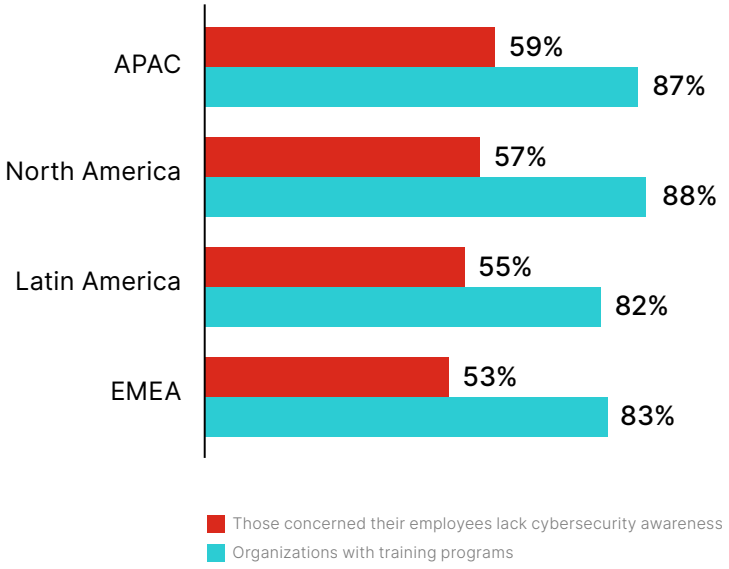
Concerns about cybersecurity awareness are similar across all regions.

Concern is slightly higher in the Asia-Pacific region and lowest in Europe, the Middle East, and Africa.



Training is common, yet gaps persist.

It is interesting to see, while more than half of leaders in all regions believe cybersecurity awareness is lacking, the majority of companies offer training programs.



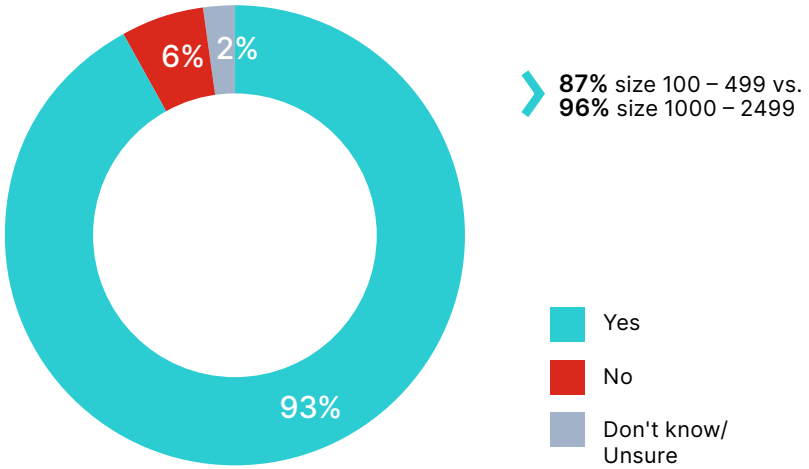
Cybersecurity Is a Growing Priority for Boards of Directors

A resounding 93% of leaders with a direct line to a board of directors say their boards are asking about the organizations' cyber defenses.

It is reasonable to take this as a sign that boards are serious about their responsibilities to manage corporate risk and protect the brand, and that they are aware of the increase in attacks and breaches.

Since many attacks target users, it seems likely that boards see—or will soon see—that employee cybersecurity awareness is a critical part of the "defense equation". Ninety-three percent of leaders believe that increased employee cybersecurity awareness would help decrease the occurrence of cyberattacks.

Boards of directors are asking about cybersecurity



*Asked only to those organizations whose boards of directors are asking about how their organizations are protecting themselves against the increase in cyberattacks.

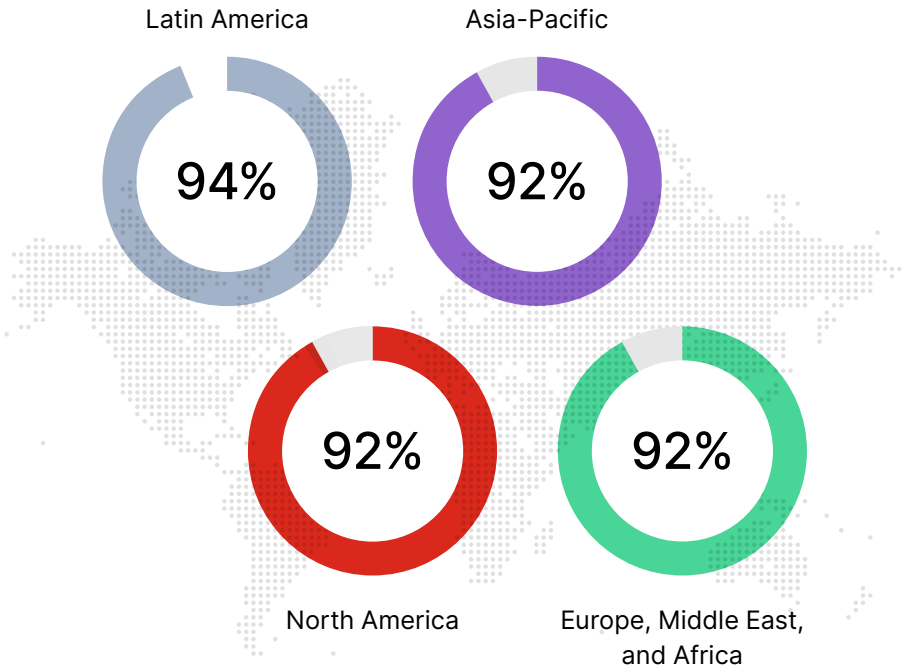
Digging Deeper

- **Board interest in cybersecurity is increasing—up to 93%** in this current survey from 88% as reported in *Fortinet's 2022 Cybersecurity Skills Gap Report*.
- **Board interest in security is largely consistent across industries**, though somewhat higher in financial services, healthcare, and telecommunications (94–95%) than in education, media, and entertainment (88%).

Regional Highlights

Boards in all regions are asking about cybersecurity.

Survey findings show similar levels of concern among boards worldwide.



*Asked only to those organizations whose boards of directors are asking about how their organizations are protecting themselves against the increase in cyberattacks.

Conclusion

With 84% of leaders reporting at least one cyber breach in the last 12 months—and nearly half citing a total cost of breaches above $1 million—it is vital for organizations to keep strengthening their cyber defenses. Organizations need to develop an all-encompassing approach to cybersecurity, one that includes sophisticated, automated solutions; expert teams; and—as these survey results show—an effective security awareness and training program.

Employees are an essential line of defense.

Since many of the most common types of cyberattacks—phishing schemes, certain forms of malware, and password attacks—target users directly, low employee cybersecurity awareness likely weakens an organization's overall security posture significantly. Conversely, effective cybersecurity awareness and training programs can improve security posture, adding extra layers of protection to an organization. Leaders seem to recognize this, with 93% responding that they believe greater employee training and awareness would help decrease the frequency of cyberattacks.

Training needs reinforcement.

Cybersecurity awareness and training programs are widely recognized methods of reinforcing employee cyber culture. Not surprisingly, the majority of organizations have programs in place. Yet over half of all leaders surveyed are still concerned that their employees lack cybersecurity awareness. A critical evaluation of security awareness and training programs may reveal opportunities to address the human element of cybersecurity more effectively, thereby reducing the overall risk. Taking steps to ensure programs sufficiently cover a broad range of topics in a practical way, and to ensure that learning is reinforced with reminders and checks, should help improve training outcomes.

Boards of directors are focused on cybersecurity.

With a solid training program, organizations can raise employees cyber-risk awareness and empower them to defend the organization, laying the foundation for a strong and ready cybersecurity culture. This may resonate with corporate boards of directors who, as this year's survey results show, are increasingly concerned about cybersecurity, and will likely focus on the human element going forward—recognizing that it plays an essential role in protecting business interests and the reputation of the corporate brand.

Organizations know that they need advanced cybersecurity solutions, and that technology certifications build the cybersecurity capabilities of their IT teams. To date, employee awareness may not have received the full attention it deserves, yet it could prove pivotal in the fight against cyberattacks in the years to come.

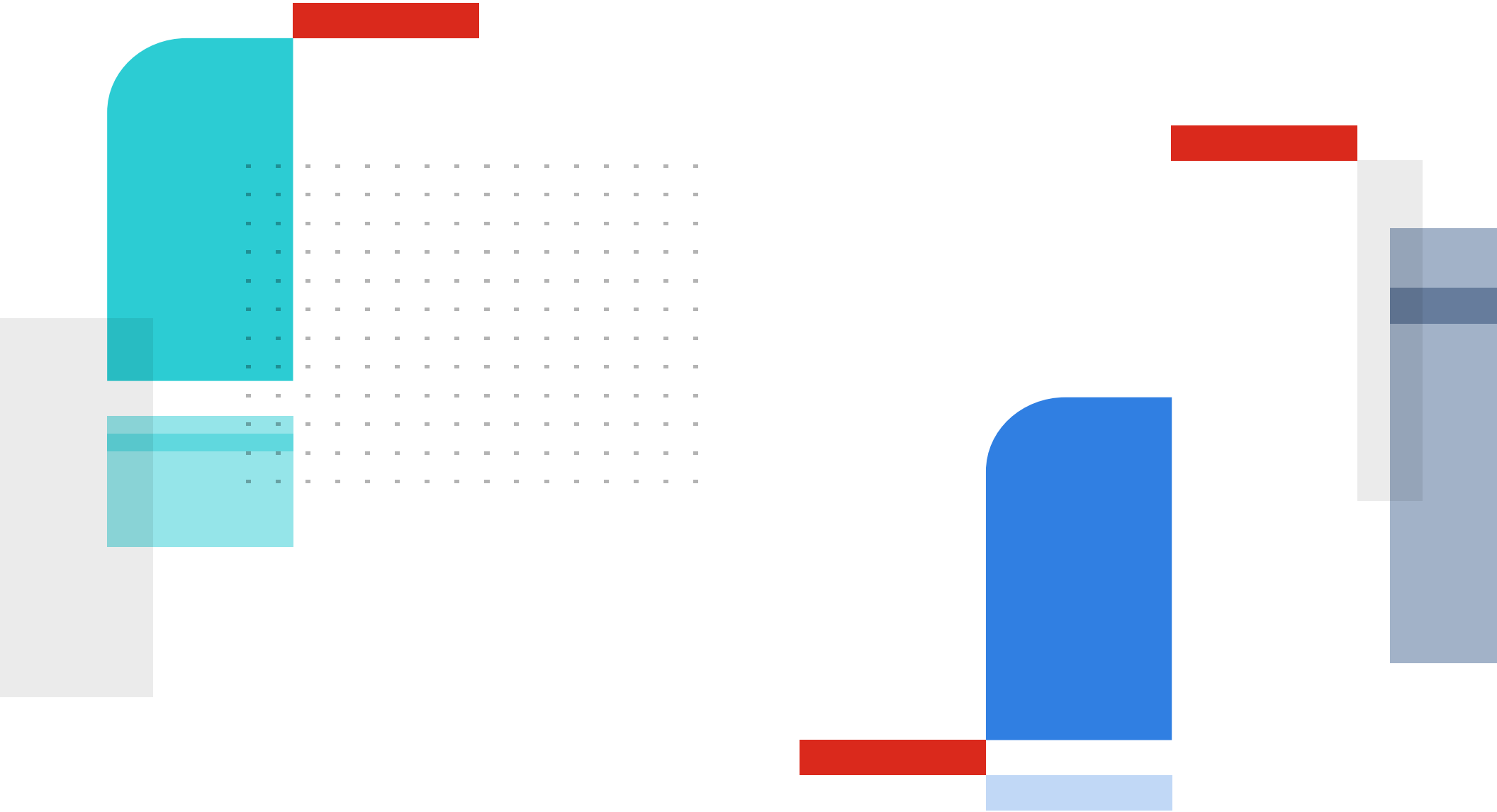
You can find a broader and more detailed view of organizations' cybersecurity needs and challenges in Fortinet's 2023 Cybersecurity Skills Gap Global Research Report.

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 rated protection and actionable threat intelligence. Learn more at https://www.fortinet.com, the Fortinet Blog, and FortiGuard Labs.



FORTINET

Training Institute

www.fortinet.com

May 2023