FORTINET
Training Institute

2024 Security Awareness and Training

Global Research Report

Methodology

The findings in this report are based on responses obtained from online interviews with 1,850 executive-level and management-level professionals at organizations that have security awareness and training in place. The interviews were conducted by Sapio Research in May and June 2024. Responses were obtained from individuals 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 **22%**
500-999 employees **21%**
1,000-2,499 employees **21%**
2,500-4,999 employees **18%**
5,000+ employees **18%**

Gender

67% of respondents were male
33% of respondents were female

Total respondents: 1,850

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

Role Type

7% held Owner positions
26% held C-Level Executive positions
7% held Vice President positions
18% held Head of Department positions
17% held Director positions
25% held Manager positions

Top Three Business Sectors:

Manufacturing **17%**
Financial Services **13%**
Professional Services and Technology **11%**

Executive Summary

Leaders recognize that people are a crucial first line of defense against cyberattacks. It's why many executives are concerned about their employees' level of cyber risk awareness—and even more worried about new AI-generated threats, which are already proving harder to spot and block than "traditional" cyberattacks.

Organizations are bracing for AI attacks

- **62%** of leaders expect employees to fall victim to attacks in which cybercriminals use AI.
- **95%** are using, implementing, or researching AI solutions to prevent cyberattacks.
- **80%** report that attitudes towards security awareness training have improved due to the use of AI by bad actors.
- Despite concerns about AI risks, **31%** of organizations do not manage or monitor how employees use AI applications.

Leaders need cyber-aware employees

- **67%** worry their employees lack general security awareness, up from **56%** in 2023.
- Core drivers for adopting a security awareness and training program:
  - Past security breach or threat of a security breach (**52%**)
  - Corporate sponsorship (**21%**)
  - Compliance and regulatory requirements (**13%**)
- **94%** are interested in implementing stricter cybersecurity policies for high-risk users.

Training is key to raising security awareness

- **97%** of decision-makers say more training and awareness would help reduce cyberattacks, up slightly from **93%** in 2023.
- **89%** report improvements to their organization's security posture after implementing security awareness and training.
- The most important security awareness and training topics are:
  - Data security (**48%**)
  - Data privacy (**41%**)

  which is consistent with 2023 findings.

Training needs to be engaging and intentional

- On average, **81%** of organizations felt that three hours of training a year was needed to raise cyber awareness.
- **75%** of security awareness campaigns are planned in advance, and delivered on a monthly (**34%**) or quarterly (**47%**) basis.
- **86%** of leaders are satisfied with their current security awareness and training solutions. Of those who reported being dissatisfied, **41%** said their programs lacked engaging content.

A new and expanded look at awareness and training

The topic of security awareness and training was previously part of Fortinet's Cybersecurity Skills Gap Global Research Report. The growing importance of human cybersecurity factors prompted us to issue a standalone survey in 2024, digging deeper into the topic.

While many questions were asked for the first time this year and have no baseline for comparison, we included select year-over-year comparisons against data from our 2023 Security Awareness and Training Global Research Brief.

INTRODUCTION

No Weak Links Allowed

Employee security awareness and training have become high-profile concerns for leaders who want to reinforce their organizations' cyber defenses by every means possible.

This report presents survey findings related to the state of cyber awareness and training worldwide:

- Where leaders are focusing
- How organizations are handling the urgency
- What keeps decision-makers up at night

As AI continues to permeate every aspect of our lives, business leaders are increasingly on edge about AI-related threats, ranging from deepfake schemes and next-level phishing attacks, as well as employee use of large language models, coding companions, image generators, and other AI tools. Despite those anxieties, nearly a third of organizations don't manage or monitor employees' use of AI applications, suggesting a gap in corporate policies for some.

Today, cybercriminals are using AI to make phishing schemes harder to detect. Because phishing targets individual users directly, organizations are overwhelmingly focused on teaching employees how not to fall victim to these attacks. Nearly all respondents say phishing prevention is a component of their training programs and plans. Other top priorities for awareness and training include data security and data privacy.

This year's survey also sheds light on how organizations tend to approach security awareness and training. It shows that most are highly intentional, pre-planning training topics and offering content installments at regular intervals throughout the year. Most leaders support these efforts and believe more training and awareness is needed.

As noted in our 2024 Cybersecurity Skills Gap Global Research Report, organizations view awareness and training as part of a three-pronged approach to mitigating cyber risk, which also includes hiring and retaining skilled IT security staff and implementing effective cybersecurity solutions.

In 2024, we are seeing the elevated role that policy is playing, or can play, in cybersecurity, whether that relates to managing employee behavior online or the rising popularity of cyber insurance. These findings suggest that leaders understand that cybersecurity is rooted in organizational culture—and that policy, awareness, and training all contribute to it.

62% of organizations expect employees to fall victim to more cyberattacks in the future due to attackers' malicious use of AI.

Organizations Are Bracing for AI-Driven Attacks

Corporate users and cybercriminals alike have embraced AI to speed up, scale, and simplify their work. Business leaders are aware of the threats posed by internal misuse of AI tools and AI-enabled external attacks, and they are eager to do something about them.

The majority (62%) of survey respondents say they expect employees to fall victim to more attacks as bad actors increase their use of AI. Nearly all (96%) are researching, implementing, or already have incident response plans related to combatting external AI-related threats, which today includes hard-to-detect audio and video deepfakes designed to trigger scam transactions as well as highly targeted phishing schemes. New types of AI-enabled attacks continue to emerge.

Most respondents (80%) say enterprise-wide knowledge of AI attacks has made their organizations more open to security awareness and training. The majority (95%) also report having or developing security policies to manage internal risks related to the use of AI tools.

These policies tend to revolve around information leakage, including private or proprietary data appearing in public-facing AI outputs, inadvertently disclosing secrets, or de-anonymizing personally identifying information.

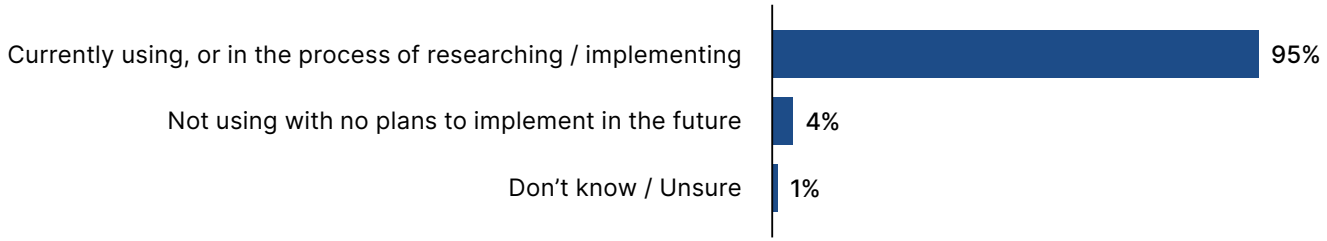
Leaks can happen all too easily—for instance, when an employee copies corporate content into a large language model (LLM) for editing or composes a detailed prompt to answer a question. Such inputs could be used to train AI models or be queried by outside parties, causing private information to be made public.

While creating policies to govern corporate AI use is important, in nearly a third (31%) of organizations, these policies aren't supplemented with active management or monitoring of employees' AI use, leaving potential vulnerabilities unchecked.

Organizations are using AI for cybersecurity

Almost all survey respondents (95%) say their organization is currently using AI-driven security solutions to prevent cybersecurity attacks or is in the process of researching or implementing such tools.

Percentage of organizations using or adopting AI for cybersecurity



DIGGING DEEPER

Training, Awareness, and Confidence Go Hand-In-Hand

Stronger support for awareness and training boosts AI confidence

Organizations with more internal support for awareness and training tend to be more confident about employees' ability to handle AI-related threats:

- 60% of respondents with strong support for training said they thought employees would fall for more attacks due to AI.
- 66% of organizations with moderate support for training are concerned more employees are at risk.
- 70% of organizations with little or no support for training worry more employees will fall for AI-powered attacks.

Most organizations do not yet manage employee AI use

The majority (53%) of respondents say their organization is either still implementing or does not have processes for managing and monitoring employee use of AI tools:

- 31% have no measures in place and another 10% don't know or aren't sure.
- 22% say they're working on it but are not finished implementing processes for monitoring and management.

Of those with measures in place, 21% sanction specific AI applications for internal use and 16% impose technical controls.

Concerns about AI threats vary by industry

Respondents in certain industries and sectors are much more concerned about AI causing employees to fall for threats:

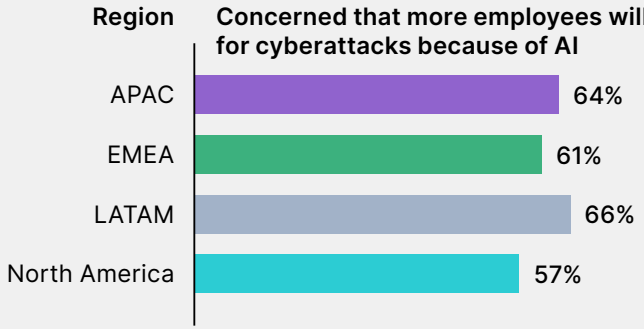
- 70% of media and entertainment companies expect employees to fall for more attacks because of attackers' use of AI.
- State and local governments are a close second at 68%.
- Energy and utility companies (59%), healthcare (57%), and retail (56%)

Less than a quarter of organizations (**21%**) sanction specific AI applications for employee use.

Regional Highlights

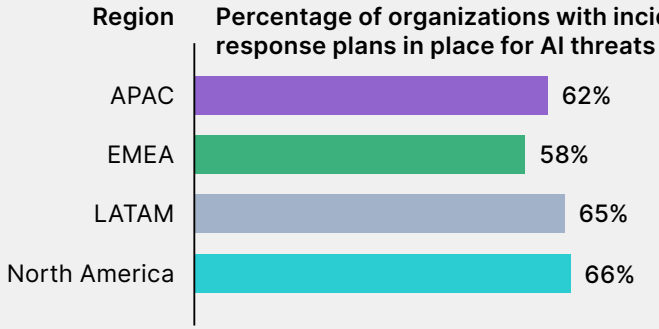
AI concerns are highest in Latin America

Organizations in Latin America (LATAM) are most likely to think employees will increasingly fall for cyberattacks because of attackers' use of AI.



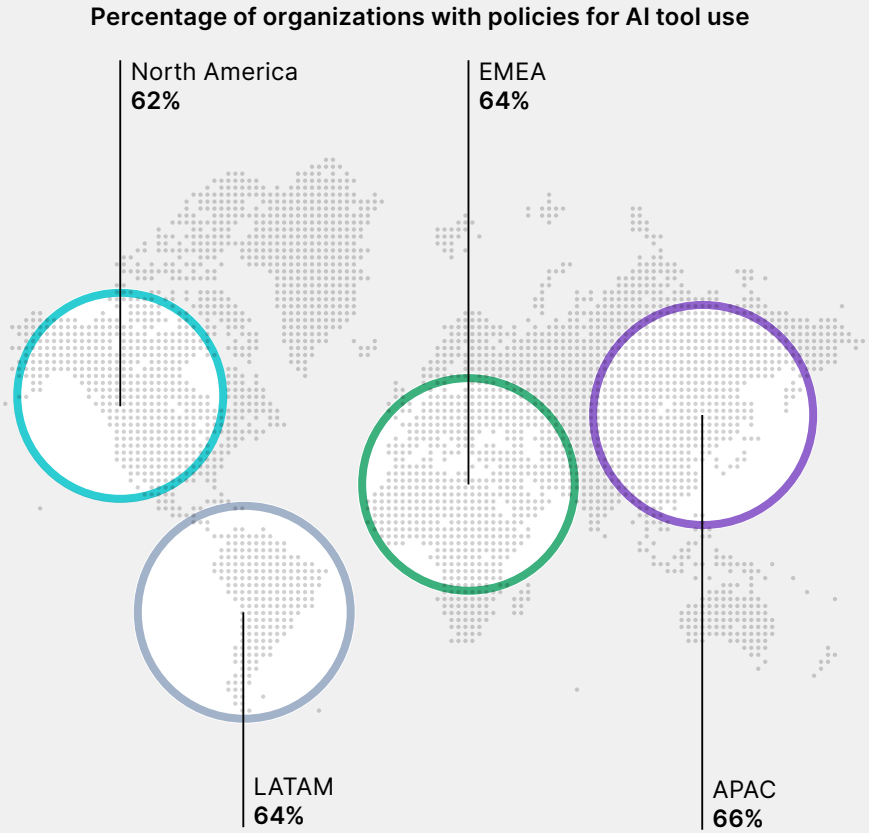
Incident response plans are least likely in Europe, Middle East, and Africa

Fewer companies in Europe, Middle East, and Africa (EMEA) have incident response plans for AI-related threats, while those in North America are most likely to have such plans.



Most organizations have security policies to govern AI tools

Respondents in all regions are almost equally likely to have corporate policies to govern the use of AI tools.



The majority (**67%**) of decision-makers think their employees lack security awareness.

Leaders Need Cyber-Aware Employees

Whether threats are related to new technologies like AI or are more conventional cyberattacks, decision-makers remain concerned that employees may not have the degree of security awareness they need to protect themselves and their organizations.

Just over two-thirds (67%) of respondents say they think their employees lack security awareness and knowledge, a notable increase from 56% in 2023. This correlates with the Fortinet 2024 Cybersecurity Skills Gap Global Research Report findings where a lack of security awareness is considered to be one of the top three causes of breaches.

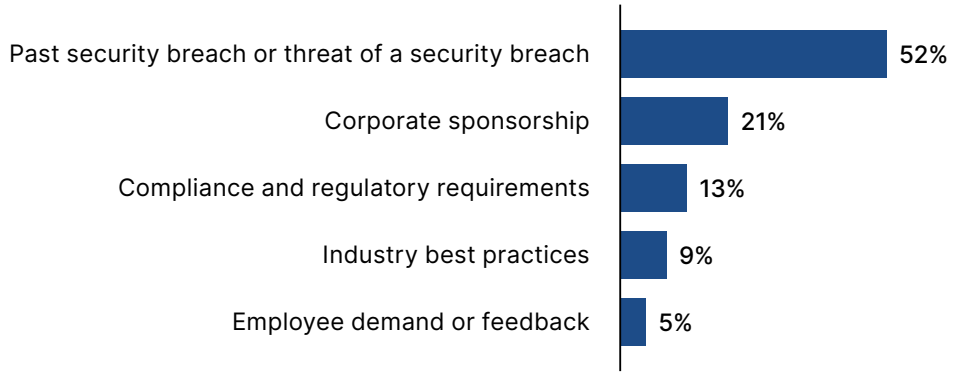
Given these findings, it's not surprising that support for security awareness and training is generally high. Almost all decision-makers (96%) say their leadership team supports implementing training to raise employees' cybersecurity awareness. IT leaders (57%) and security leaders (54%) are generally the champions of security awareness and training, with CEOs / Heads of Organizations a distant third at 40%.

At the same time, recognizing the gravity of the situation, 94% of leaders also say they would be interested in applying stricter cybersecurity policies to users who exhibit high-risk behavior. Such users might be identified through methods such as company-run phishing campaigns that reveal which employees are most likely to fall for AI-powered attacks.

Awareness of threats drives training adoption

Most organizations are motivated to introduce security awareness and training based on their experience being breached or knowledge of threats in their industry or sector.

Organizations' reasons for adopting security awareness and training



DIGGING DEEPER

Mitigating Cyber Risk Is a Growing Corporate Priority

Awareness, training, and cybersecurity insurance have similar drivers

Organizations invest in cybersecurity insurance because:

- It's a corporate priority (51%).
- More breaches are occurring in general (46%).
- More breaches are occurring in their industry (42%).

This aligns with the top reasons for implementing security awareness and training: threat of breaches or actual breaches (52%) and corporate sponsorship (21%).

Cybersecurity insurance is growing in popularity

Most organizations (95%) have prioritized cybersecurity insurance.

- 77% have cybersecurity insurance.
- 18% are looking to obtain it in the next 12 months .

Organizations with 1,000 to 4,999 employees are most likely to have cybersecurity insurance:

- 1,000 to 2,499 employees (81%)
- 2,500 to 4,999 employees (81%)
- 5,000+ employees (77%)
- 100 to 999 employees (74%)

Resources are key to getting security awareness and training off the ground

When asked what kept organizations from implementing a security awareness and training program in the past, respondents said:

- Limited human resources (31%)
- Other corporate priorities—awareness and training ranked lower (26%)
- Limited budget (22%)
- Did not feel they required a program (18%)

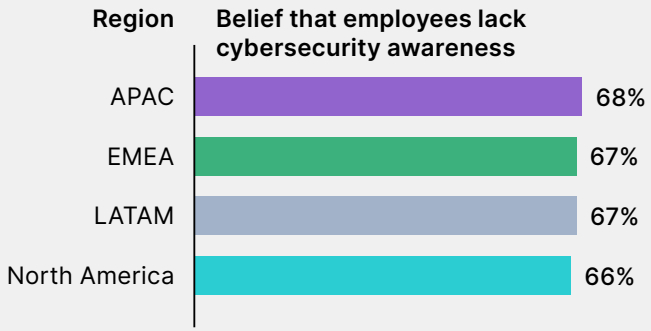
Large organizations (5,000+ employees) tend to have more established security awareness and training programs, with an average duration of 12 years compared to seven for those with 100 to 999 employees.

A third (**31%**) of respondents say human resource constraints kept them from rolling out security awareness and training programs.

Regional Highlights

Concerns about insufficient security awareness and training are widespread

Organizations in all regions have roughly equivalent concerns that employees lack cybersecurity awareness.

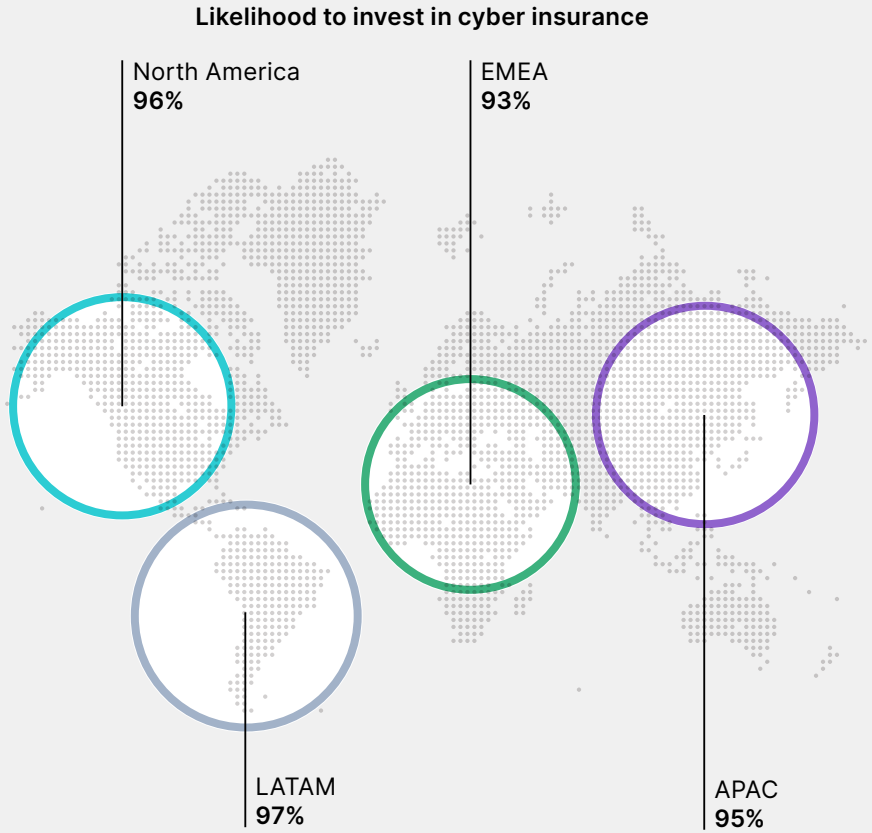


Support for security awareness and training is also prevalent

Leadership teams in all regions are in favor of offering security awareness and training for employees.

Organizations in LATAM are most likely to invest in cyber insurance

More respondents in LATAM say they have or are planning to acquire cyber insurance than in any other region.



97% of decision-makers believe increased security awareness would help reduce cyberattacks.

Training Is Key to Raising Security Awareness

Decision-makers agree that greater awareness would improve their organization's cybersecurity posture and that internal campaigns and training are effective ways to further manage risk.

According to this year's survey, 97% of leaders think increased employee awareness would strengthen cybersecurity. This is up slightly from 93% in the 2023 Security Awareness and Training Service Global Research Brief.

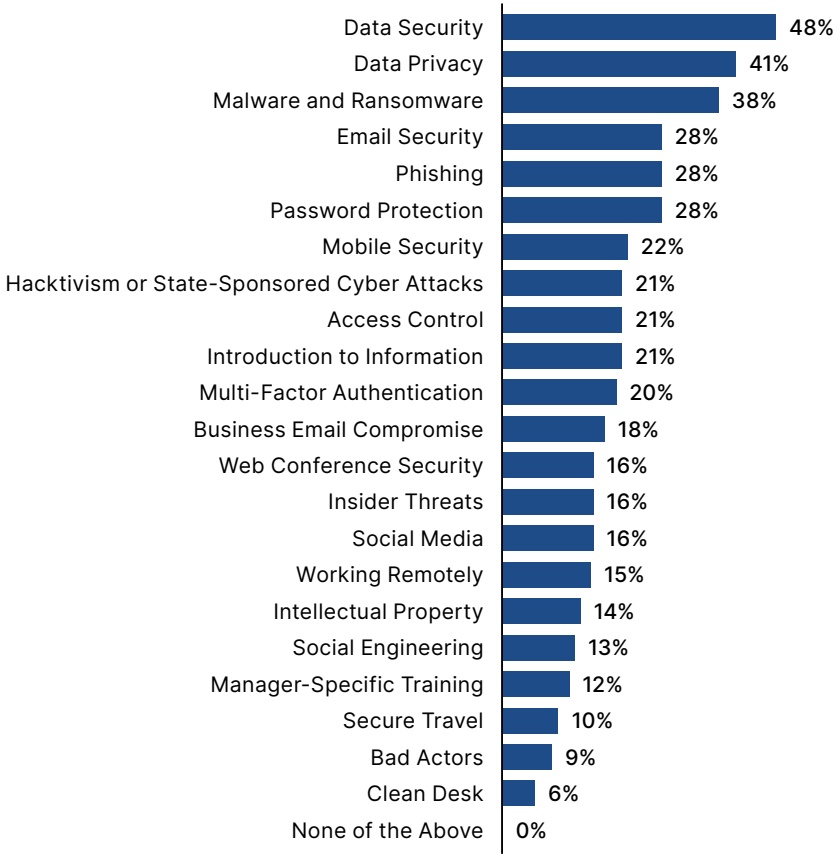
Respondents seem to have a good reason for holding this view. An overwhelming majority (89%) say their organization saw at least some improvement in its security posture after security awareness and training was implemented—and not a single respondent claimed to see no improvement. Most (86%) add that their employees view security awareness and training positively, with 55% saying "very positively."

When it comes to training priorities, data security and data privacy top the list at 48% and 41%, respectively. Awareness of phishing attacks is also key: Almost all respondents (98%) say their programs include or will include phishing-related campaigns. This aligns with our 2024 Cybersecurity Skills Gap Global Research Report finding that phishing attacks are the second most common form of attack encountered by organizations.

Keeping Data Safe Is Most Important

What leaders want most is security awareness and training that teaches their employees how to keep data secure and private. This echoes the responses from 2023, which indicated that employees knowing how to keep sensitive data and systems secure when working remotely was a top priority.

2024 security awareness and training priorities



DIGGING DEEPER

Training Requires Management and Support

All organizations benefit from security awareness and training

Regardless of size, the majority of organizations report at least some improvement to their security posture after implementing security awareness and training:

- 100 to 999 employees (88%)
- 1,000 to 2,499 employees (92%)
- 2,500 to 4,999 employees (91%)
- 5,000+ employees (88%)

As a potential indication of those improvements, more than two thirds (69%) of leaders rate their average employee's ability to identify a spoofed email as good or very good.

Leadership support produces better results

When leaders strongly back security awareness and training, organizations are more likely to see some or significant improvement after implementation:

- 96% with 'extensive' leadership support report some or significant improvement post implementation.
- With 'a certain extent' of leadership support, that drops to 79%.
- Only 47% of organizations with little or no leadership support report some or significant benefits after implementation.

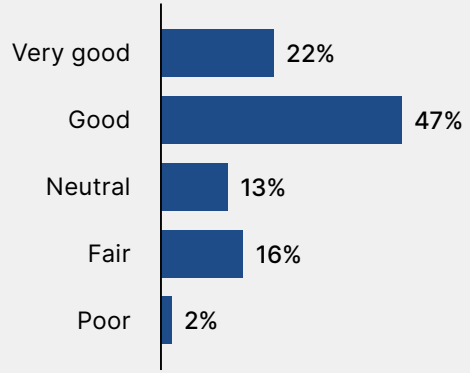
Employees balance multiple training commitments

Even though 86% of respondents say their employees view security awareness and training positively, more than half (58%) think staff would prioritize other training. Managing 'training fatigue' is a reality for organizations.

The other types of mandatory training most commonly seen are:

- Health and safety (71%)
- Compliance (66%)
- Customer service (61%)
- Product or service (61%)

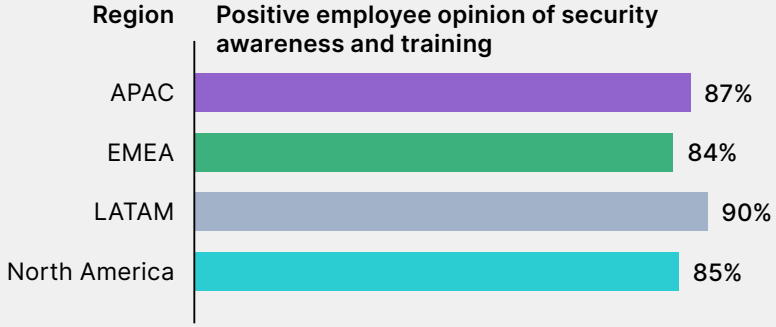
More than two thirds (69%) would rate their organization's average user's ability to identify a spoofed email as good or very good



Regional Highlights

Employees in all regions view security awareness and training positively

LATAM posts the highest result at 90% and EMEA the lowest at 84%.

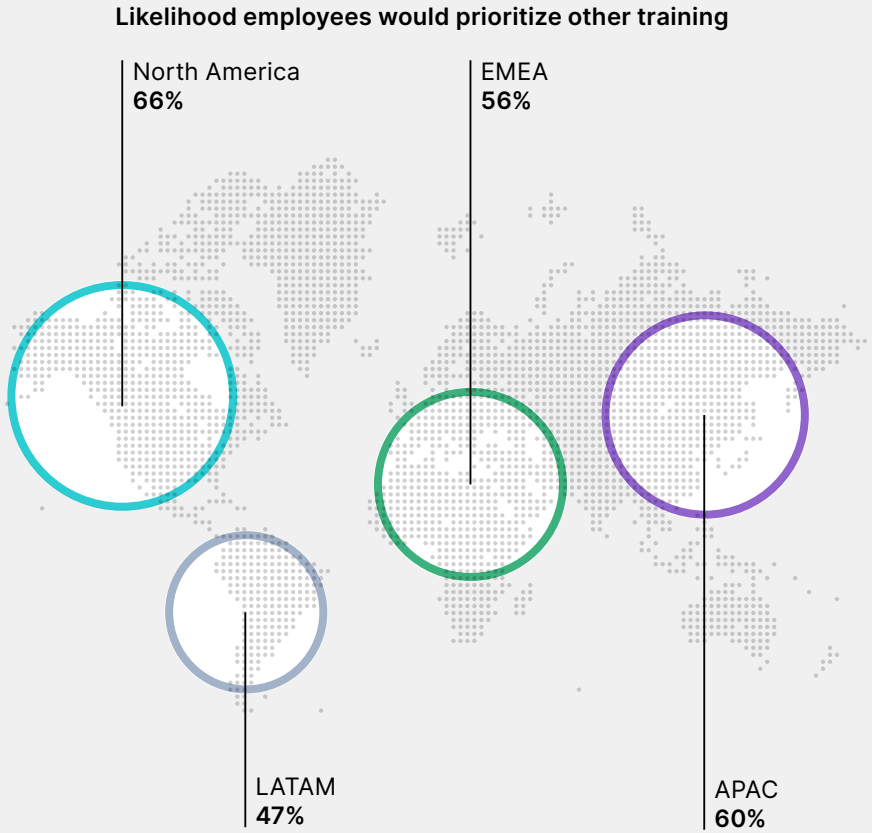


Not all regions experience gains equally

Respondents in EMEA were least likely to see cybersecurity improvements after implementing training.

LATAM employees least likely to prioritize other training

Respondents in LATAM were least likely to think employees would prioritize other training over security awareness training.



41% of decision-makers who are dissatisfied with current training have concerns that content is not engaging.

Training Needs to Be Intentional and Engaging

As proof that security awareness and training is a disciplined and well-considered undertaking in most organizations, 75% of respondents say their campaigns are planned in advance, with an average of three hours of training per year considered to be sufficient.

Eighty-one percent (81%) of organizations run security awareness and training for employees either monthly or quarterly. That regularity affords opportunities for refreshers and reinforcement, as well as net-new training on emerging threats and topics relevant to the organization.

The three-hour average aligns with last year's survey, where 59% of respondents said it would be reasonable for employees to spend 1 to 3 hours a year in security awareness training. With best practices suggesting a range of 5 to 15 minutes per learning module (and up to 30 minutes for complex topics), that allows for the coverage of up to 12 discrete topics in the course of a year.

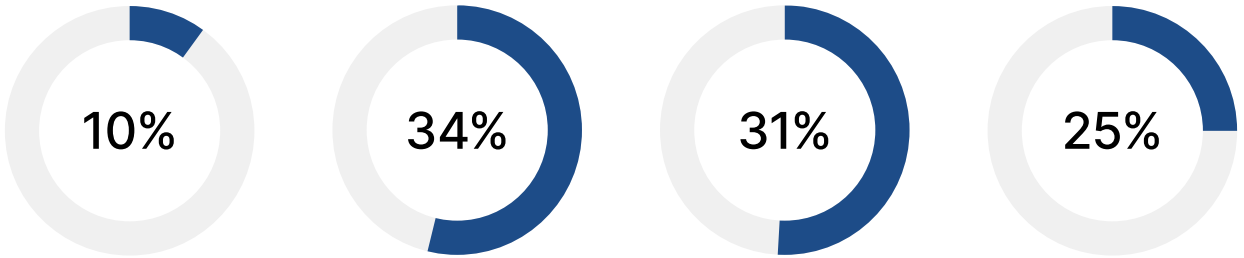
While 86% of decision-makers say they are satisfied with their current security awareness and training solution, among those not satisfied, the biggest complaint by far was a lack of engaging content, at 41%.

Enough time to make an impact

Too little time allocated to security awareness and training can lead to sub-optimal results. Yet demanding too much time from employees can also overburden them or force them to prioritize other mandatory training. Between 1.1 and 2.0 hours is the most common amount of time proposed, with three hours as the average.

34% of decision makers feel that 1.1 to 2 hours is a reasonable length of time for employees to spend on security awareness and training

Mean: 3 hours



DIGGING DEEPER

The Quality of Content Counts

Lack of engaging material is the biggest cause of dissatisfaction

While most organizations are very satisfied with their security awareness and training service (41%), those that are somewhat or very unsatisfied have several reasons:

- Lack of engaging content (41%)
- Cumbersome onboarding (26%)
- Poor customer service (23%)
- Lack of features and reports (9%)

Organizations rely on a mix of technologies to manage training

Respondents have access to different applications for different training:

- 51% manage employee security awareness and training through a combination of in-house learning management systems (LMSs) and software-as-a-service (SaaS) programs.
- 30% use in-house LMS only.
- 19% use external SaaS only.

Training content comes from multiple sources

The responsibility for developing security awareness and training content differs across organizations:

- 22% develop their own material in-house.
- 22% rely on third-party providers.
- 22% rely on a combination of the two.

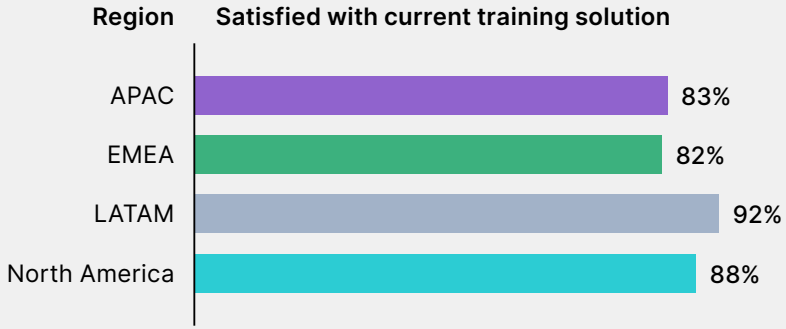
Regional Highlights

North America and APAC are most likely to plan in advance

Respondents in North America and Asia Pacific (APAC) are most likely to plan security awareness and training campaigns in advance, while those in LATAM are least likely.

LATAM organizations are happiest with their training solutions

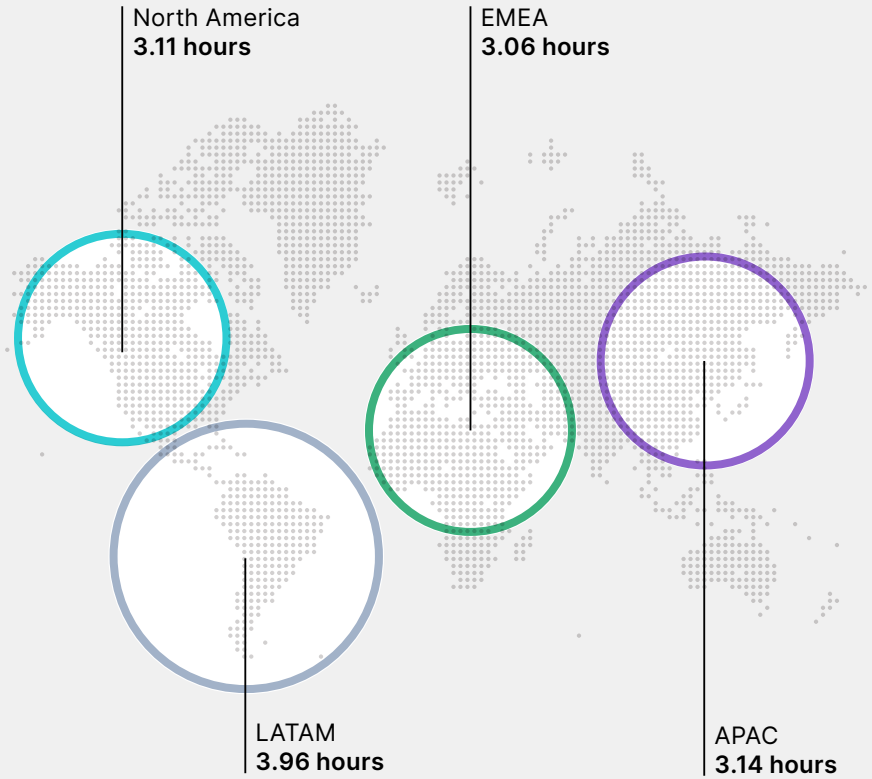
Respondents in LATAM are most satisfied with their current security awareness and training solutions compared to other regions.



LATAM organizations would spend more time on training

Leaders in LATAM say an average of nearly four hours of annual training would be appropriate compared to three hours in the other regions.

Average time reasonable to spend on security awareness and training



Conclusion

Decision-makers know security awareness contributes directly to the strength of their organization's security posture. Most are investing time and money in structured training and awareness programs for employees. While they're seeing results, it's clear the work is far from done—especially in light of emerging threats like AI.

Organizations need to ensure their people know how to safeguard against new and increasingly powerful attacks. Since even a single breach has significant repercussions to a business, building up a three-pronged defense of awareness and training, technical cybersecurity skills, and advanced security solutions is critical.

With nearly all (94%) respondents to this year's survey using or planning to use AI tools for cybersecurity, it's clear that AI will be a key part of those solutions going forward.

Organizations are also looking to complement security awareness and training with good governance: corporate policies to guide employees' digital behavior, including the use of AI tools and cyber insurance to backstop against losses and help strengthen internal practices. Though as of today, many still need to catch up when it comes to managing and monitoring work-related AI tool use.

It's also clear that training content needs to be engaging to be effective. What that means may vary from organization to organization, though broadly speaking, it points to material that is learner-centered and interactive with concise, easy-to-understand modules and multimedia or interactive elements to deepen knowledge and support retention. It also means keeping training relevant through regular updates that reflect evolving needs.

Our 2024 security awareness and training survey shows that strong organizational support contributes to more positive employee attitudes and greater leadership confidence in training outcomes. In Fortinet's experience with customers, that support must include coordination among executives, HR leaders, IT representatives, and cybersecurity teams to establish a consistent program for employees. This can be a challenge when resources are tight, and is a reason why many firms seek to partner with awareness and training vendors.

At the end of the day, as attacks continue to evolve—increasingly with employee end users as their targets—security awareness and training are only going to become more vital. Organizations can help ensure they get the best possible return on their training investments by building up and maintaining programs that are engaging and up to date.

Beyond teaching individuals what to do when they encounter threats, awareness and training are about creating a culture of cybersecurity to guide the organization both today and in the future.

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

October 17, 2024 11:29 am / MKTG-69-0-0-EN