ARCTIC WOLF

REPORT

Human Risk Behavior Snapshot

SECOND EDITION

An analysis of IT leader and end user attitudes in an evolving threat landscape

2025

Table of Contents

Introduction

Human risk is a growing component of organizations' attack surfaces, especially in the age of user-centric perimeters, hybrid work models, and digitalization. Combine these new risk points with an evolving threat landscape where threat actors are all too eager to exploit users for access to launch both simple and sophisticated attacks, and a concerning picture comes into focus.

To better understand how organizations are addressing and combatting human risk within their own environments, we surveyed over 1,700 IT leaders and end users around the world. We examine how, and how often, human-related breaches occur, attitudes toward human risk within organizations' environments and cybersecurity strategies, and the relationship between confidence and reality in relation to human risk reduction.

The findings revealed worrying gaps. Gaps between an understanding of large language models' (LLMs) potential value and a recognition of their risks — 60% of IT leaders and 41% of end users who adopt tools such as ChatGPT input confidential data. Between the beliefs of 76% of IT leaders who say their organization won't fall for a phishing attack, and the reality that 65% of IT leaders have clicked on a link they thought could be phishing.

This report aims to help close these gaps by illuminating the role of human behavior and human risk in cybersecurity while demonstrating how leading organizations can best support and benefit from their greatest cyber defense assets — their people.

Country of Residence

200 United Kingdom, Ireland

200 Switzerland, Germany, Austria

200 Australia, New Zealand

150 Belgium, Netherlands

100 Canada

500 United States

150 Norway, Sweden, Denmark, Finland

150 Japan

60 Singapore

The values shown are based on an even split of 50% IT leaders and 50% end users.

Methodology

Two parallel surveys were conducted among **855 IT and security leaders**, from C-level executive and director/VP roles, and **855 end users** whose roles include middle and senior management from departments including operations, human resources, sales, finance, and marketing. Participants were from **SMBs with more than 50 employees** to large enterprises and came from **17 countries** (listed to the left). The interviews were conducted online by Sapio Research in July 2025 using an email invitation and an online survey.

Please note when comparing this year's and last year's results that Japan and Singapore are additional countries for 2025, and Luxembourg has not been included this year.

IT Leaders	End Users
Industry	
19% Manufacturing	**17%** Financial services
18% Financial services	**14%** Retail
18% IT / Technology / Telecoms company	**14%** Manufacturing
Business Size	
36% 50 to 499	**40%** 50 to 499
39% 500 to 2,999	**33%** 500 to 2,999
25% 3,000+	**28%** 3,000+
Job Role	
54% C-Level Executive	**46%** Senior managers
46% Director / VP	**54%** Middle managers

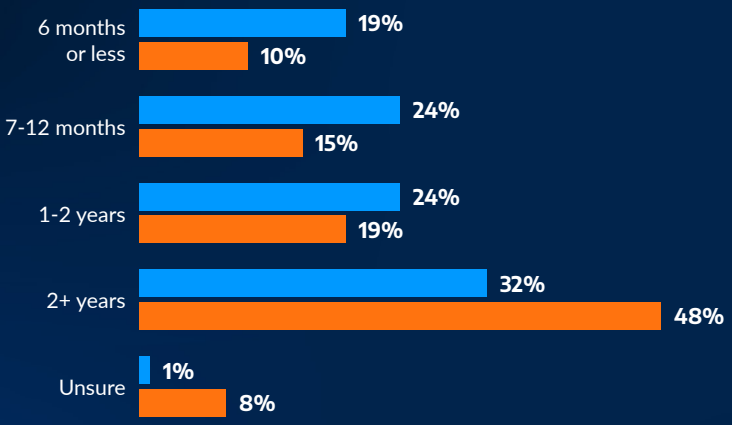
Baseline Context – Security Maturity

We asked a number of questions to understand our respondents' baseline organizational security maturity and attitudes. Their answers are included here to help you benchmark your organization as you review the findings throughout the report.

Throughout the report we use **blue to represent IT leaders** and **orange to represent end users**. This visual differentiation will help you easily follow the data and see how perspectives vary between these two groups.

Do you have security awareness training in place?

How long has your organization had security awareness training in place?



Do you have phishing simulations?

Do you know how to report an incident?

01

SECTION ONE:

When Overconfidence Confronts Reality

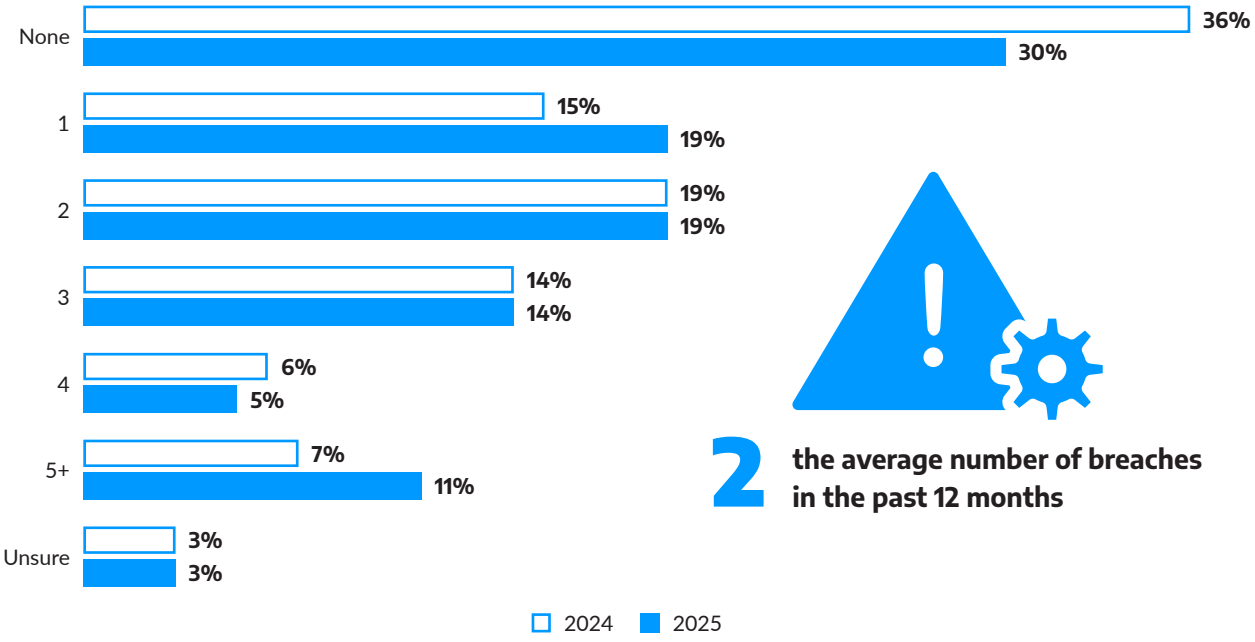
Even as cyber incidents rise and threat actors increasingly target senior leaders, IT leaders remain overly confident in their organizations' defenses.

The Number of Breaches Continue to Rise

More than two-thirds (68%) of IT leaders said their organization had experienced a breach in the past 12 months — an 8% increase from last year.

The number of organizations experiencing more than five incidents within the last 12 months has risen 4% to more than one in 10, while those reporting zero breaches has dropped from 36% to 30%.

IT leaders were asked how many breaches their organization experienced in the last 12 months.



2 **the average number of breaches in the past 12 months**

The Human Risk Factor

As the cyber landscape changes, users are one of the more reliable ways for threat actors to gain initial access to valuable assets, applications, and broader networks.

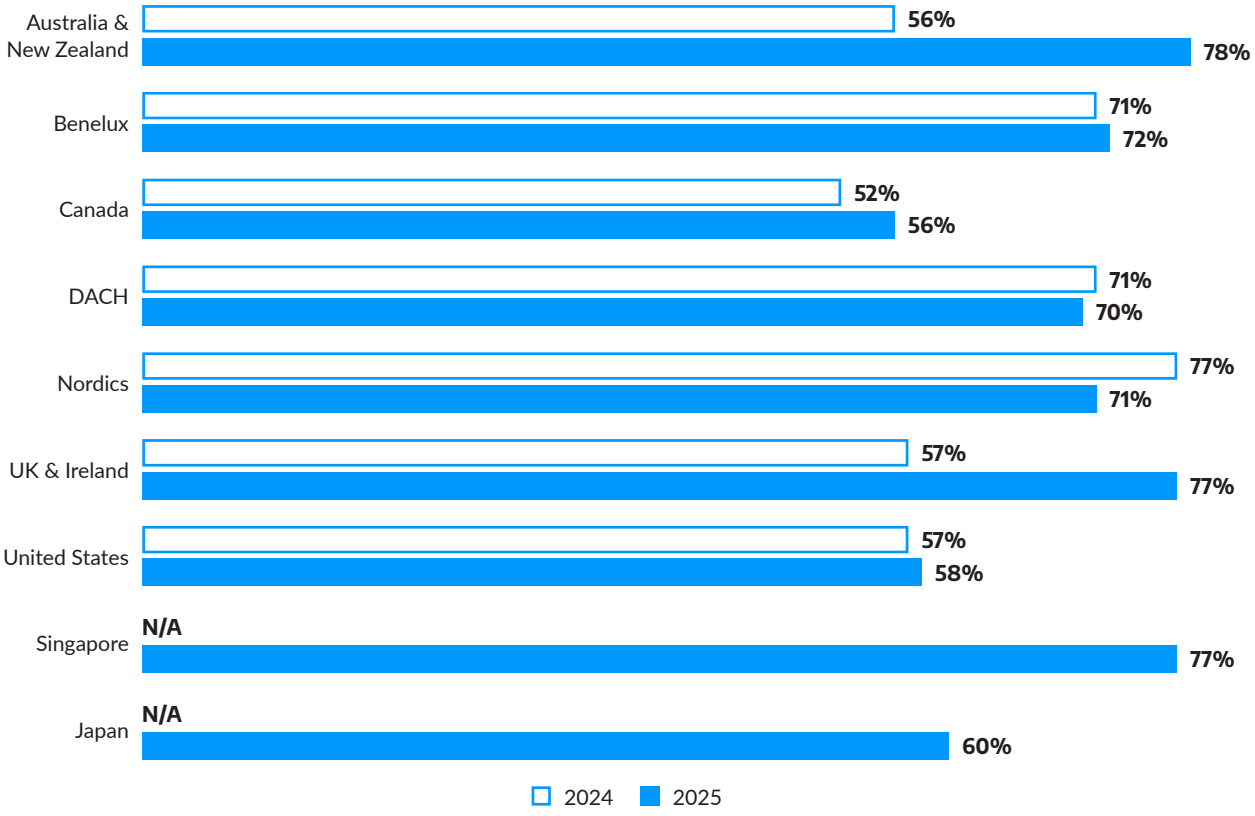
Humans can be involved in breaches in a number of ways, including credential compromise, insider threats, social engineering, and poor cyber hygiene.

Australia, New Zealand, United Kingdom, and Ireland See Highest Rise in Breaches

Australia and New Zealand saw a sharp increase in the number of breaches their organizations experienced year-over-year, **from just over half (56%) in 2024 to more than three-quarters (78%) in 2025.** We know that incidents involve humans 60% of the time[1], so human risk mitigation factors could reduce this growth.

Organizations in the U.K. and Ireland experienced a similar uptick in breaches, which rose 35% year over year. In the spring of 2025, the U.K saw a series of attacks on prominent retailers.

IT leaders that experienced one of more breaches in the last 12 months.



What's behind the U.K. breach increases?

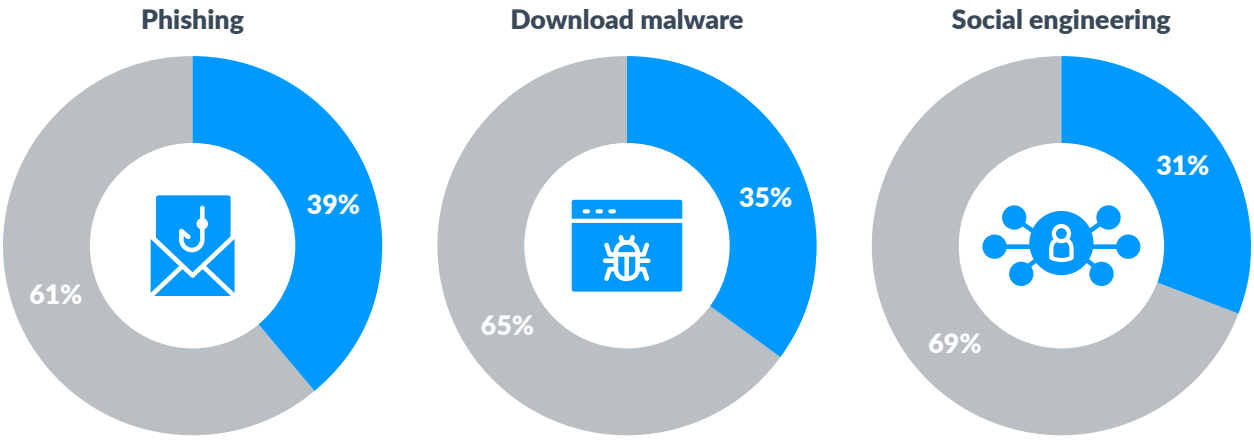
Ransomware activity targeting U.K.-based retailers is increasing. Contributing factors include the sector's historical reliance on legacy systems, seasonal spikes in consumer activity, and the complexity of managing customer data across distributed environments. Recent incidents involving well-known U.K. retailers such as Marks & Spencer, Co-op, and Harrods have given insight into the evolving tactics of threat actors like DragonForce and Scattered Spider. DragonForce has been associated with ransomware-as-a-service (RaaS) operations, which has lowered the threshold to entry for cybercriminals and enabled more frequent and widespread attacks. While these attacks are serious, they also reflect a broader shift in threat actor behavior toward more opportunistic and scalable methods, making retail a prime target.

1. 2025 Verizon Data Breach Investigations Report

Leaders Are Targeted in Phishing Attacks

The C-suite and senior leaders are an attractive target for cybercriminals thanks to their access to high-value data, permissions, and even funds, so it's perhaps no surprise that **39% have been targeted by phishing and 35% by a malware download.**

IT leaders were asked if their leadership team or C-suite had ever been the initial victim of any of the following cyber incidents (selecting all that applied).



69% **of IT leaders have been the initial victims of cyber incidents**

> "A strong security posture starts with leadership. When executives make cybersecurity a priority, it sets the tone for the entire organization and builds a culture where protecting sensitive data and systems is everyone's responsibility."
>
> *Adam Marrè, CISO at Arctic Wolf*

Phish First, Scam Later

According to the FBI Internet Crime Complaint Center (IC3), more than $6.3 billion (USD) was transferred as part of business email compromise (BEC) scams in 2024[2]. More than a third (35%) of organizations suffered a BEC attack in 2024[3]. BEC attacks often target senior leaders within an organization due to their access. While phishing is often seen as an "obvious" scam, it can lead to serious consequences and/or more sophisticated attacks. Phishing (72.9%) and previously compromised credentials (18.8%) are the leading root causes of BEC cases[4], pointing to employee training, credential management, and biometric- or possession-based MFA as effective defenses.

2. 2025 Verizon Data Breach Investigations Report
3. 2025 Arctic Wolf Threat Report
4. 2025 Arctic Wolf Threat Report

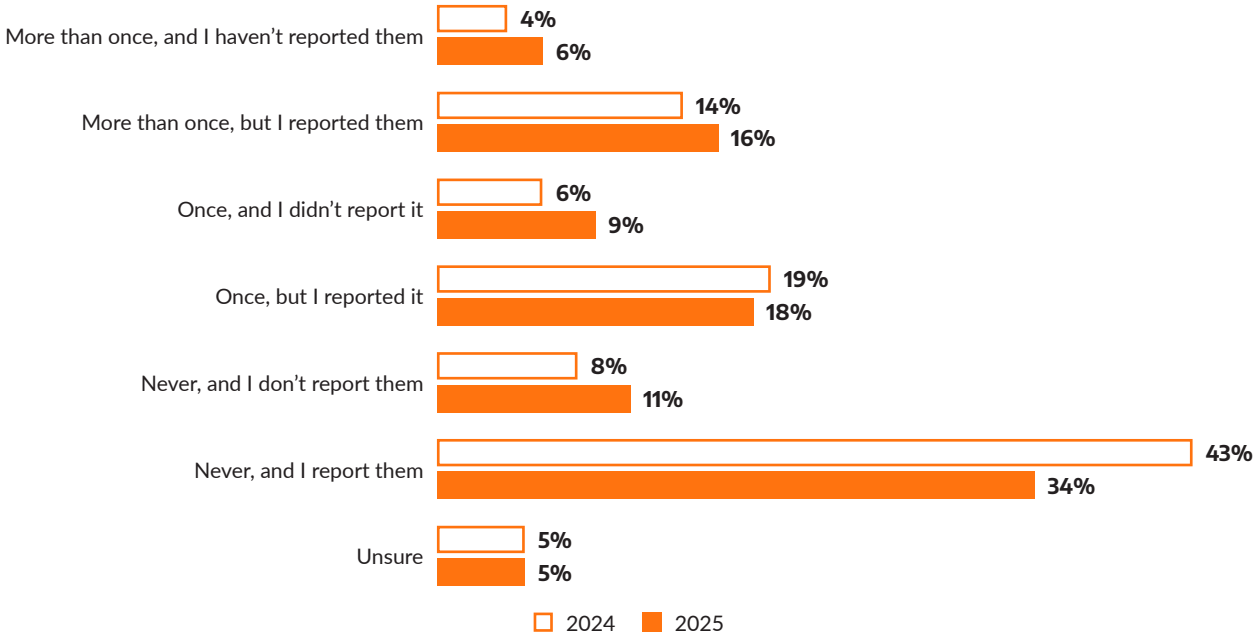
The Perennial Phishing Threat

Phishing is big business for threat actors, which means it's not going anywhere soon — especially if IT leaders and end users keep clicking.

50% of end users have clicked a link they thought could be phishing. Of those, 15% say they didn't report it

19% of end users say they never receive phishing simulations

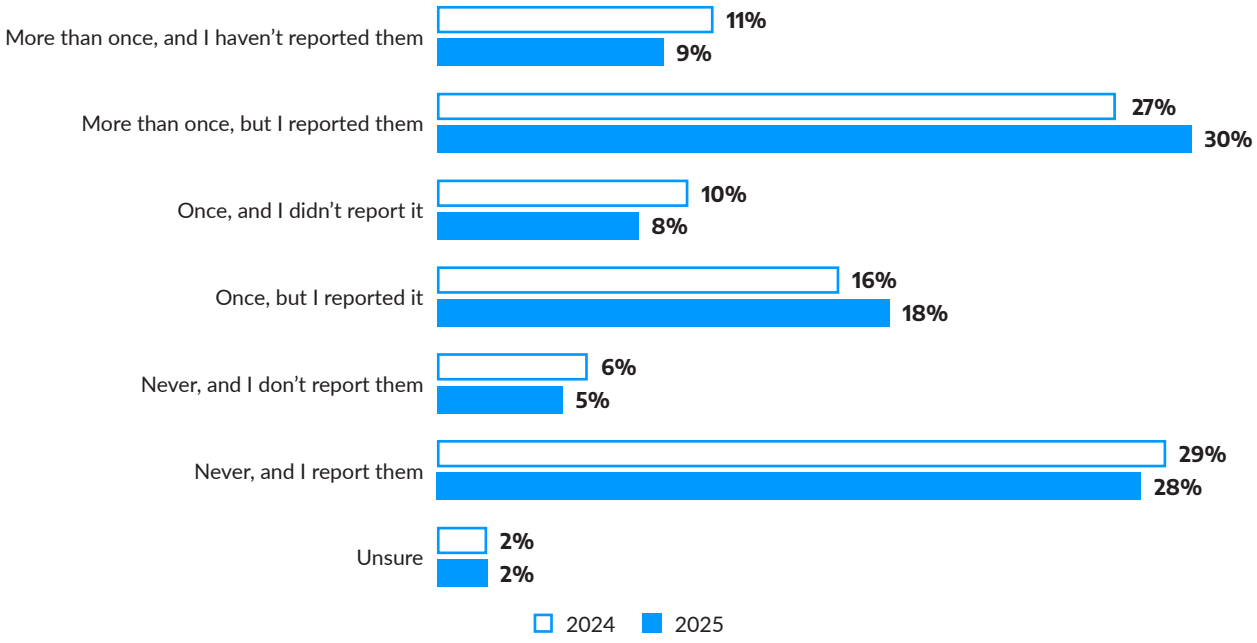
End users were asked if they had ever clicked a link in an email they thought could be phishing.



Nearly Two-Thirds of IT Leaders Have Clicked on Phishing Links

Almost as surprising as the fact that 65% of those in senior IT roles have clicked on phishing links is the fact that almost one-fifth (17%) didn't report it. While there isn't clear-cut reasoning behind this lack of accountability, as we'll discuss below some company cultures penalize or even terminate employees for clicking on phishing links. A level of embarrassment (or fear of their own termination) could be preventing leaders from notifying others of what's occurred.

IT leaders were asked if they had ever unintentionally clicked a link in an email they thought could be phishing.



Spear Phishing

Spear phishing involves threat actors crafting highly credible messages based on detailed information they've gathered on high value targets, such as IT leaders. These kinds of phishing attacks are becoming more common — in part due to the research powers of AI — and can be damaging for victims. Analysis of 50 billion emails found that while spear phishing only accounted for less than 0.1% of emails, it also led to 66% of successful breaches[5].

5. 2023 Spear Phishing Trends, Barracuda Networks

Phishing Overconfidence Exposes Organizations to Risk

Unfounded confidence on the part of IT leadership is opening organizations up to attacks. **While 65% of IT leaders and 50% of end users acknowledge clicking on potentially dangerous links, 76% of IT leaders are confident their organization won't fall for a phishing attack.**

Given how prevalent phishing threats are, and how often end users and IT leaders click on phishing links, this overconfidence is both hindering a culture of security and creating unnecessary risk. Misplaced confidence can lead to leaders not investing in certain technology, downplaying the threat of phishing, or being less on guard for potential phishing emails in their inboxes.

IT leaders were asked how confident they were that their organization wouldn't fall for a phishing attack.

> "Cybersecurity readiness means accepting it's not a matter of if, but when. The organizations that succeed are those that stay vigilant and continually strengthen their response."
>
> *Adam Marrè, CISO at Arctic Wolf*

Who's most confident?

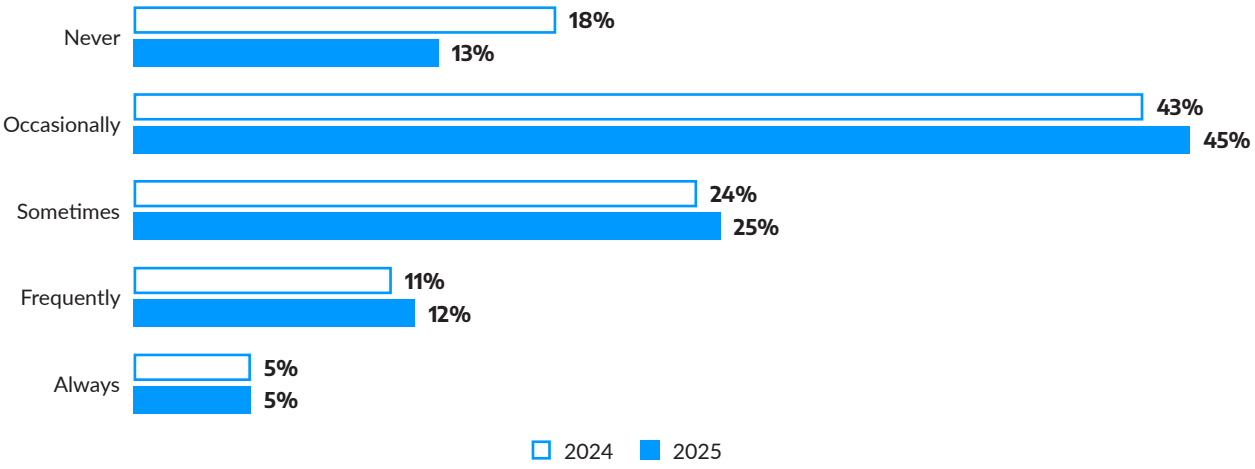
Despite the 39% surge in overall breaches in Australia and New Zealand from 2024 to 2025, these countries — along with the U.S. — are among the most confident about resisting phishing attacks (84%). Other groups with high confidence levels are those who have security awareness training weekly (92%), and companies with between 3,000-4,999 employees (85%).

91% of IT Leaders Send Phishing Simulations

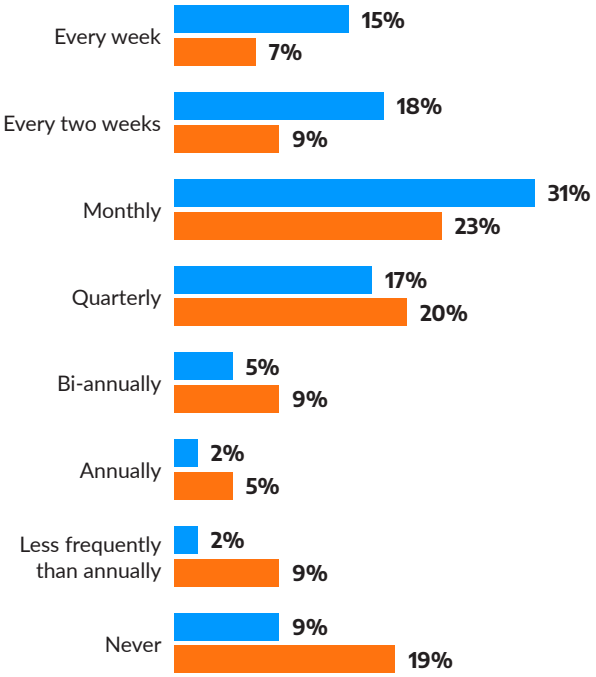
Almost all IT leaders (91%) send phishing simulations to their organizations, with nearly a third (31%) sent on a monthly cadence. 87% say employees click on simulation links (up from 83% last year).

> "Today's biggest breaches still start with yesterday's trick: phishing. Groups like Scattered Spider pair simple lures with credential theft to pivot fast — exactly why culture, simulation, and strong authentication matter. If we reduce clicks and require MFA universally, we shrink the blast radius of the next headline."
>
> *Adam Marrè, CISO at Arctic Wolf*

IT leaders were asked how often employees click phishing simulation links.



IT leaders were asked how often they currently send phishing simulations to their organization. End users were asked how often their organization sends phishing simulations to help them feel prepared to spot an attempted attack.



Phishing Simulation Best Practices

Nearly half (49%) of end users say phishing simulations are only "somewhat effective."

But the data tells a different story — global IT leaders see clear results. An overwhelming 91% of them run phishing simulations, and thanks to those efforts, only half of end users are now falling for real phishing attacks. Phishing simulations, when used as an additional component of a larger phishing and BEC mitigation strategy, can be effective and measure impact and progress while also identifying potential concerns. Regular practice boosts awareness and helps build a culture where everyone plays a part in keeping the organization secure. The most effective simulations don't aim to trick or punish — they teach employees how to spot and report phishing attempts with confidence.

A Phishing Case Study: Scattered Spider

The data above is concerning, as it shows that neither IT leaders or end users are taking the threat of phishing seriously. This simple technique can yield massive results for threat actors — take **Scattered Spider** for example.

Utilizing basic social engineering tactics such as phishing to obtain user credentials, this cybercrime gang has been responsible for the major data breaches at **Marks & Spencer, Harrods**, and the MGM and Caesar's hack back in 2023. This notorious group is known to gain initial access using stolen credentials obtained from SMS phishing operations. SIM swapping attacks have been conducted against telecom providers to obtain access to targeted customers of those providers. **They've also had success posing as IT staff in sophisticated phishing attacks against targeted organizations.**

02

SECTION TWO:

AI Uptake Exposes New Risk Points

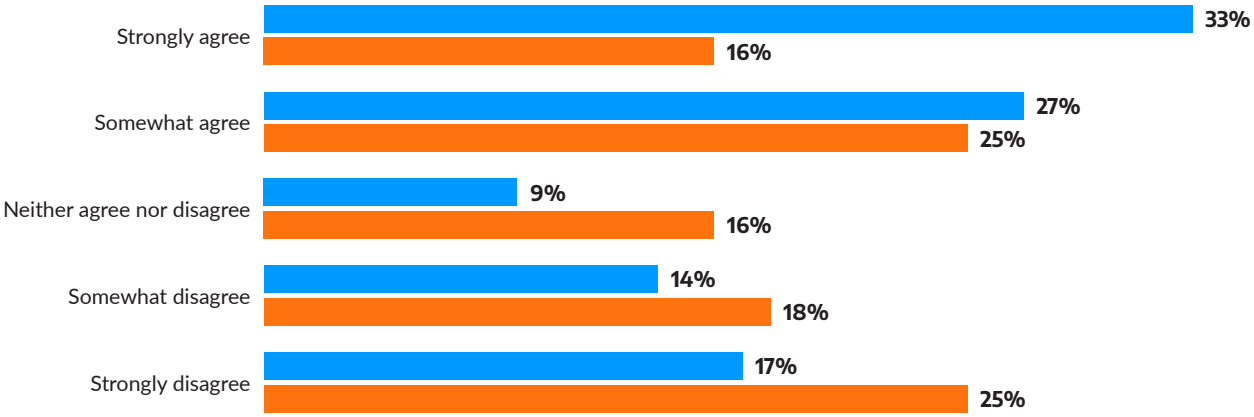
With AI adoption increasing among end users and IT leaders, organizations are enhancing governance efforts as many users acknowledge sharing confidential data in LMM tools like ChatGPT.

Nearly Two-Thirds Use ChatGPT at Work

Of the 63% of end users employing LLM technology, such as ChatGPT or other generative AI tools for work, 41% say they've shared confidential information in these tools. **Astonishingly, an even higher proportion of IT leaders have used these systems (80%) and have shared confidential material (60%).** Both groups' usage has also increased since last year.

In recent Arctic Wolf reports, "AI, large language models (LLMs), and associated privacy concerns" were chosen by 29% of respondents as their top cybersecurity concern[6]; while a third (33%) of organizations noted their growing concern about data privacy[7].

IT leaders and end users were asked to what extent they agreed with the statement "I have shared confidential information in LLM, such as ChatGPT."



AI Policies Mature

As uptake of AI and LLM technology grows, so does the level of governance around it. 88% of IT leaders (60% in 2024) and 57% of end users (29% in 2024) say they have a policy regarding the use of generative AI like ChatGPT in the workplace. However, 43% of end users don't think or are unsure if their organization has such a policy.

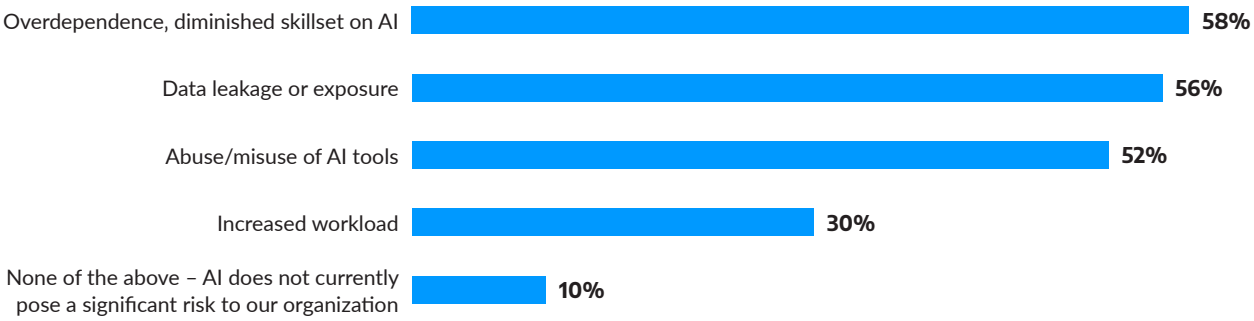
This gap shows a lack of communication, as well as awareness training, around the risks of AI tool use. Organizations need to ensure their policies are communicated clearly and enforced and offer training to help users understand the risks AI technology can pose to their data and network at large.

6. The State of Cybersecurity: 2025 Trends Report
7. Navigating The Human-AI Relationship For Security Operations Success

Over Half of Organizations Fear AI Will Create Unintentional Data Leaks

Most IT leaders have concerns of some nature about AI, as only one in 10 say the technology poses no risk to their organization. The top concerns relate to overdependence — leading potentially to a loss of skill and critical thinking — and sensitive information being shared through AI systems.

IT leaders were asked what risks Artificial Intelligence (AI) poses to their organization.



Educating Employees on Safe LLM Use

The emergence of LLMs that are easily integrated into countless applications have made them a prime target for adversaries. Without robust security measures in place, AI infrastructure remains vulnerable to threats such as data leakage — exemplified by the 2025 DeepSeek breach, where user and prompt data were exposed due to an insecure database.

As part of their response to these threats, IT leaders must develop comprehensive policies around LLM use and educate end users on the risks of sharing confidential information. Not only do IT leaders need to develop comprehensive governance policies around LLM use and educate end users, but they must also instill a culture of security by following those policies.

03

SECTION THREE:

Culture and Communication

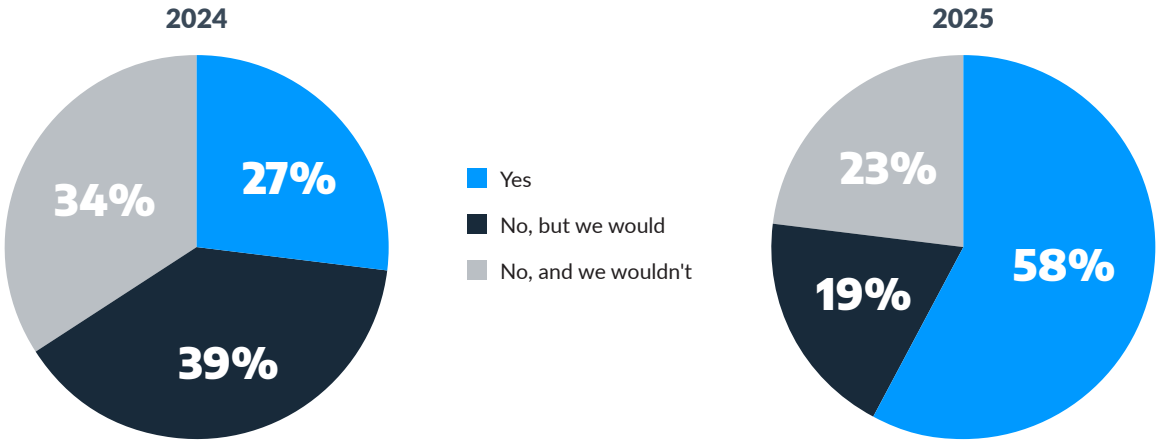
While end users feel comfortable reporting security incidents, leaders are taking a punitive approach to this honesty.

More Leaders Consider Terminating Scammed Employees

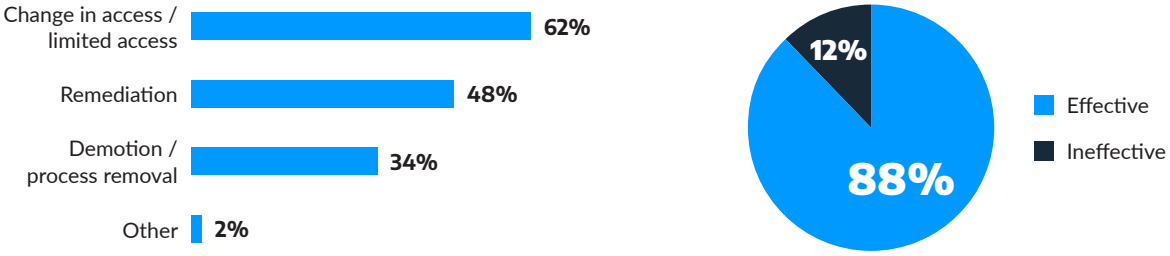
More than three-quarters (77%) of IT leaders say they either have or would terminate an employee for falling victim to a social engineering attack such as phishing — up from 66% last year. But where does the fault really lie? Better trained and equipped end users are less likely to become victims of a social engineering attack. Sixty-two percent of IT leaders have changed employees' access or limited their access as an alternative corrective action for falling for a scam.

Among those who have implemented remediation, almost nine in 10 (88%) IT leaders state the outcome is effective. Taking this education-based approach allows IT leaders to build a culture of security free of fear, better reducing overall human risk. However, fewer than a third (31%) of organizations consider "building a culture of security awareness" to be a primary cybersecurity objective — a worrying attitude as the impact of human risk continues to grow.

IT leaders were asked if they have ever terminated an employee for falling victim to a scam such as phishing.



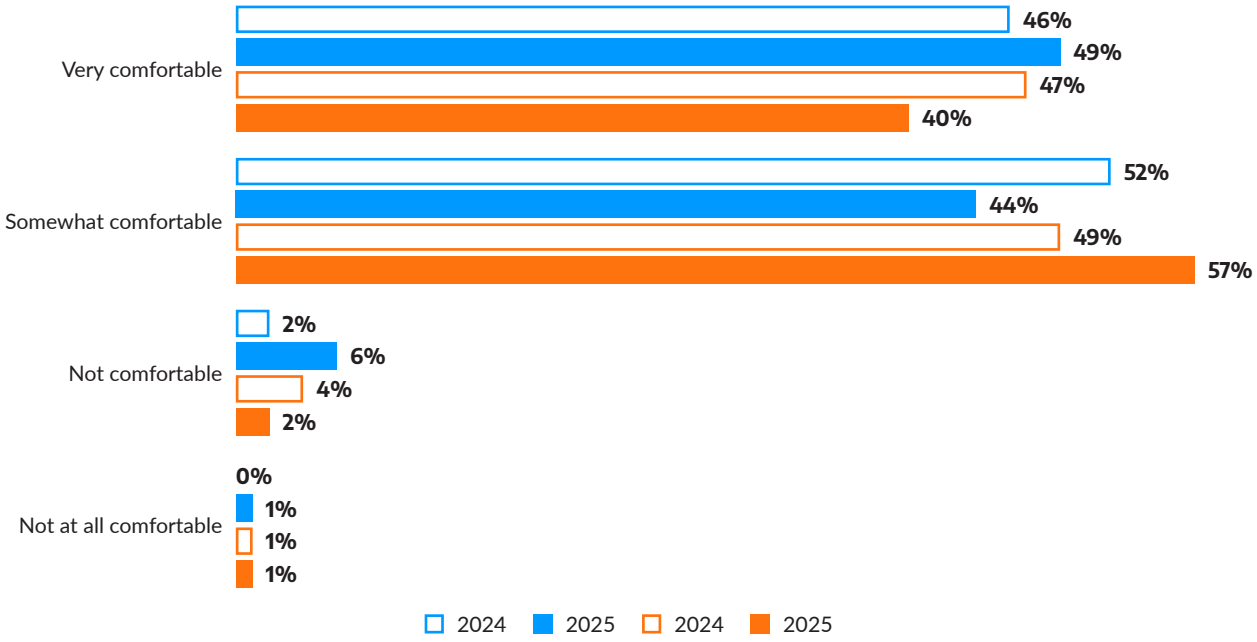
IT leaders were asked if they have taken other correction action on an employee for falling for a scam such as phishing. IT leaders were asked how they would describe the outcome of remediation.



Most Feel Comfortable Reporting Incidents

Despite IT leaders' increased willingness to consider termination for victims of attacks, **97% of end users said they felt comfortable reporting security failures or suspicious activities.**

IT leaders were asked how comfortable they thought employees felt reporting security incidents or suspicious activities to the appropriate channels in their organization. End users were asked to what extent they felt comfortable reporting security incidents or suspicious activities to the appropriate channels in their organization.



While employees feel they are in a safe, supportive environment, the reality is somewhat different. Rather than considering remediation or cultivating a culture of security and trust, IT leaders would easily terminate employees for a mistake.

> "Terminating employees for falling victim to a phishing attack may feel like a quick fix, but it doesn't solve the underlying problem. Our research shows that better-trained and better-equipped end users are far less likely to be duped — and when organizations take an education-first approach, nearly nine in 10 see positive outcomes. Building a culture of security that empowers, rather than punishes, employees is the most effective way to reduce human risk over the long term."
>
> *Adam Marrè, CISO at Arctic Wolf*

04

SECTION FOUR:

A Roadmap for Human Risk Reduction

Building a strong security culture starts at the top, yet with a quarter of leaders bypassing security measures and training often lacking impact despite being widespread, many organizations face challenges in fully establishing.

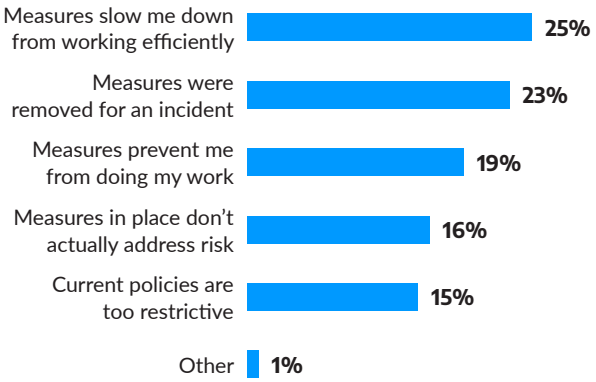
Basic Security Measures (Intentionally) Overlooked

Disabling security measures is a standard procedure during incident response (IR), and 23% of IT leaders say they've switched security off for that reason. However, we did see respondents select answers not related to incident response situations, with **25% of IT leaders say they have disabled security measures to work more efficiently.** Overall, more senior IT personnel are disabling security systems this year (51%) than last year (36%). Bypassing or disabling security measures increases risk and opens environments to more threats. If there is not a concrete reason to disable security measures (such as an IR investigation), it should not occur. Policies such as strong identity and access management (IAM) and better access controls can prohibit IT leaders from having these kinds of capabilities, reducing overall risk.

The number of end users attempting to bypass security is also on the rise, more than doubling from 12% in 2024 to 32% in 2025. The fact that 16% of end users were successful in their attempts should be concerning. End users' endpoints should be monitored for suspicious behavior (such as application disabling), and access controls should prohibit these application changes. Such measures can significantly reduce human risk.

IT leaders were asked if they had ever disabled security measures on their system. End users were asked if they had ever looked for a way to bypass security measures on their computer.

IT leaders were asked why they disabled security measures on their system.



Leading by example?

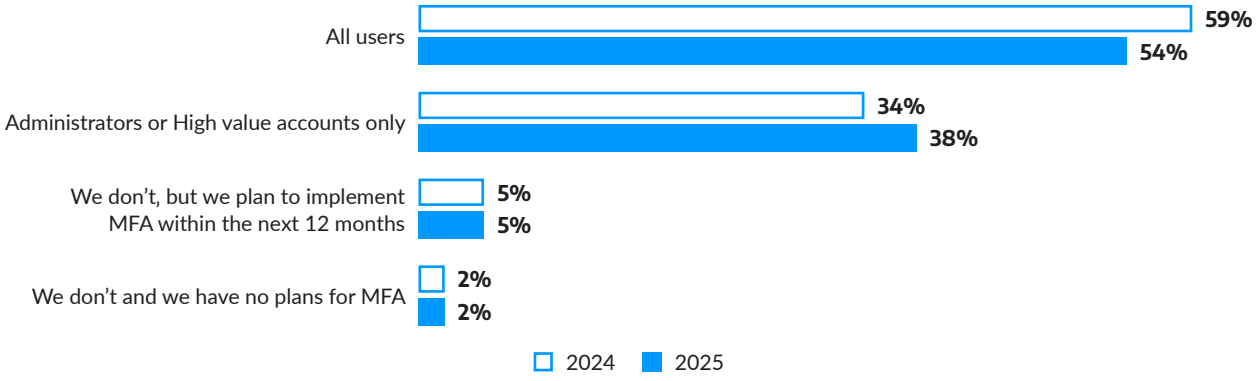
The number of IT leaders bypassing security measures is deeply concerning given that threat actors will often target the endpoint of senior team members, due to the privileged access they hold.

A culture of "do as I say, not as I do" will open organizations up to unnecessary risk: in particular of social engineering attacks like business email compromise (BEC) which often target the top of the company.

Only Half of Organizations Implement Multi-Factor Authentication (MFA) for Everyone

Multi-factor authentication (MFA) might not be a silver bullet, but it is a critical tool in the cyber defense kit. **The fact that only 54% of IT leaders apply it to all user accounts, and 38% mandate it for administrators or high value accounts only, is worrying.** Threat actors always choose the path of least resistance, therefore accounts without MFA are a target. Additionally, initial access is only the first step in a sophisticated attack chain. An IT department may (wrongfully) assume a low-level employee does not need MFA, but if a threat actor gains access to their endpoint, they can launch malware, ransomware, or jump to a more high-value endpoint or application within the network.

IT leaders were asked to what extent they currently enforce multi-factor authentication (MFA) for user accounts.



The best-protected organizations implement security strategies which consider and optimize both sides of the equation: people and tech. Teams need to be trained to be security aware but also need to be given the technology to make it easy to comply with policies and reduce their own risk. MFA is one such technology that is known to reduce incidents. 56% of organizations that had a significant cyber attack in 2024 had not implemented MFA[8].

8. The State of Cybersecurity: 2025 Trends Report

Frequency of Training Matters...

IT leaders and end users who receive security awareness training at least quarterly are more likely to to be confident in their organization's ability to defend against phishing and to be confident in their ability to protect against cyber attacks more broadly.

Both IT leaders and end users agree that a lack of awareness and training is the top reason humans pose a risk to cybersecurity. Other key contributing factors are keeping up with changes in technology (No. 2) and the sophistication of social engineering (No. 3) — both reasons why leaders should be equipping teams with the right technology and controls as well as relying on training.

How respondents who receive security awareness training at least quarterly responded to our other survey questions.

LLM Policy

85%
Yes

48%
No policy exists / Not sure

Confidence in company's anti-phishing defences

81%
Confident

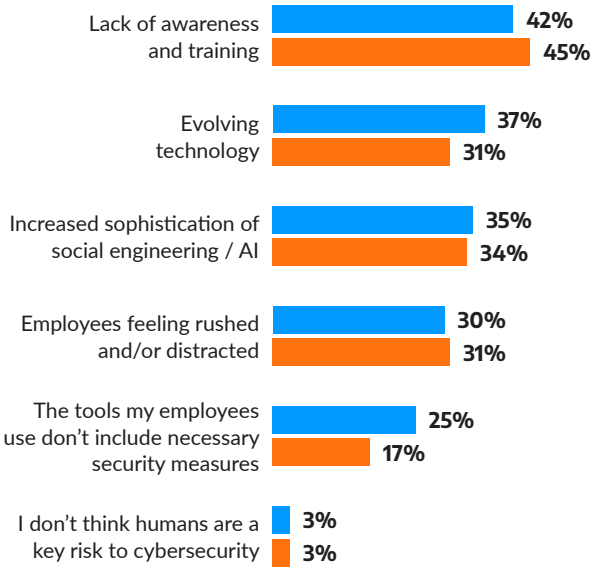
70%
Not confident

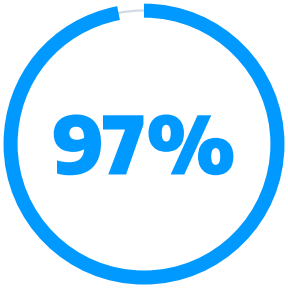
Confidence in company's ability to prevent with a cyber attack

82%
Confident

54%
Not confident

IT leaders and end users were asked what the main reasons are that humans are a key risk to cybersecurity.





of IT leaders receive security awareness training, with 80% being trained quarterly.

...but Training Content Could Be Improved

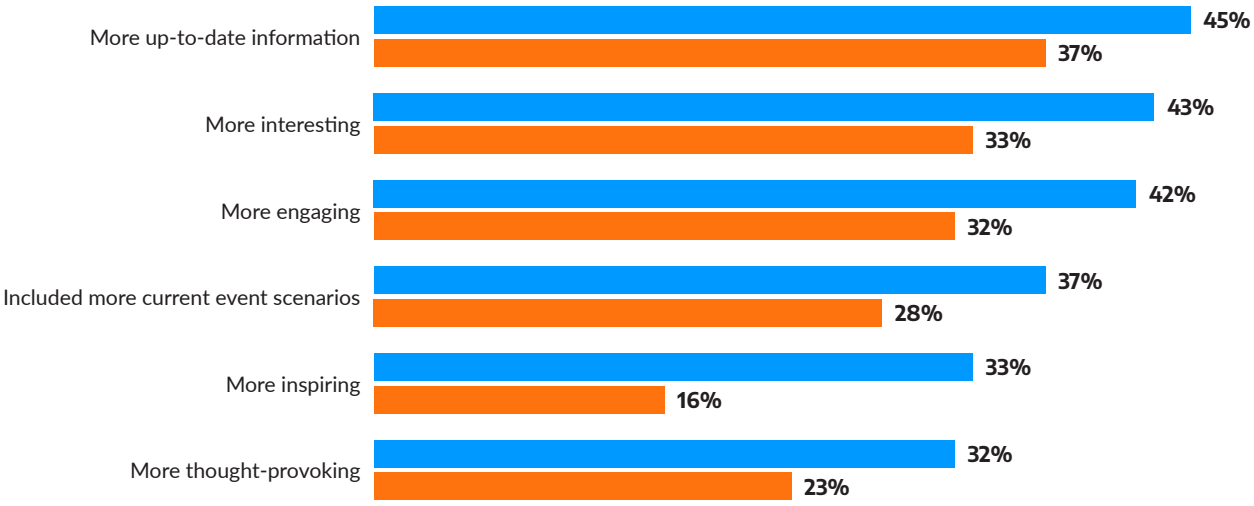
Organizations recognize the benefit of security awareness training, with 99% of IT leaders saying they've run it for at least six months. But when asked how the training could be improved, **almost half (45%) said it would benefit from more up-to-date information, and almost as many said it should be more interesting (43%) and engaging (42%).**

According to IT leaders:

32%
of organizations have had security awareness training in place for over two years

24%
of organizations have had security awareness training in place for between 1-2 years

IT leaders were asked how they would improve their organization's current security awareness training. End users were asked what improvements they would like to see within their organization's current security awareness training.



Effective Training: The Arctic Wolf View

Critical elements of effective security awareness training include:

- New lessons regularly, including rapid response training on emerging threats
- Bite-sized awareness sessions (maximum three minutes) to increase engagement
- Password- and-login-free, email-based lessons for convenient access
- Materials designed for how the brain processes and stores information, to maximize recall

Conclusion and Recommendations

As threat actors continue to target users, and as the IT environment shifts further emphasis onto mobile endpoints, user-centric perimeters, web-based applications (including email), and hybrid or remote work models, human risk increases.

As such, equipping your users (e.g employees, third parties, etc.), with the needed defenses and reducing organization-wide human risk requires a comprehensive strategy that incorporates multiple strategies.

Lead by Example

Defending against cyber attacks starts at the top of the organization. Bad actors are using advanced phishing capabilities, powered by AI, to produce highly targeted campaigns aimed at accessing privileged credentials. IT leaders who practice what they preach not only set the right example for the wider workforce; they reduce the real risk of becoming a breach point themselves.

Communicate Clearly

Organizations are keen to capitalize on the value offered by LLMs such as ChatGPT. But if guidance around how to use AI safely isn't fully communicated and understood, this technology represents a major risk. IT leaders must develop comprehensive policies around LLM use and educate end users on the risks of sharing confidential information.

Build on the Basics

While threat actors may be using more sophisticated tactics, some of the most dangerous attacks start with a simple phishing email. Phishing (72.9%) and previously compromised credentials (18.8%) are the leading root causes of BEC cases[9], pointing to employee training, credential management, and biometric- or possession-based MFA as effective, foundational defenses.

Educate Rather Than Punish

The most successful security cultures encourage transparency and communication. Rather than using phishing simulations as a reason to punish employees, or terminating those who fall for scams, use learning opportunities to better educate and equip teams. Among those who have implemented remediation as a response to scams (such as changing access levels), almost nine in 10 (88%) IT leaders reckon the outcome is effective.

9. 2025 Arctic Wolf Threat Report

About Arctic Wolf

Arctic Wolf® is a global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk.

Built on open XDR architecture, the Arctic Wolf Aurora™ Platform operates at a massive scale and combines the power of artificial intelligence with world-class security experts to provide 24x7 monitoring, detection, response, and risk management. We make security work.

For more information about Arctic Wolf, visit **arcticwolf.com**.

About Sapio Research

Sapio Research is a full-service B2B and tech market research agency that helps businesses grow thanks to high quality, efficient and honest research solutions.

We deliver valuable insights to support our clients understand their audience, build powerful brands, cut through the noise with great content and thought leadership. We're based in the UK and have access to over 149 million people across 130 countries, working with clients that range from top tech companies to global consultancies, Marketing/PR agencies and household name brands.

Our purpose-driven team of expert market researchers is passionate about providing data confidence for all and performing research that makes a difference. We're here to support our clients every step of the way in all areas of quantitative and qualitative research, so they can save time and thinking space, deliver with confidence, and unlock more value with their research.

For more information about Sapio Research, visit **sapioresearch.com**.

AW_R_HUMAN RISK_1025