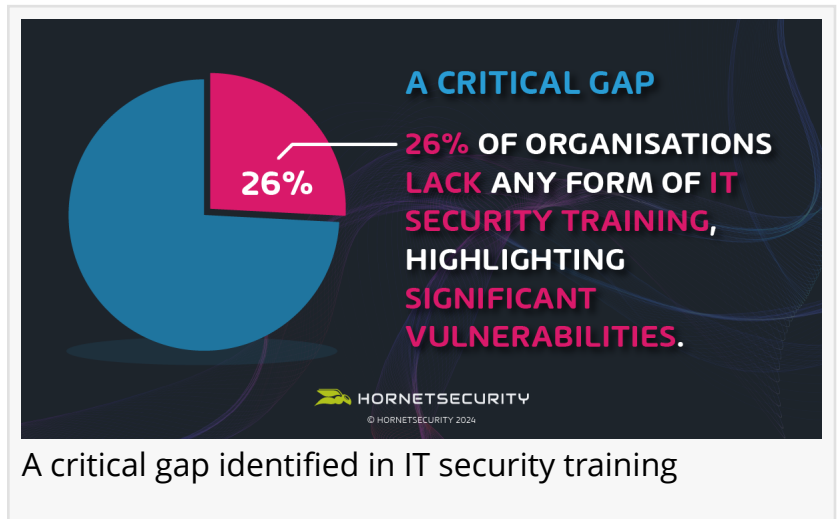


# Urgent training gap exposed: a quarter of organisations unprepared for cyber-attacks

Survey reveals 26% of businesses skip end-user security training with 25% facing breaches, 23% in the past year. 39% say AI is not covered by current training.

EXCEL LONDON, UNITED KINGDOM, June 4, 2024 /EINPresswire.com/ -- [A new survey](#) by cybersecurity provider [Hornetsecurity](#) has uncovered significant gaps in IT security training, with a quarter (26%) of organisations still providing no form of training to their end-users. The company issued the survey results at Infosecurity Europe 2024, where it is exhibiting at stand E60.



“

Our latest research shows a clear disconnect between the perceived effectiveness of security training and its actual relevance and responsiveness to modern cyber threats.”

*Daniel Blank, Hornetsecurity  
COO*

The survey, which compiled feedback from industry professionals around the world, also reveals that fewer than 1 in 13 (8%) of organisations offer adaptive training that evolves based on the results of regular security tests. In a rapidly evolving cybersecurity landscape, where malicious threat actors are constantly devising new ways to infiltrate and harm, this is a significant business concern.

## Engagement and Effectiveness in Training

People represent the frontline of every company's cybersecurity strategy. The most popular type of cyber-

attack is phishing, which preys on a person's trust. Employees must therefore be equipped with the skills, understanding and confidence to spot malicious behaviours. Sadly, Hornetsecurity's survey revealed that not only is there a significant gap in training, but training initiatives are seen to be ineffective. Nearly a third (31%) of respondents reported that their training was unengaging or only slightly engaging.

Despite the low engagement levels, 79% of organisations believe their IT security awareness training to be at least moderately effective in combating cyber threats. However, nearly four in ten (39%) reported that the training does not cover recent or AI-powered cyber threats adequately. In a world where AI is expediting and increasing the scale of attacks, this is alarming.

Daniel Blank, COO of Hornetsecurity, says, "Our latest research shows a clear disconnect between the perceived effectiveness of security training and its actual relevance and responsiveness to modern cyber threats, especially the recent boom in AI-driven attacks. Employees must be equipped with ongoing training to bolster any technical defences and serve as a human firewall. The ongoing aspect is essential for the training to have the most impact. It's important to invest in the latest cybersecurity technology, but a sustainable security culture means investing in people as well."

Post-incident adaptations and reporting gaps

[The survey found](#) that one in four organisations had suffered a cybersecurity breach or incident - 23% of which had occurred in the last year. Notably, 94% of these organisations took steps to strengthen their security by implementing additional controls post-incident. Yet, despite these efforts, 52% of respondents noted that end-users often ignore or delete identified email threats without reporting them, and 38% forget the training content, showing the need for ongoing and engaging training enhancements.

The survey highlighted that people are particularly interested in more effective post-training resources, which could help in retaining and applying the learned security measures. Another area for improvement is feedback on reported threats, with 28% stating the lack of feedback as a reason for not adhering to training protocols.

The need for updated training



23% of cybersecurity breaches occurred in the last year alone



45% of decision makers identify inadequate security training in the face of evolving cyber threats

A significant 45% of decision-makers in IT believe their current training programmes are outdated and ineffective against AI-powered attacks. This sentiment is echoed by 39% of general respondents, showing a critical need for training content that is both current and comprehensive.

Daniel Blank adds, "It's imperative that organisations not only provide regular, engaging, and adaptive training but also ensure that these programmes thoroughly address the latest and most sophisticated cyber threats. This is why we developed Hornetsecurity Security Awareness Service, a next-gen solution that delivers the right amount of training customised per employee in an automated way. That way, organisations can provide the right level of ongoing training without draining IT resources to set this up and deliver it."

He stressed: "Proactivity is key: instead of strengthening after incidents, organisations should pre-empt attacks and have robust systems and processes in place. Doing so saves significant time, effort and cost."

#### Cyber insurance and preventative measures

Over half of the surveyed organisations (56%) now use cyber-insurance, indicating a growing reliance on financial safeguards against cyber incidents. Additionally, 79% of organisations attribute the prevention of cybersecurity incidents directly to their IT security training programmes, while 92% acknowledge that the training has enabled end-users to spot security threats across various media, not just email.

- ENDS -

#### Notes to Editor:

The study, Company IT Security Awareness, was conducted by Hornetsecurity in April 2024 and had more than 150 respondents.

#### About Hornetsecurity

Hornetsecurity is a leading global provider of next-generation cloud-based security, compliance, backup, and security awareness solutions that help companies and organizations of all sizes around the world. Its flagship product, 365 Total Protection, is the most comprehensive cloud security solution for Microsoft 365 on the market. Driven by innovation and cybersecurity excellence, Hornetsecurity is building a safer digital future and sustainable security cultures with its award-winning portfolio. Hornetsecurity operates in more than 120 countries through its international distribution network of 12,000+ channel partners and MSPs. Its premium services are used by more than 75,000 customers.

Angelica Micallef Trigona

Hornetsecurity  
+356 2032 3461  
[email us here](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/714996367>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.