knowbe4

Navigating Cyber Threats

Infosecurity Europe 2025 Findings

WWW.KNOWBE4.COM

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | Email: Sales@KnowBe4.com

Infosecurity Europe 2025 Findings

KnowBe4 once again attended the Infosecurity Europe 2025 conference. Beyond the networking opportunities, the conference served as a great setting for KnowBe4 to gauge the current sentiment within the cybersecurity industry. To do this, we conducted a survey to understand the issues that are top of mind for security professionals.

Over the three days, we spoke to and surveyed over 100 security professionals, of which the majority (43%) were from organisations over 1,000 employees.

The survey findings show that phishing attacks continue to be the dominant cybersecurity threat, with impersonation tactics proving especially effective. The findings also highlight a notable disconnect between the human element and technical solutions within cybersecurity, with employee behaviour remaining the primary vulnerability.

Organisations are responding with increased investment into their cybersecurity efforts, though there are potential gaps in strategic allocation thereof. The emergence of AI-enhanced cyber threats adds new dimensions to an already complex cybersecurity environment, which requires thoughtful preparation and response.

Impersonation:

Everyone Wants To Be Your Boss

The survey findings paint a clear picture: phishing remains the most significant cybersecurity threat facing organisations today. An overwhelming 74% of respondents identified phishing attacks as their greatest threat over the past 12 months, more than double the next most common threat—social engineering via social media platforms such as LinkedIn (30%).

When we asked which was the most frequently encountered tactic, almost half of respondents cited impersonation of senior leadership or trusted contacts. Tactics using malicious links or attachments followed at 37.8%. Despite growing concerns about advanced technologies, only 10.8% of respondents reported deepfakes or AI-generated content as their most frequent threat.

The persistence of phishing as the dominant threat vector suggests that cybercriminals continue to find success with these tried and tested approaches versus more advanced tactics such as deepfakes. Criminals are still finding success in the basics by pretending to be people we trust. It's like they've realised it's easier to borrow authority than to hack it.

Distracted Minds, Not Sophisticated Threats:

Where Cybersecurity Danger Truly Lies

Perhaps the most revealing finding concerns why employees fall victim to cyberattacks. Distraction (43.2%) and lack of security awareness training (41.4%) emerged as the primary factors, with only 17.1% of respondents attributing successful cyberattacks to the sophistication of the threats themselves.

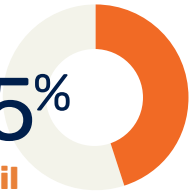
This statistic challenges the narrative that today's threats are simply too advanced to defend against. Instead, it points to human vulnerabilities that technical controls alone cannot address.

What do you believe are the primary reasons employees fall victim to cyberattacks in your organisation?

In a 2023 KnowBe4 survey report, TAPPED OUT, we examined how stress and distraction in the workplace lead to less secure cultures, posing immense cyber risks to organisations. Two years on, it still seems to be a problem. The modern work environment, characterised by multitasking, rapid communication, and information overload, creates ideal conditions for cybersecurity lapses. Organisations must recognise that security awareness is not merely about knowledge transfer - it is about creating a culture where vigilant behaviour becomes natural even under pressure and distraction.

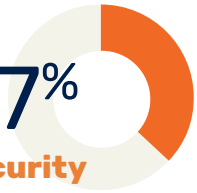
Cybersecurity Investment

The survey results reveal encouraging trends with regards to increasing cybersecurity budgets, with 65% of organisations planning to increase their cybersecurity spending (23% significantly, 42% slightly). Only 4% anticipate decreasing their budgets, while 24% expect spending to remain the same.

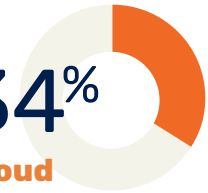


45%
Email security

Specific investment priorities for the coming year:

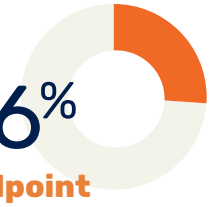


37%
Security Awareness Training

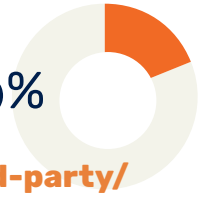


34%
Cloud security

26%
AI-based threat detection systems



26%
Endpoint protection



19%
Third-party/ vendor risk management

20%
Identity and Access Management

Interestingly, this pattern partially aligns with what respondents believe would be most effective in reducing successful cyberattacks.

These investment priorities reflect a growing understanding that effective security requires a harmonious blend of technical controls and human capabilities. With email security and security awareness training leading the investment priorities, organisations are clearly recognising the interconnected nature of technical and human risk. This aligns well with a Human Risk Management (HRM) approach, where defensive controls work alongside user education and empowerment to create a comprehensive security posture.

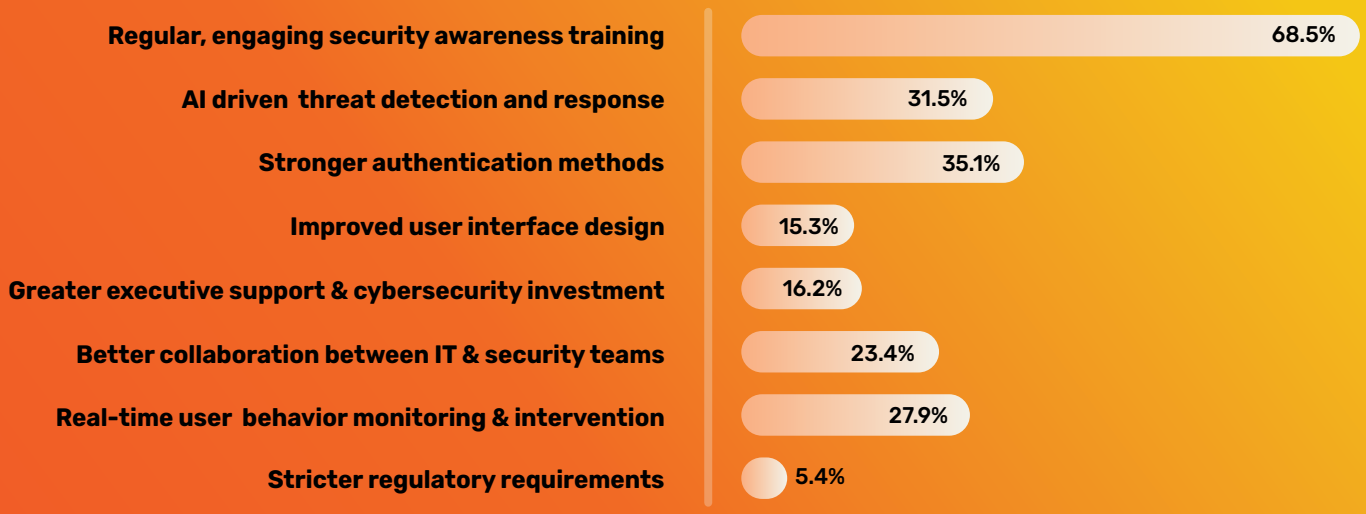
The significant investment in cloud security and AI-based detection systems further supports this holistic strategy, providing the technical foundation needed to protect users while enabling them to work securely. Organisations appear to be moving away from viewing technology and human factors as separate challenges, instead adopting a more integrated approach to managing security risks.

69%
Cited regular and engaging security awareness training

35%
Identified stronger authentication methods like Multi-Factor Authentication (MFA)

32%
Pointed to AI-driven threat detection and response tools

What do you believe would have the greatest impact in reducing successful cyberattacks on end users?



The gap between perceived effectiveness and planned investment in AI-driven security tools (31.5% vs. 26%) suggests either budget constraints, implementation challenges, or uncertainty about these new technologies. Organisations should carefully examine whether their investment priorities align with their security needs rather than following industry trends.

The AI Challenge

Looking towards future threats, 60% of respondents expressed greatest concern about AI-generated phishing and deepfakes, followed by ransomware (48%) and shadow IT or unsanctioned AI tools (42%).

This concern about AI-powered threats appears somewhat disconnected from current experience, where only 11% reported AI-generated content as their most frequently encountered threat. This suggests organisations are anticipating a significant evolution in threat tactics rather than responding to current conditions.

It's like preparing for a hurricane while still dealing with daily rain - organisations know the big storm is coming. While today's threats still mainly involve someone pretending to be the CEO asking for gift cards, security teams are bracing for a future where that "CEO" might video call you with a perfectly cloned voice and face. The gap between current reality (11%) and future concerns (60%) shows that security teams are strategically anticipating future cyber threats rather than focusing solely on immediate threats. The question is: are we preparing for tomorrow's threats while still leaving the umbrella at home today?

Organisations have a window to prepare for the anticipated wave of sophisticated AI threats before they become prevalent. This preparation should include both technological defenses and human risk management for recognising increasingly convincing deceptions.

Business Impacts

Organisations that experienced successful cyberattacks during the last 12 months reported an array of business impacts:

23%
Suffered operational downtime

19%
Experienced data loss

14%
Incurred financial losses

12%
Faced reputational damage

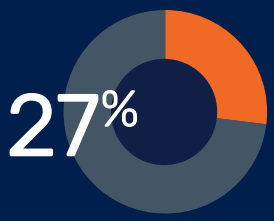
11%
Reported loss of customer trust

While operational disruptions create immediate visible disruption, the long-term damage to reputation and customer trust may ultimately prove more costly. These impacts often receive less attention in cybersecurity planning but can fundamentally undermine an organisation's market position and growth trajectory.

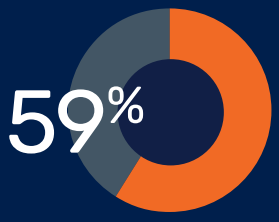
The diversity of impacts underscores the need for comprehensive resilience planning beyond simple technical recovery. Organisations should develop specific response strategies for each category of impact, including communication plans for managing reputational damage and customer relationship recovery.

The Confidence Gap

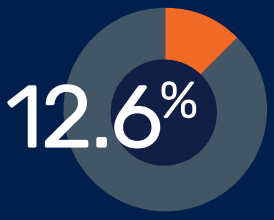
Perhaps most concerning is what our findings reveal about organisational confidence. Despite the prevalence of successful cyberattacks and vulnerabilities, confidence in cybersecurity capabilities remains remarkably high:



27% **Feel very confident in their ability to respond effectively to cyberattacks**



59% **Feel somewhat confident**

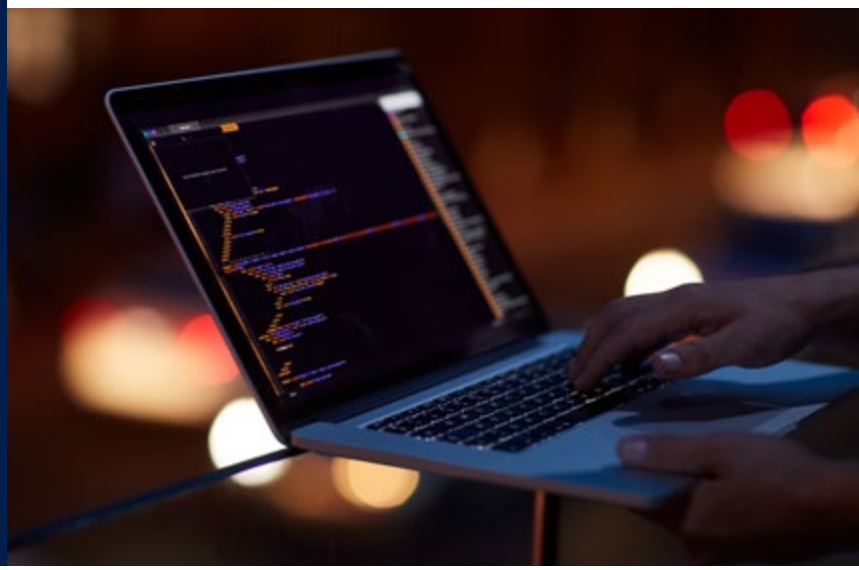


12.6% **Express low or no confidence**

This high confidence stands in contrast to the reality of successful attacks and known human vulnerabilities within organisations.

Earlier this year, we conducted a global survey, Security Approaches Around the Globe: The Confidence Gap, which showed that 86% of employees believed that they could confidently identify a phishing email. However, as we delved deeper into the numbers, a troubling paradox emerged - confidence does not always translate to competence.

This confidence paradox represents a significant risk in itself. Organisations that overestimate their cybersecurity capabilities may under invest in necessary improvements or fail to implement appropriate safeguards. Security leaders should implement objective assessment mechanisms that challenge internal confidence with external validation.



Moving Forward: Actions to Take

To navigate the complex and evolving cybersecurity landscape, organisations must adopt a proactive and multi-faceted approach. The following recommendations outline key strategies for strengthening security posture, preparing for future threats, and building a more resilient cybersecurity culture.

Embrace Human Risk Management:
Deploy a unified platform that combines technical controls with human-centric security

Strengthen Core Security:
Implement non-phishable MFA such as FIDO, email security, and Zero Trust as baseline controls

Prepare for AI Threats:
Develop capabilities to detect and respond to AI-enhanced attacks while managing AI tool usage

Build Organisational Resilience:
Create and regularly test incident response plans that address both technical and reputational impacts

Bridge the Confidence Gap:
Replace assumptions with metrics through regular third-party assessments and realistic testing

Future-Proof Your Security:
Invest in adaptable security programmes that can evolve with emerging threats

Address Digital Distraction:
Implement mindfulness practices and create environments that support focused security decisions

Conclusion

The findings reveal both persistent challenges and emerging threats in the cybersecurity landscape.
While phishing and human vulnerability continue to dominate current concerns, the anticipated rise of AI-enhanced threats suggests a coming evolution that will test even mature security programmes.

The most successful organisations will be those that recognise the fundamental human nature of the cybersecurity challenge. Technical controls remain essential, but insufficient without paying attention to how humans interact with systems, process information, and make security decisions under real-world conditions.

By addressing the confidence gap and aligning budgets with actual threat patterns, organisations can build resilient cybersecurity programmes capable of withstanding both today's challenges and tomorrow's emerging threats.

About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk.

For more information, please visit www.KnowBe4.com

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

knowbe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com