KnowBe4

Infosecurity Europe 2024 Survey Findings

Part 3

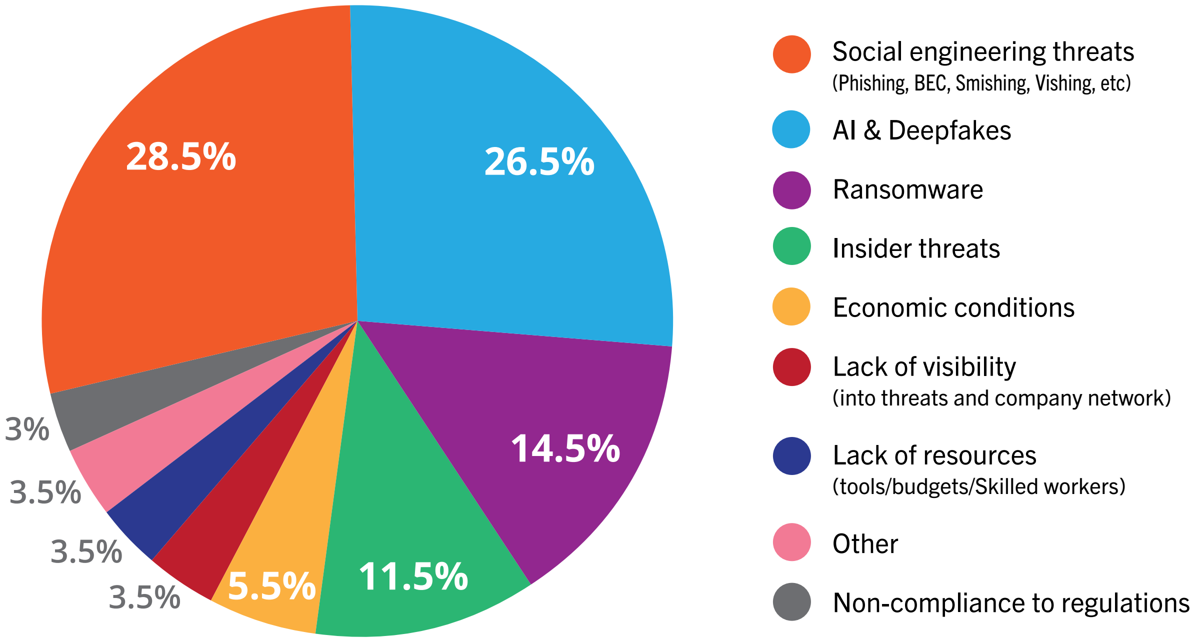
KNOWBE4 INFOSECURITY EUROPE 2024 SURVEY FINDINGS PART 3

Whilst attending another fantastic instalment of Infosecurity Europe this year, we conducted a survey to gain a better understanding of the cybersecurity issues faced by over 200 security professionals that attended the three-day conference this year.

In this third and final findings in the series, we will take a deep dive into the growing dangers of AI use in the workplace and how responsibly it is used by employees.

The survey's findings showed that over one-quarter (27%) of security professionals perceive AI and deepfakes to be the biggest cybersecurity risk to their organisations. However, the findings also show that almost one-third (31%) of respondents don't have 'responsible use' policies for AI in place and have no intention of implementing one in the near future. There is a clear disconnect between the leading concerns of security professionals and the policies that they have in place, resulting in a higher chance of suffering a breach.

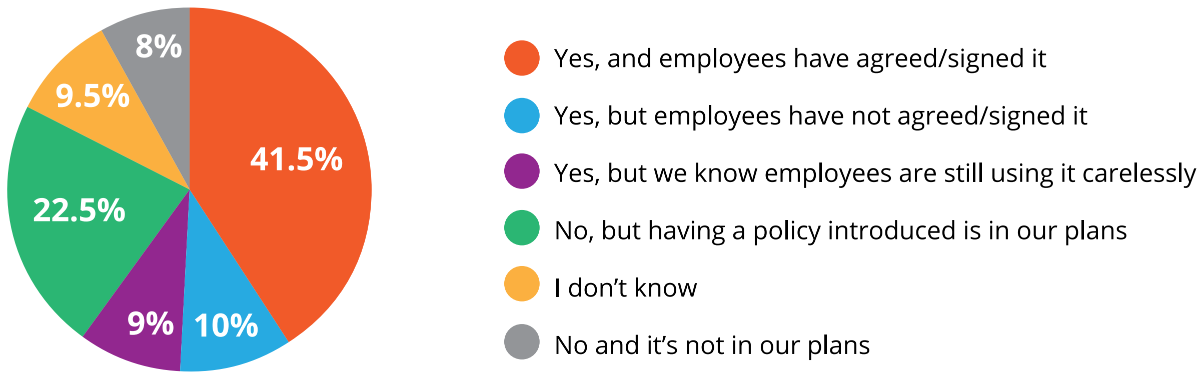
What do you perceive as the biggest cybersecurity risk to your organisation currently?



AI and deepfakes are becoming common tools used by cybercriminals, usually in social engineering campaigns to gain access to a user's computer or personal information. As more employees use AI at work and incorporate it with business systems, it is imperative that organisations establish clear guidelines on how to appropriately use this technology.

Equally concerning, the survey revealed that one in ten security professionals have 'responsible use' policies on using Generative AI (GenAI) but their employees have not agreed or signed it, with a further 9% saying that employees have signed the policy but still use GenAI carelessly.

Do you have a “responsible use” policy on using Gen-AI within your company?



The results of this survey show that despite understanding the increased threat AI is posing, security professionals aren’t doing enough to protect themselves from potential threats. Allowing employees to use and integrate AI at work isn’t sustainable and ‘responsible use’ policies are vital to reduce the threat of cyberattacks. It is imperative that once these policies are implemented, checks are put in place enforcing employees to use AI responsibly.

As AI continues to develop, organisations must invest in secure cyber defences to reduce the risk of breaches. It is equally vital to encourage a security culture where employees are trained on the importance of cybersecurity and how to avoid making mistakes in the future.

The results of the survey indicate that security professionals aren’t taking the risks behind AI seriously despite understanding the risks and witnessing the consequences. It is the responsibility of these security professionals to design systems and processes that reduce the chance of risky behaviours and promote safe and secure actions within the workplace.

To view part 1 and part 2, click here:

PART 1 →

Biggest Frustrations Felt By Security Professionals

PART 2 →

Risky Security Behaviours at Work

Additional Resources

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

About KnowBe4

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 65,000 organisations around the globe. Founded by IT and data security specialist Stu Sjouwerman, 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 to awareness training on security.

The late Kevin Mitnick, who was an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as their last line of defense and trust the KnowBe4 platform to strengthen their security culture and reduce human risk.

For more information, please visit www.KnowBe4.com

KnowBe4

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