KnowBe4

Infosecurity Europe 2024 Survey Findings

Part 1

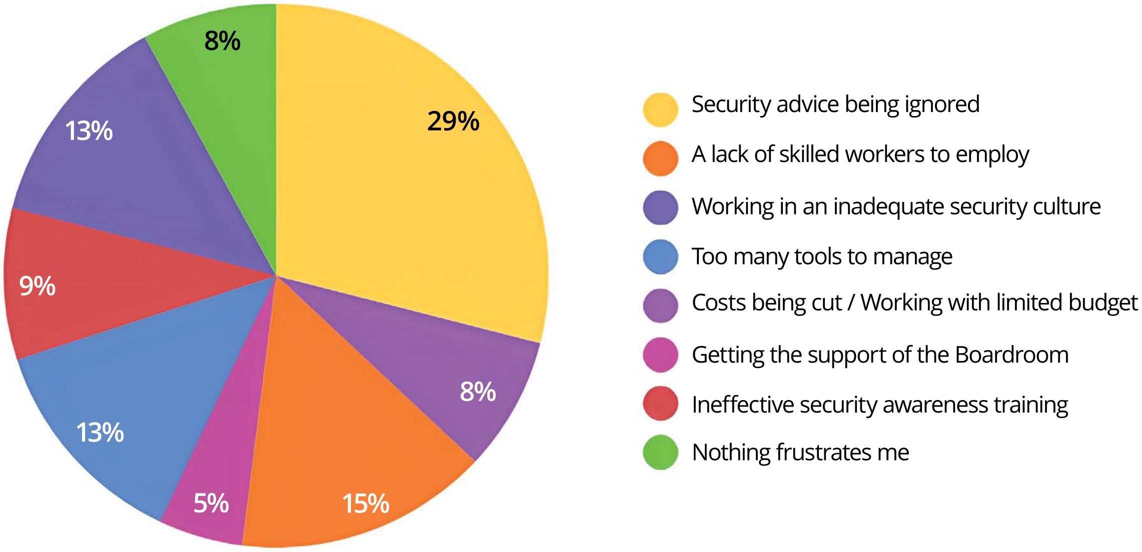
KNOWBE4 INFOSECURITY EUROPE 2024 SURVEY FINDINGS PART 1

KnowBe4 attends Infosecurity Europe every year, and this year was no different. While the conference offers great networking opportunities, it also provides a great setting for KnowBe4 to get a sense of how the industry is feeling at present, and thus we conducted a survey to get a finger on the pulse of certain cybersecurity issues which are top of mind for security professionals.

Across the three days, we spoke to and surveyed over 200 security professionals, of which the majority (47%) were from organisations of over 1,000 employees. Of these, 18% identified as CISO or head of cybersecurity while most of the respondents (28%) were security professionals or in another technical role.

A recurring theme that emerges from the survey results is the frustration felt by many security professionals due to their advice being ignored (29%) and working in an inadequate security culture/environment (13%). This highlights the importance of fostering a robust security culture within organisations, where cybersecurity is viewed as a shared responsibility rather than the sole responsibility of the IT department.

What frustrates you (if anything) the most as a security professional?



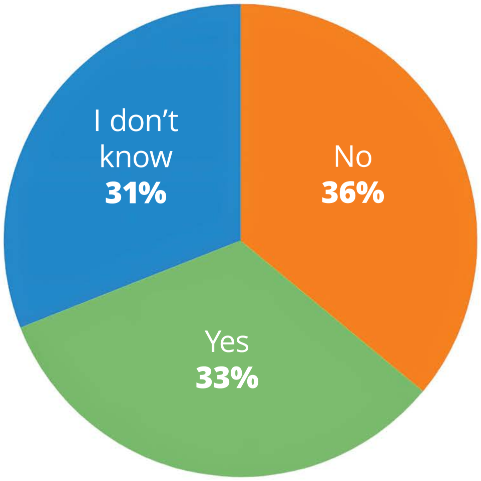
Whilst these frustrations are entirely valid, it raises the question as to what factors contribute to the ineffectiveness of security awareness training, and why organisations continue to rely on it. From a practical standpoint, the answer often lies in organisations going through the motions of a tick-box compliance exercise to appease an auditor.

It is clear that organisations must shift away from the antiquated once-a-year training model, where they inundate employees with an overwhelming amount of information over an hour or more in a bid to complete the training. Instead, newer, more user-friendly approaches should be adopted.

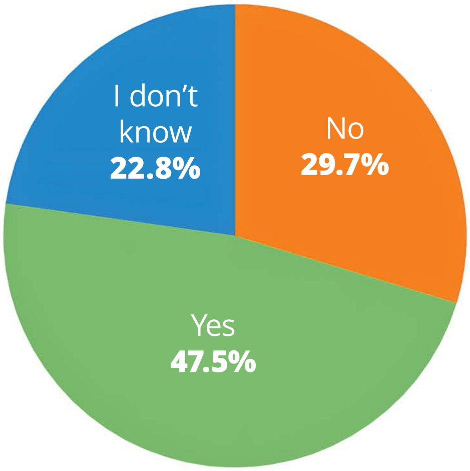
Finding a training style that resonates with users, incorporating elements of comedy or drama, and keeping sessions concise and impactful can make a significant difference. Furthermore, organisations can leverage short, timely interventions, such as nudges, which can prove to be incredibly powerful in promoting security awareness and fostering a culture of cybersecurity vigilance.

The survey results have also shed light on a fascinating dichotomy in opinions regarding the potential reintroduction of National Service and the inclusion of cybersecurity education within its framework. Interestingly, the respondents found themselves evenly split on the matter, with 48% expressing support for the idea of National Service incorporating cybersecurity education, while an equal proportion remained either unsure or opposed to the concept.

Would you support the reintroduction of National Service?



Would you support the reintroduction of National Service if it included cybersecurity education?



This division in perspectives shines a spotlight on the complex nature of the issue at hand. There appears to be a growing recognition of the pressing need to broaden the scope of cybersecurity education and equip individuals with the necessary skills to navigate an increasingly digital landscape. The fact that nearly half of the respondents favoured the integration of cybersecurity education into National Service suggests that there is a significant appetite for such an initiative.

However, the equal proportion of those who were either unsure or opposed to the idea serves as a reminder that the specific approach of leveraging National Service as a vehicle for cybersecurity education remains a contentious point. This hesitation may stem from concerns about the effectiveness of such a programme, the potential impact on individual liberties, or the practicalities of implementation.

Ultimately, the divided opinions revealed by this survey serve as a valuable reminder that there is no one-size-fits-all solution to the complex challenge of cybersecurity education. It is only through ongoing discussion, experimentation, and adaptation that we can hope to develop a comprehensive approach that equips our citizens with the knowledge and skills they need to thrive in an increasingly digital world.

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