FMBusinessDaily

Security Awareness Training is not Alleviating Breach Risk, New Survey Finds

10 months ago

Leading Human Risk Management Platform, CultureAI, has unveiled new research that revealed companies are pouring an increasing number of resources into their security awareness and training (SA&T) programmes. 96% of respondents allocate between 5% to 20% of their security budgets to awareness training. While 78% train employees at least monthly. Yet, it was found that human-related breaches are still happening at an alarming rate.

Surveyed organisations said the leading motivation for delivering training is to change behaviours and equip employees to handle risks (51%), followed by compliance (25%) and breach prevention (24%). But regardless of the objective behind the training, 79% of surveyed organisations suffered a cyber breach due to human error in the last 12 months, with 34% experiencing multiple breaches.

The study was conducted by independent research company, Opinion Matters, and surveyed 200 UK-based cyber security teams at organisations with over 1000 employees. This forms the basis for CultureAI's 'Time to Adapt: The State of Human Risk Management in 2024' report which examines how far training can go in improving behaviours and reducing risks, evaluating whether investments of time and money offer substantial returns or if resources could be more effectively allocated elsewhere.

Human risk demands attention, and training alone isn't enough

Employees face an increasing range and volume of risks as they go about their daily tasks; with the widespread and increasing adoption of SaaS, GenAI, and collaboration tools creating more vulnerabilities for cyber criminals to exploit. As the threat landscape evolves, so must defences.

Despite significant investments in training, human-related breaches remain commonplace. 79% of

organisations reported having at least one breach, whether they trained twice a week, or once a month. While training is required for compliance reasons, the findings suggest that spending extra time, resources, and customisation on training, will not necessarily deliver the results hoped for.

Organisations need to take a proactive stance, embracing innovative interventions and technologies that help accurately quantify and manage the risks caused by and affecting employees.

Security teams are driving down risk with human risk management

Companies are beginning to adopt HRM solutions at scale. With 94% of surveyed organisations using at least one HRM capability. Yet there is still room for growth, as only 22% of respondents were using three or more different capabilities.

There is a notable correlation between the number of HRM capabilities utilised and the incidence of human factor-related breaches over the past year. Specifically, 91% of organisations with only one capability experienced a breach, compared to 70% of those employing four.

When examining the respondents who reported no data breaches, the research found a preference for more technical HRM capabilities. The most popular choices were human risk triage (45%), coaching based on risk levels (37%), nudges triggered by risks (37%), and automated interventions (32%).

Shifting investment from SA&T to HRM

63% of respondents currently spend 5% to 10% of their security budget on training with another 33% reporting that they spend 11% to 20%. This is more than anticipated, as in 2023 Gartner reported 60% of teams spend 5% or less on awareness activities, including people, processes and technology1.

However, among those spending 11 to 20% on training, 80% experienced a security breach in the past year. This suggests that allocating up to 20% of the budget to training alone might be a missed opportunity. While training has a place, it has limits. Instead of investing in single-focus platforms, it could be better to invest in a more comprehensive HRM platform. Leveraging data from a range of technology and security tools, to provide real-time visibility into potential risks and automate risk response.

John Scott, Lead Security Researcher at CultureAI, comments on the survey findings: “Human error is inevitable, but it’s not a moral failing. We all make mistakes. Unfortunately, these mistakes can be catastrophic for organisations. It’s a challenge that every business must grapple with, and the research serves to demonstrate the prevalence of human-related breaches, even as companies invest more time and resources into security awareness and training programmes.”

“Training can go some way to address gaps in knowledge, but cyber criminals exploit gaps in attention and perception to achieve their goals. Effective use of technical interventions and nudges can help close those gaps. But human risk management isn’t just a shift in technology, it’s a complete change of mindset, and one that is desperately needed. Enabling companies to adapt to the new normal.”

To read the full research report, please click here.