Changing the human conversation

Effective enterprise security relies on culture, not just IT.

Anna Collard, managing director of Popcorn Training

Hack the human. This is a growing trend understood very clearly by the well-funded and organised cybercrime landscape. The cyber-syndicate and criminal know that it is far easier to access systems through people than it is to go through the technology.

According to security software company Trend Micro, a staggering 91% of successful breaches started with attacks that were focused on the weakest link in the security chain - people. The human factor is what allows for the opportunistic phishing attack, extortion scheme, or clicking of an unfortunate attachment, but it is also one that requires that the enterprise transform its security culture to ensure ongoing education and understanding.

“The attack vectors aimed at people are becoming incredibly sophisticated,” explains Anna Collard, managing Director of Popcorn Training, a KnowBe4 Company. “The cybercriminals can spoof people’s email addresses, use voice recordings to instruct people to do things under the guise of being an employer or decision-maker, and unleash extortion schemes that can defraud people of large sums of money. The human factor has become very important to the security of the organisation and yet security education is still a begrudging project often dumped with IT.”

A significant number of successful cyberattacks are from people making mistakes that could be avoided if they understood the risks and the warning signs. It's easy for those with inherent security understanding – the decision-maker, the IT department, the chief security officer – to assume that the average employee can recognise a threat, but the truth is that they often can't. A sophisticated phishing message can catch anyone off guard, from a physician to a retail executive to a technically savvy millennial.

Relook at security culture

"A lot of companies assume that the millennials, the so-called digital natives, are security savvy and more aware of the risks than the older generation but this isn't the case at all," says Collard. "They know how to use the technology, but they don't care as much about the threats. This ties into how certain behaviours can impact on a company's security culture and posture. Even if a security education campaign is run successfully, the challenge is that people will still behave in certain ways and it is this behaviour that needs to be addressed when transforming a security culture."

Human beings are creatures of habit and can adapt to two to three new behaviours a year, if at all. To achieve a security culture that educates around the principles of risk and the understanding of threats, then the training process has to be steady, relevant and repeatable. It can't be rolled out in volume with a new session every month as this only results in cognitive overload.

"It's the analogy of – if I throw one or two balls at you, you will likely catch both, but if I throw ten at you, you won't catch any of them," says Collard. "To ensure that security message sticks you need to select a few key messages for each year and drive these throughout. It's also important to include varied methodologies into the training to ensure that the lessons are heard, learned and understood."

Security training is needed

Collard advises the inclusion of gamification and stories to create security training solutions that are memorable. Through the use of anecdotal evidence, employees can see how the risks directly affect them and the business, can understand what to look out for, and can develop a clear understanding of the company's security requirements and regulations.

"The goal isn't to turn every person in your company into a security specialist but to rather give them the level of understanding they need to apply the rules and remain secure," concludes Collard. "People need to understand that if they use technology, they have to be cognisant of the risks. Organisations can support this understanding by investing into training that's relevant, targeted and memorable. Training that can sustainably transform the company's security culture."