BIZCOMMUNITY

Cybersecurity awareness is no longer a generic exercise for business

By Simeon Tassev

7 Feb 2023

Ransomware and phishing remain the top two cyber threats today, a fact that many different studies will attest to, and often, human error is to blame for successful breaches. Cybersecurity awareness training has become essential for business, but it is often an exercise that is not given sufficient attention because the liability for a breach has been limited.

Source: Unsplash

However, recently a new precedent has been set, with ENSafrica being ordered to pay R5.5m and legal fees to an individual who lost money due to a manipulated email from the firm. As cybercrime incidents continue to rise, ignorance can no longer be used as a valid excuse, and businesses need to implement specific, tailored, and effective cybersecurity awareness training to safeguard themselves in the future.

The ENSafrica case

In the case of ENSafrica, a leading law firm in South Africa, the High Court found the firm liable for money which was stolen as a result of manipulated emails showing incorrect banking details. This is a very common scam known as business email compromise (BEC) and in the past, these types of cases generally held limited liability for business. However, with the judge finding in favour of the plaintiff, awarding the law firm to pay her the R5.5 million plus interest and legal fees, a new precedent has been set.

The plaintiff's argument centred on the fact that ENSafrica owed her a duty of care, and a legal responsibility to warn her of the dangers of BEC, and that they should have made use of secure channels to send banking details, rather than unencrypted channels and unsecured PDFs. It also emerged during the trial that cybersecurity training was inadequate at the firm, despite the growing threat landscape. Essentially, the plaintiff won the case because the firm did not have the right policies or procedures in place. This highlights the need for greater awareness and training on cybersecurity for business.

Ignorance is not an excuse

The entire case comes down to the fact that all reputable companies should know and do better. The false belief that breaches of this nature are not a business' problem has now been shaken because there is a legal precedent showing that they are. In today's threat landscape, especially with the implementation of the Protection of Personal Information Act (PoPIA), privileged communication should always be protected and encrypted, and awareness of the risks and how to mitigate them needs to become a priority.

This also cannot be a generic exercise, because there are specific potential risks and scenarios that will apply to different businesses. An individualised risk assessment is essential, as is developing a playbook on how to deal with potential threats. Knowing the risks, planning the response and having processes in place to deal with threats is imperative.

Perks of expert assistance

Knowing and planning are not enough unless all staff are also aware of and trained on the risks and the procedures to follow. This is not just about phishing scams anymore – training needs to be focused and relevant and put into context, so that people can understand real-world examples and consequences of a cyber breach. In addition, businesses need to perform simulations and penetration testing to see whether or not their approach is working.

This is typically not a core skill for most businesses, which is where an expert outsourced provider can assist. A cybersecurity expert can assess risk, compile a complete training plan covering all components, and implement measurements to test these, as well as tailor training to individuals depending on their role and risk.

With cybercrime continually on the rise, and businesses now being potentially liable for the financial losses of clients as a result of breaches, the importance of cybersecurity awareness has never been more evident. A focused, specific, and effective approach is essential in ensuring organisations play their part in protecting against cyberattacks.

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa

- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...