BIZCOMMUNITY

4 ways to manage the human threat to cybersecurity

By Carey van Vlaanderen

18 Jul 2023

Two out of every five responses to a 2022 cybersecurity survey admitted to having made mistakes at work that compromised cybersecurity. That same Tessian report also claims that 85% of data breaches are caused by human error.

High pressure modern business environment. Source: Fauxels/Pexels

Whether it's recycling passwords, a company laptop being stolen or lost with confidential client information, or intentionally overriding company security policies - humans are the biggest threat in the cybersecurity space. Chief security officers, chief information officers (CIOs)
and individuals in similar positions of responsibility spend a lot of their time worrying not about technology, but about people.

Humans make mistakes. These mistakes range from failure to properly delete data from devices to preventable errors like clicking on links in phishing emails, to misconfigured network devices and servers. Humans are also capable of negligence, unfortunately.

How 3 South African entrepreneurs are using blockchain to drive financial inclusion

5 Jan 2023

Data leaks that arise because of human error, such as failure to update security patches or correctly configure servers with known vulnerabilities, are on the rise and now occur almost as frequently as direct security attacks. Then there's insider threats, which are unimaginably difficult to detect. From malicious employees, or an employee whose credentials have been compromised, all of these vulnerabilities share a common root: humans.

Managing human risk from the inside

An effective programme for managing human risk involves several key components. These include providing regular training and increasing employee awareness, establishing clear policies and procedures, maintaining efficient communication channels, developing plans to respond to security incidents, and conducting regular security assessments

to identify and minimise potential risks.

Other necessary steps include implementing robust access controls, monitoring network activity, reviewing and updating security policies while fostering a culture that prioritises security. Cybersecurity awareness and training work hand-in-hand to address the human element of risk in a number of ways:

1. Prevention of human error: Awareness and training can help employees understand their role in maintaining security integrity and avoid common mistakes that can lead to breaches. For example, they can learn how to create strong passwords, how to identify phishing emails, and how to properly handle sensitive data.

2. Early detection: Cybersecurity awareness and training can teach employees how to recognise and report suspicious activity. This can help identify security incidents early, allowing for a quicker response and minimising the impact of an attack.

3. Improved incident response: Employees who have received cybersecurity training are more likely to know how to respond to security incidents by following established procedures and protocols to minimise the damage caused by an attack.

4. Creating a culture of security: Cybersecurity awareness and training can help create a culture of security within the enterprise. When employees understand the importance of security and their role in maintaining it, they are more likely to take it seriously and make it a priority.

Focusing on managing human risk and security training requires strong leadership from within. Leadership commitment is a key ingredient in achieving the organisational momentum needed to create an ongoing culture of learning and growth. With executive buy-in, sustained investment is possible in the necessary training and development resources such as courses, workshops and mentorship programs.

Balancing security training and production

With the increasing tech talent shortage in Africa, CIOs are scrambling to ensure that employees brush up on skills and technologies that facilitate business agility and resilience, with cybersecurity knowledge topping the list, despite competing priorities.

Training and upskilling needs to be a deliberate exercise, but small teams are often vulnerable to the delivery pressure created by the current needs of the business.

This means that critical training (such as cybersecurity training) takes second place behind current projects, which results in a short-term productivity gain at the expense of long-term skills progress. Creating a balance of short-term project delivery and upskilling/training as outputs to current projects is essential.

Constant vigilance and continuous learning

By providing regular cybersecurity training and increasing employee awareness, organisations can prevent human errors, detect incidents early, improve incident response, and create a deep culture of security.

As cyber threats increase in complexity and frequency, investing in security skills training is a critical step towards ensuring the protection of people, assets and data from threats, both internal and external.

ABOUT CAREY VAN VLAANDEREN

Carey van Vlaanderen is CEO of ESET Southern Africa. ESET is a global provider of security software for enterprises and consumers and is dedicated to delivering instant, comprehensive protection against evolving computer security threats.

- 4 ways to manage the human threat to cybersecurity - 18 Jul 2023
- A cybercriminal's tricks and trades to get into your phone - 23 Mar 2018
- What is encryption, how does it work and why is it important? - 6 Mar 2017
- Five common security threats that demand attention - 9 Mar 2016
- Face 2016 with a proactive attitude of security awareness - 22 Jan 2016

View my profile and articles...