How to create a cybersecurity culture

By Simeon Tassev

16 Jan 2019

'Cybersecurity' is still a relatively new word, making its first appearance to reference "protecting a computer or computer system" in 1989. Since then, the term has evolved to incorporate every aspect of IT, information and cybersecurity.

Simeon Tassev, managing director and qualified security assessor at Galix Networking

As networks have expanded from local to wide, to the world, so too has the need to protect against threats. However, hacks and cybercrime still happen every day - not just because of the rate at which cybercriminals are keeping pace with technology, but also because users aren't quite keeping pace with either cybercrime or technology.

While IT professionals understand the risks and know of the many threats that linger outside of unprotected networks, most of the people who actually use the systems, devices, networks and Internet aren't quite as mindful – or aware – of cybercrime and security. Businesses looking to properly safeguard their IT environments need to ensure that their staff, who operate within this environment, know what the risks are and how to prevent them.

Security starts at home

Many people who work in an environment where they come into contact with IT are vaguely aware of the “annoying” protocols and firewalls that the business puts in place on devices and systems used. However, very few technology users apply any security to their personal devices and applications.

Luckily, most social media and other technology application vendors have put their own security measures into place, such as two-factor authentications (where, for example, a web site prompts users for their username and password as well as one-time password PIN to verify their identity.)

Blurred lines

An organisation may have a better understanding of the risks, however, the lines between personal and business life have blurred. Users’ lack of awareness may spill over from personal to business life, impacting the business’s potential risk. Most people use their own smartphones within their work IT environment with other devices such as laptops and even wearable devices connecting to business networks.

Every device that enters a business’s IT environment is a potential door through which a hacker can penetrate the business. Despite the best boundary protection, the business needs to be able to control all points of entry that appears in their environment. But, how can businesses achieve this when user behaviour is such a variable, and people are constantly “opening new doors”?

Creating a security culture

In a world where everyone uses technology and where technology enables the business through user functionality, cybersecurity should not be just an IT concern; it should be everyone’s concern. Unfortunately, businesses cannot ensure that people are security minded at home, but they can educate their staff on the risks and create a culture where security colours every aspect of a business.

New short course teaches you how to think like a cybersecurity expert

Enterprises University of Pretoria 8 Jan 2019

There are a few steps businesses can take to create a security culture that extends beyond simply planning and implementing controls:

- **Assess the risks**
  This needs to be a collaborative exercise between the business, information security and operational security, and should also include the relevant legislation and liability officers. Risk varies from business to business, and each department plays a vital role in understanding not just the risks, but their impact.

- **Prioritise**
  A business shouldn’t invest more in security than its data is worth. It’s paramount to focus on critical areas first and

work outwards from there.

- **Awareness**
  The business should ensure its staff is constantly made aware of the risks, new threats, the potential for damage (both personal and to the business) and what users can and should do every day to protect themselves. This should become an entrenched practice; almost second nature.

- **Training**
  This should be provided as regularly as possible to back up and underpin the awareness and should encompass both how to prevent attacks as well as what to do in the event of a breach.

- **Legislation awareness**
  Part of the training of risks and security controls should include awareness of data security legislation and the impact on individuals as well as the business. This helps users understand what they are protecting within a business but also helps them to understand their rights when it comes to their own data.

- **Incident management**

  Incident management and cybersecurity incident management are two different albeit related things. Businesses should review, test and update their incident management process often, ensuring they cover all their bases so that everyone in the business understands what to do and their role in the event of an incident.

Despite controls put into place by the business, users still wield their smartphones and personal laptops with very little thought to the potential threats they are exposed to and, when they are hacked, they're often disbelieving and surprised.

It's important for anyone using technology at any level to educate themselves on the risks of cybercrime and how to avoid incidents such as identity theft and fraud.

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...

For more, visit: https://www.bizcommunity.com