Cyber threats are becoming all-too-real for businesses

By Byron Clatterbuck

10 Jan 2019

The promise of enhanced business performance in practically every area - from cost-cutting to employee productivity and customer service - has business owners around the world embarking on the journey of digital transformation in bigger and bigger numbers every year. And South Africa is no exception.

Byron Clatterbuck, CEO at SEACOM

Around half of South African organisations are already well on their way to reaping the benefits of digital transformation, aided in large part by cloud computing and the easy access to a multitude of cloud-delivered products and services that it enables. But in this increasingly interconnected landscape, the risks of cybercrime are naturally rising as well, and this is one occurrence for which most South African organisations are worryingly unprepared.

A number of high-profile hacks and data breaches in South Africa have thrown this vulnerability into sharp focus in recent years. Each year these attacks become bigger, more severe, and more costly to recover from. And to complicate things even further, new technologies and devices mean new vulnerabilities and rapidly shifting goal-posts for those mandated to champion digital security within an organisation.

Realistically, there's only so much a service provider can do to protect a business. It is internal policies and the practices enforced on a daily basis in the workplace that offer the highest level of defence, and so it is up to each individual business owner to make sure that every weak link is strengthened.

In this endeavour, four key areas must be secured to minimise the risks and maximise the rewards of digital business transformation.

- **People**

No matter what firewalls you have in place, a fact unchanged since the dawn of cybercrime is that human error on the part of well-meaning employees is usually to blame for breaches. There is no technology that can take the place of simple training and education, and these must be the basis of any solid cybersecurity strategy.

Human error: the main cause of data breaches

Drew van Vuuren 4 Sep 2018

Phishing and whaling attacks, malware, and a host of other destructive threats are most commonly passed on through email, and educating employees about simple best-practices regarding suspicious emails and links can often be the best – and simplest – way to stay safe.

- ## Endpoints

In the age of the cloud, and with more and more businesses embracing the advantages of remote workplace policies, every device that enters and exits your business's premises, and makes use of its network, is a potential entry point for would-be cyberattacks. Securing every endpoint, from smartphones to tablets and laptops, should be a key priority in keeping sensitive business information protected.

- ## Connection

It's the lifeline of any digitally-enabled business – so why, then, do so many businesses neglect the simple necessity of securing the internet connection that their employees use every day? A strong password policy, a fool-proof firewall, configuring office Wi-Fi for separate public and private access, and even reconsidering the physical placement of routers can all help to ensure that your Internet connection is better protected from intrusion.

- ## Backups

The importance of backing up your business data cannot be overstated. Most organisations are still of the opinion that backups are a grudge purchase, and these are the same organisations that quickly fall into line once the safety of their data has been compromised. Can your business afford the delays caused by the loss of customer invoices, purchase orders and payroll records? Can it afford the stiff penalties it faces if it turns out that your backup practices are not compliant with POPIA and GDPR?

Best practices to ensure an effective data backup strategy

Chris de Bruyn 6 Dec 2018

In the case of GDPR, for example – which imposes a penalty of €20m or 4% of annual turnover – it's becoming glaringly obvious that the answer is no. The expense of an off-site or online backup service is minimal when compared to the potential cost of losing your records or having them fall into the wrong hands.

We are all familiar with the saying “A chain is only as strong as its weakest link.” Cloud-based, security-minded packages from a single, trusted provider are often the best way to ensure that the entire chain is of consistent quality, with each link built-for-purpose, and a single entity responsible for its performance.

ABOUT THE AUTHOR

Byron Clatterbuck is CEO at SEACOM