Cybersecurity is for all businesses, even SMEs

By Ignus de Villiers

23 Aug 2023

One of the myths that surround cyber security is that SMEs don't need it to the same extent larger enterprises do. The perceived wisdom is that cybercriminals - aiming to score a payday or cause widespread damage - target mainly large corporations, governments, and global organisations to maximise their impact.

SMEs should not neglect cyber security. Source: Christina @ wocintechchat.com/Unsplash

According to a report by Liquid C2, which features research and analyses across Kenya, South Africa and Zimbabwe about evolving cyber security threats, cyber-attacks against large enterprises have ramped up dramatically.

The report further reveals that the number of cyber-attacks on businesses in Kenya, South Africa and Zambia increased by 76%, and while the research was compiled using data from large corporations, SMEs should sit up and take notice too.

SMEs are an attractive target for cybercriminals

This is because the view that small businesses needn't worry about implementing cyber security strategies and supporting safeguards is not only inaccurate but also dangerous to both SMEs and their partners operating in the online space.

Trends every SME should look into in 2023

SME South Africa 1 Feb 2023

SMEs are, in fact, more attractive targets because they're perceived to have weaker security measures, and the impact of a successful breach can be even more damaging to them than larger enterprises. In some instances, it can mean the end of the business.

Cybercriminals can use a wide array of avenues to breach an SME. The biggest threats are phishing attacks via email, leading to fraud, and malware (ransom) attacks that are typically linked to malicious links and/or files from unknown senders that are opened.

Attacks on passwords are also common, and they typically lead to complete compromise, including elevated rights and ownership by attackers. All it takes is one employee to open a malicious link, and an entire private network can be compromised.


Ignus de Villiers. Source: Supplied

Furthermore, those SMEs that employ remote working or hybrid working models are more at risk than others. Employees using unprotected networks should be a major security concern to employers, as should load shedding, which sees workers hopping between private and public Wi-Fi networks, accessing critical corporate software and data, many without any protective cyber security measures.

The negative impacts of a breach against a business that suffers a cyber-attack have been well documented – loss of data, including extorsion, liability fees, loss of revenue, damage to reputation, and loss of trust by consumers and partners. In the case of SMEs, there is another concern; they can become a gateway for hackers who want to breach the larger entities they are partners with or suppliers for.

In such instances, an SME can find its ability to grow its operations through a bigger partner permanently halted thanks to reputational damages incurred by a cyber-attack. Unfortunately, this type of occurrence has become so widespread and harmful that many larger companies refuse to conduct business with SMEs that do not have a cyber security programme in place.

In addition, many countries/industries now have legislation and regulations governing data protection and privacy, so implementing cyber security measures enables SMEs to comply with these legislative/regulatory requirements and avoid fines or legal action.

Every business – no matter its size – that conducts operations in the online space can afford to be without a comprehensive cyber security strategy and complementing measures or safeguards.

Cyber Security is easier than you think

The good news is that implementing a cyber security programme is easier – and more cost-effective – than most SMEs may imagine.

Investing in the right cyber security programme does not have to be complicated or expensive. Installing countermeasures – such as advanced endpoint protection including antivirus (malware) software, strong authentication, data backups, data encryption and managed security services – can mitigate a lot of attempted breaches and, in some instances, stop attacks even before they start.

An incident response plan in the event of a cyberattack, as well as considering native cloud security solutions, are equally important – and many of these solutions are cost-effective and scalable for SMEs. It's crucial to make these purchases from a reputable vendor with a proven track record in the cyber security space, as they provide a substantial number of native security safeguards that can be enabled and optimised to protect SMEs effectively against most attacks.

Employees are the first line of defence

But perhaps the most important aspect of any successful programme is the training and education of employees on best cyber security practices. Workers need to use strong passwords with multi-factor authentication for all accounts and be aware of the need to regularly update the software they're using by installing security patches.

Data back-ups are imperative and need to be maintained and protected to mitigate the permanent loss of data in the event

of a successful breach. Training also needs to involve identifying phishing emails and not clicking on links or files from unknown senders, as well as backing up important data regularly and storing it securely.

Much like gym memberships, cyber security programmes only work if the people using them are committed and trained in how to use the equipment effectively (in this case, security software and hardware rather than weights and treadmills). All the firewalls and anti-virus software in the world won't make any difference to an organisation if its employees can still be fooled into allowing criminals to breach the network through a lack of knowledge or social engineering.

Employees are a company's first line of defence, and ensuring they are trained and aware of cyber security measures is a central plinth in any strategy aimed at protecting a business in the online space.

Cyber Security is needed by everyone

Cyber security in businesses – as well as government and NGOs - is key to ensuring the growth of the digital economy. It must receive the strategic priority it demands for sustainable business success. Cybercrime affects all companies, not just the big ones, and as is the case with larger enterprises, cyber security for SMEs is no longer a grudge purchase. It should be at the centre of any business conversation.

ABOUT THE AUTHOR

Ignus de Villiers is managing executive at Liquid C2 Cyber Security