The rising tide of cyber threats: Safeguarding African SMMEs in the digital age

Issued by The Innovator Trust

7 Jul 2023

Globally, our first encounters with cybersecurity took on the form of antivirus protection in the form of the first official commercial antivirus software released in 1987. We've come a long way since then, with the digital world intricately woven into our lives. As the era of exponential tech unfolds more rapidly every day, cyber threats have evolved, and so has our need for cybersecurity.

IOL references cybercrime as one of the biggest threats South African businesses face in 2023: "Innovations such as artificial intelligence, the internet of things and robotics have changed how the world operates regarding business. Simultaneously, however, the developments have run parallel to the rocketing of cybercrime." As we transition into a fluid and immersive digital world, perhaps to understand the significance of cybersecurity for SMMEs, we need to take a step back to examine the state of the African SMME nation and where we are on the cybersecurity usage scale.

State of the African SMMEs and cybersecurity

With the youngest population in the world, Africa's youth have a far greater demand for IoT than ever before. KnowB4 interviewed 800 SMMEs from eight African countries, including South Africa, and highlighted the following intriguing findings concerning cyber threats and security amongst African SMMEs. KnowBe4's Africa End User Cyber Awareness Survey 2022 reveal that 71% of the respondents from eight African countries use their mobile data to access the internet.

- 63% use their mobile phone for mobile banking and payments.
- 32% will continue remote work.
- 68% are concerned about cybercrime but lack a basic understanding of threats.
- 57% are unaware of ransomware attacks.
- 21% experienced vishing attacks, and 32% lost money to scams.

- Only 38% were confident in security roles, and 21.25% found cybersecurity training adequate.
- 36% fell victim to crypto scams, and 57% know others who were scammed.
- 52% attribute security mistakes, like clicking on phishing emails, to a need for more awareness or training. 38% cited distraction, multitasking, and cognitive overload as the second leading cause.

The benefits of digitalisation for businesses across sectors have been far reaching and with it, an increasing vulnerability to online threats. Major network providers such as Vodacom in South Africa, have placed extensive emphasis on mitigating business security concerns with a number of unique offerings for businesses of all sizes with the overall aim of minimising impeding cyber threats. Based on the insights mentioned above, there is much work to be done concerning SMMEs specifically, and actively taking the correct steps with the software they need to protect their information. An excellent place to start is to understand the common cyber threats facing SMMEs today and how to overcome them.

Malware attacks
These are apps designed to carry out malicious attacks. From spying on your devices to accessing valuable information, malware attacks are rife, with the most popular form being ransomware. In this instance, you are asked to pay a ransom to regain your data - there is often no guarantee that you will.

Phishing attacks
These forms of social engineering involve fraudulent emails or messages that deceive individuals into sharing sensitive information or clicking on malicious links. They are ubiquitous.

Business email compromise (BEC)
This occurs when cybercriminals impersonate a legitimate business entity to deceive employees into transferring funds or sensitive information. They frequently mimic a known email address and contact so closely that it's difficult to spot fake mail. They duplicate invoices and change the bank details to their own.

Password attacks refer to a malicious attempt to gain unauthorised access to a system or an account by trying various methods to guess or crack the password. A password attack aims to bypass the authentication process and obtain sensitive information, compromise accounts, or gain control over a system. Weak passwords are compromised with greater ease. Companies using cloud-based technology are particularly at risk. The forms of attack include dictionary attacks, keylogger attacks, brute force attacks and rainbow table attacks.

Man in the middle (MITM)
In a MITM attack, the perpetrator positions themselves between the target's device and the intended recipient, enabling them to intercept and manipulate the exchanged information. This grants the attacker unrestricted access to the data and empowers them to exploit it as desired. MITM attacks frequently occur when connecting to an insecure Wi-Fi network or utilising an unsecured online platform.

Insider threats
These are risks from within the company which have the potential to cause harm to organisations, compromise sensitive information, and violate legal and ethical boundaries. They include:

- Unauthorised access
- Data theft and breach
- Sabotage and disruption
- Fraud and financial crimes
- Violation of trust and confidentiality

A need for more data backups
While this may seem out of place, the threat is equally costly to the business. Insufficient backup practices expose businesses to the risk of data loss, which can have detrimental consequences. When a business's data is compromised or lost due to a cyberattack, natural disaster, human error, or other unforeseen events, it can cripple their operations. This can result in financial setbacks, damage to their reputation, and potential legal complications.

According to ITWeb SA, 60% of backups will remain incomplete, 50% will fail to restore, and 20% of SMMEs will be hacked this year alone. Implementing robust backup measures is essential to safeguard against these risks and ensure the continuity of business operations, even in the face of unforeseen events or cyber threats.

With all this being said, where to from here? To safeguard against typical cybercrimes, SMMEs should establish a robust cybersecurity policy delineating security objectives, procedures, and accountabilities.

- **Unlock the next level of your success with the Innovator Trust's cutting-edge incubation programme** 20 May 2024
- **SKJ Group: Built on resilience, driven by innovation** 19 Apr 2024
- **Catalyst for success: Innovator Trust's R145k grants elevate 10 SMMEs** 19 Jan 2024
- **Innovator Trust unveils 2023 SMME Women in Tech Award recipients** 7 Dec 2023
- **From AI to 5IR: Engineering a sustainable African future with Katlego Malatji** 25 Oct 2023

The Innovator Trust

THE INNOVA-TOR TRUST

The Innovator Trust was created to support the growth of small black-owned Information and Communications Technology (ICT) businesses in South Africa. Our programmes facilitate training that develops their skills as business owners.

Profile | News | Contact | Twitter | Facebook | RSS Feed