# Cybercrime on the rise in SA: How to protect your business, customers and employees

Issued by Business Partners Limited

18 Aug 2022

The plight of prominent corporates falling prey to cyberattacks continues to make headlines throughout the country. Large businesses, however, are not the only victims of cybercrime, with research by Accenture revealing that 43% of cyberattacks target small businesses. It is therefore imperative for South African small and medium enterprises (SMEs) to implement risk management measures to guard against the threat of cybercrime.

Jeremy Lang: Executive director

This is the opinion of Jeremy Lang, executive director at Business Partners Limited, who says that it's more important than ever for SME owners to be aware of the extent to which a cyberattack can cause business disruption and have a significant impact on their bottom line.

He points to statistics, which highlight that losses incurred by local SMEs account for a large proportion of the R2.2bn in damages that the country suffers every year due to almost 600 cyberattacks every hour. In a survey conducted by specialist cyber risk consultancy, Storm Guidance, just under 85% of respondents acknowledge that cybercrime is a serious problem amongst SMEs in South Africa.

Lang says that as this finding suggests, the level of seriousness with which cybercrime is being regarded is increasing. "There are, however, a few fundamentals that SMEs need to become more aware of in order to secure adequate protection.

"While digital disruption has opened doors of possibilities for SMEs to make their mark in the larger business world, it has also introduced real risks in terms of revenue loss as well as substantial legal repercussions due to cyberattacks," Lang explains. Expanding on his opinion, he emphasises the importance for SMEs to have a strong understanding of the attacks to which small businesses are particularly vulnerable.

According to internet security software specialist, Kaspersky, in 2022, the number of Trojan Password Stealing Ware (PSW) detections in the country increased by almost 70% when compared to the same period in 2021. This amounted to 20,922 detections in 2022 alone. This kind of malware allows cyber criminals to steal passwords and other account information, providing access to the business' larger network.

Another common form of cyberattack is a data breach, where confidential files containing personal information are used by cyber criminals to hold businesses to ransom. This kind of attack has far-reaching implications for businesses in terms of damage to their reputation, losing the trust of their customer base and the cost of mitigating the effects of a data breach in addition to the possible payment of a ransom.

As Lang suggests, another important dimension of this kind of risk that needs to be considered involves the potential legal ramifications. If an attack on an SME results in customer information being used for identifying theft or fraud, those third parties could sue the small business who may be found liable due to negligence or the lack of adequate cybersecurity processes and procedures and the SME can incur a fine from the National Information Regulator for breaching the Protection of Personal Information Act (POPIA).

Beyond implementing cybersecurity software solutions, Lang provides the following advice for how small businesses can protect themselves against these risks:

**Reinforce best practices**

The term 'cyber hygiene' is now being used to refer to the industry best practices that exist to help people protect their valuable information. Any cybersecurity policy you introduce into your business needs to include mandatory cyber hygiene practices like regular password changes, never using universal passwords, using VPNs and multi-factor authentication, and file storage and transfer policies that disallow the use of unsecured software.

**Ensure that staff are well trained on cybersecurity awareness**

Putting cybersecurity policies in place is a good place to start, but it is important for employees to understand the reason for these policies. This is particularly important for SMEs who allow for remote working. When training your staff, avoid technical jargon and explain the risks in simple terms by quantifying the potential cost implications of a cyberattack to illustrate the seriousness of this issue.

**Prioritise data back-ups**

Although backing up your data may not prevent a cyberattack, it may help your business to recover quicker and easier. SMEs therefore need to include mandatory back-up procedures for information like customer and employee data as well as confidential agreements, contracts and sensitive company information. Human error is behind a large number of cyberattacks and is something that hackers and cyber criminals use as opportunities to infiltrate a business. This can be counteracted by strict adherence to back-up processes."

**Obtain cyber insurance**

As an SME, your stance on cybersecurity should always be one of prevention rather than reaction. But as a final line of defence, you need to consider having cybersecurity insurance should your risk management processes fail to prevent an attack. This kind of insurance will cover aspects such as legal costs, data recovery costs, third-party liability claims, cover for business interruption and, by extension, the cost of cyber extortion. Speak to your insurer to discuss your SME's needs as well as your budgetary restrictions in order to apply for an adequate degree of cover.

As Lang concludes: "Cybersecurity is no longer an option for SMEs, it should be regarded as a business requirement. We live in an age of rapid digital advancement and, while this is great news for small businesses, it also means that cyber criminals are getting smarter and more innovative. The only way to protect yourself and your business is to keep abreast of developments and treat the need for cybersecurity as a necessity that is certainly here to stay."

- **New SME survey results reveal upcoming national elections a deep concern for SA small business owners** 25 Apr 2024
- **30 years on, entrepreneurs are making the most of SA's enduring miracle** 24 Apr 2024
- **3 ways SME owners can cultivate a culture of human-rights in their businesses** 25 Mar 2024
- **SA entrepreneurship event sheds light on the need and the value of women in business** 14 Mar 2024
- **4 ways to turn your business idea into a thriving business** 12 Mar 2024


**Business Partners Limited**

BUSINESS/PARTNERS

We're Business Partners Limited, one of the leading business financiers for viable small and medium enterprises (SMEs) in the world. We provide business finance ranging from R500 000 to R50 million to established entrepreneurs with a viable formal business.

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