BIZCOMMUNITY

3 steps for small businesses to bolster cybersecurity

By Ben Bierman , issued by Business Partners Limited

10 Oct 2023

It has been widely reported that South Africa is poised to overtake Nigeria as the continent's capital for cybercrime. According to the latest research conducted by Interpol, South Africa has seen a staggering 100% increase in mobile banking application fraud over the last year and is estimated to experience as many as 577 malware attacks every hour. While the broader media have made great strides in bringing awareness to the prominence of cybercrime in the country, the message needs to be amplified in the small business sector in particular.

Busting the myths

Ben Bierman, Business Partners Limited

One of the biggest misconceptions held by South African small businesses is that their ventures are too small or relatively insignificant to present an attractive prospect for opportunistic cybercriminals. Another commonly held belief among the small business community is that there is no viable reason for cybercriminals to target them – no personal vendetta to act upon or score to settle. Both opinions, however, are unfortunately misguided.

Recent estimates published by the Council for Scientific and Industrial Research (CSIR) puts the annual cost of cybercrime in South Africa at over R2bn, with most of the attacks being targeted at small businesses and individuals.

The reality is that even the smallest, seemingly insignificant dataset can be immensely valuable to criminals looking to sell data on the black market. And even one email hack or OTP scam can catalyse a ripple effect that can rob someone of their entire identity or clean out their bank account.

Experts also caution small business owners against believing that without a clear motive, cybercriminals would simply not be interested in hacking their businesses. In fact, a growing body of research suggests that cybercriminals are simply ‘playing a numbers game’ – using automated scripts and bots to scan companies for cyber vulnerabilities and attacking them in large volumes, knowing that a few of their 'leads' may materialise in lucrative results.

The real cost of cybercrime

Some of the most common forms of cybercrime include ransomware attacks, malware, online banking scams, cryptocurrency trading scams, phishing and website hacks. At this stage, most business owners are aware of the immediate financial implications of losing valuable data or money. However, there are other, more far-reaching consequences to consider as well.

The reputational damage of a cyber breach could stretch on for months – or even years – after the initial attack and could deteriorate to the point of forcing a business to close its doors for good. This is largely due to the breakdown of customer trust and confidence that a hack can catalyse.

There is also the possibility of litigation – businesses being sued by customers whose data has been stolen, for example. In many cases, the data lost can be irretrievable – even in the case where data is held for ransom and then released, business owners simply have no guarantee that the data recovered has not been duplicated for sale elsewhere on the dark web.

A further harsh reality is that cybercrime is notoriously difficult to investigate and prosecute in South Africa. While the Cybercrimes Act (ratified in 2021) has gone a long way in remedying this situation, the South African Police Service is still

relatively under-resourced, with little statutory means by which to convict and charge criminals, let alone help companies recover their losses. The real cost of cybercrime is therefore far more extensive than most realise.

Three steps to better cybersecurity

South African small businesses cannot afford not to build a robust line of defence against cybercrime. Fortunately, there are measures that can be taken to implement risk mitigation policies and procedures that don't necessarily require large capital outlays. Although making a substantial investment into top-notch security software comes highly recommended, there are a few other simple steps that can be taken in managing the associated risks. These include:

1. **Using a managed cybercrime security service**
   Many businesses have hesitated to adopt outsourced Security Operations Centre (SOC) due to perceived high costs, while others using security information and event management (SIEM) platforms have found them inadequate and overwhelming with alerts, draining resources. international Cyber Security Specialists, KHIPU Network's "Secure the Data Centre" initiative aims to address these challenges.

   Starting at an annual cost of R469,392.37, the initiative aims to make outsourced SOC services accessible to South African businesses. It provides ongoing cybersecurity monitoring and is ideal for organisations looking to enhance the integrity of their cybersecurity systems.

2. **Implement strong password policies**
   In the world of cybersecurity, passwords are the keys to your digital kingdom. Small businesses often underestimate the importance of robust password policies, but they're the first line of defence against opportunistic cybercriminals. Encourage your employees to use passwords that are complex and robust. Consider implementing multi-factor authentication (MFA) wherever possible. MFA adds an extra layer of security by requiring users to provide two or more forms of identification before gaining access. Encourage employees to use password management tools like LastPass, Dashlane, or 1Password. These tools can generate secure passwords, safely store them, and even autofill login details, making it easier for your team to use strong and unique passwords without the burden of remembering them all.

3. **Consider cyber insurance**
   This specialised insurance is designed to mitigate the financial impact of a breach, covering costs like legal fees, data recovery, customer notifications, and even reputation management. It's not a replacement for strong cybersecurity practices but rather a crucial supplement, ensuring that if the worst happens, your business can bounce back financially without crippling losses. Investigate your options and consult with insurance experts to find a policy that suits your business needs.

- **Why optimism and entrepreneurship go hand in hand (and why it's crucial to a growing business)** 31 May 2024
- **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

Business Partners Limited

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