

# A quick guide to end-to-end business security

 By [Elaine Wang](#)

6 Feb 2019

The threat of cyber attacks has been at the forefront of discussions in the media and in the technology industry itself, particularly over the last two years.



Elaine Wang is Cloud and Software Solutions Director at Rectron.

However, small businesses still seem to think that there is very little need for cybersecurity as they're not as lucrative targets to hackers as larger corporations are. Nevertheless, this is entirely false.

Small and medium-sized businesses experience slightly more data breaches involving personal information and the size of data breaches are usually larger.

According to a 2018 Bitdefender study, over one-third of organisations took between one week and six months to discover an attack at all.

Data has value to hackers because it has value to a business, so no matter the size of an organisation, preparation is key.

Businesses need to start taking a holistic approach to cybersecurity in the workplace, taking both preventative as well as disaster recovery measures into account. Here are some tips to help small and medium-sized businesses improve their network security.

## **Preventative**

- Training.

User training and monitoring is extremely important as users are often the weak point of a network.

Employees are usually unable to detect a fraudulent email, so companies need to educate employees on spotting malware, phishing attacks and social engineering tactics to avoid accidental breaches.

- User policy changes.

Implementing policies that limit users' ability to install unauthorised software on work devices and requiring users to update passwords regularly can go a long way in protecting the network of business.

Additionally, requesting that users employ a mobile security tool trusted by the organisation could minimise vulnerabilities.

- Network security tools.

Organisations can find multiple monitoring and anti-malware tools on the market which can help them to protect their entire network, which includes mobile device management, such as Microsoft 365 and Gravityzone Advanced Business Security.

- Consistent security updates.

A company's IT division should routinely perform software upgrades to ensure the latest security patches are rolled out across the entire organisation as there are still many companies not installing consistent software updates on devices.

## **Disaster Recovery**

- Incident response plan.

A disaster recovery system for business-critical applications is crucial to minimising downtime as a result of an attack and should account for and understand all possible risks and what exactly your business needs at a minimum for operations to continue.

- Back-up systems.

Implementing a robust backup system can help to ensure that there is no loss of data which can be costly, both monetarily and in the loss of reputation, for a business. An increasingly popular way of backing up important data is to use a cloud-based offering which can do this automatically.

Small and medium-sized enterprises are important drivers of productivity in most economies, especially in South Africa, therefore a successful economy lies in successful small business.

Because cybersecurity breaches have the potential of closing a business down permanently, businesses need to ensure that not only do they have adequate security measures in place, but also built-in contingency plans in the event a breach does take place. And in this day and age when it comes to cyberattacks, it's not a matter of if anymore, but rather a matter of when.

## ABOUT ELAINE WANG

I am a driven and extremely hard working individual, with a keen eye for business ideas and opportunities.

- #YouthMonth: A 12-year-old and their mobile device - 15 Jun 2020
- How to optimise your cloud usage - 13 Mar 2019
- How beneficial are local cloud data centres for SA business? - 20 Feb 2019
- A quick guide to end-to-end business security - 6 Feb 2019
- Technology that shines a light in the face of load shedding - 29 Jul 2015

[View my profile and articles...](#)

For more, visit: <https://www.bizcommunity.com>