ARTICLE

In South Africa, Cybersecurity Investments are Needed to Mitigate Increasing Risks Amid COVID-19 Pandemic.

As cyberattacks and exploitative activity ramp up amid the COVID-19 crisis, the stakes for strong cybersecurity practices are even higher.

Lack of cybersecurity preparedness continues to create problems and risks for companies in South Africa. The 2020 FTI Consulting Resilience Barometer, which polled more than 2,000 respondents from large companies across all G20 countries, reported that companies in the region are suffering cyber attacks and falling victim to ransomware more than global averages (33% vs. 27% for overall attacks). While most leaders in the region are aware of the risks - 84% surveyed believe they have cybersecurity gaps - less than half said they have made investments in that part of their business in the last 12 months. This disparity between known risk and response is concerning even during the best of times.

Recent changes in the ways we are working has presented cyber criminals with a multitude of opportunities to exploit weaknesses in systems, processes, and behaviour. In addition to simple email phishing scams, employees are expecting non-standard emails from their IT support teams, making them more susceptible to work-related phishing attempts. Attacks via outsourced IT providers, themselves operating in unchartered waters, are also on an uptick.

"Simple email phishing scams that capitalise on the public's anxiety and appetite for new information are on the rise, as individuals are more likely to click on false information or fake news links spread via social networks".

In addition to increased phishing and ransomware risks, working from home presents additional IT-related threats.

Most IT teams have been focused on quickly enabling employees to work remotely and ensuring continued business operations, forcing network security onto the backburner. Still, each time an employee connects to their corporate network from home, they are creating a potential access point for a threat actor to exploit.

"IT departments and cybersecurity teams face a daunting task securing sprawling, vulnerable networks remotely - and many must do so with a reduced budget and resources".

Key risks arising from today's remote work conditions include:

Unsecured Wi-Fi Networks

Not all workers will have secured their home Wi-Fi network, or even changed the router's default login credentials. Some may have to use unsecured public Wi-Fi networks, which are prime targets for threat actors to spy on internet traffic and collect data unnoticed.

Personal Devices

Considering the short timeframe available for deploying a home office, many workers will not have company-issued laptops, equipped with up-to-date security tools. They will be required to use personal devices to do their work. Such devices are often deficient in terms of up-to-date, commercial antivirus and anti-malware software. This increases the risk of malware being deployed on these devices, if not already present, and both personal and work-related information being leaked.

Scams Targeting Remote Workers

An increase in malicious attacks targeting remote workers is already occurring. This could involve targeting the individual for access to banking information or to elicit certain valuable information, or a more advanced attack to gain access to a company's IT infrastructure.

IT patching and technology stress testing, employee training and awareness, threat monitoring, critical asset and systems identification, and the provision of in-house cybersecurity expertise are some of the key initiatives in which organisations should be investing to address these risks and bolster defences for the long-term.

"Alarmingly, less than half of South African companies surveyed, have taken these steps in the last 12 months".

Even in a tough economic climate - which South African enterprises were facing prior to, and now more so during, the global pandemic - investing in adequate cybersecurity protections is critical.

36%

The 2020 FTI Consulting Resilience Barometer showed that 36% of South African businesses that experienced a cyber attack lost revenue as a direct result.

27%

27% of South African businesses suffered reputational damage. Other serious effects - including loss of customers, employees, and stock market value - were listed as consequences by roughly a quarter of respondents.

In addition to allocating sufficient resources to improve cybersecurity resilience and implementing cyber best practices, companies and their employees can proactively mitigate risks through specific steps, including:

- Identifying likely attack vectors as a result of more employees working from home and prioritise the protection of their most sensitive information and business-critical applications.

- Providing clear guidance on IT security and encouraging ongoing communication with staff. Remote-working policies should be clear, with simple steps that assist employees to make their home working environment secure and facilitate a simple process for reporting suspicious activity.

- Ensuring all corporate IT assets or managed devices are regularly updated with sufficient security tools, extending the same security best practices in the company to all remote environments as far as possible.

- Practicing good password hygiene by using complex passwords, changing them frequently, and utilising multi-factor authentication.

- Maintaining personal computer devices by installing updates and patches regularly, including on mobile devices.

- Securing home Wi-Fi networks by changing default settings and passwords on the home router in order to reduce the chance of a security breach.

- Using a virtual private network (VPN) to build a trusted connection between the home device and the company network and tools.

- Ensuring devices are used for work only and children do not use the same device for downloading and playing games, for example, to reduce the risk of a malware infection.

- Staying vigilant for phishing emails or similar scams.

The cost and damage of a data breach or cyber attack can reach far beyond the upfront investment needed to establish a stronger security posture.

As organisations continue to grapple with the challenges associated with the COVID-19 pandemic, and look ahead at returning to business as usual, engaging with IT security specialists, and deploying strong processes and technologies will be critical to reducing exposure and improving resilience.

GEOFF BUDGE
Managing Director
geoff.budge@fticonsulting.com
FTI Consulting South Africa

Learn more at fticonsulting.com/covid19

FTI CONSULTING™