ARTICLE

Strengthening Cyber Resilience in the Wake of the Pandemic

South Africa

Cybersecurity remains a significant concern for businesses in South Africa. Early on in the pandemic, cybersecurity experts reported dramatic increases in attacks on businesses in the region, with hundreds of thousands of devices and accounts being exploited each week. Unfortunately, though cyber risks have continued to increase, the pressures of the last year have prevented most businesses from taking the proactive steps needed to mitigate their risk.

Recent data from FTI Consulting's 2021 Resilience Barometer—which draws on insights from business professionals in South Africa and globally regarding the major commercial, technological, reputational and legal challenges of the last year—confirmed that this increase in risk has not been adequately addressed by most corporations in South Africa.

As our teams anticipated, and discussed in previous articles, the remote work operating model has perpetuated exponential growth in the frequency and intensity of cyber attacks and third-party risk.

Highly motivated cyber criminals continue to leverage public anxiety and sprawling, vulnerable networks to launch email phishing scams and other network exploits.

> *"As a result, roughly three in five large South African businesses have experienced external and internal cyber threats over the last year. Respondents attributed this uptick in cyber exposure directly to factors resulting from the COVID-19 pandemic."*

1/2

Still, only half of businesses are proactive about mitigating this risk.

1/3

Nearly one-third of respondents in the Resilience Barometer survey acknowledged they are fully reactive in their response to cyber risks,

19%

and 19% said they are not managing their cyber risk at all.

This is particularly concerning considering many that experienced a cyber attack in the last year reported losing revenue, assets or customer information as a result of those incidents.

"Lack of resources is the most common culprit. Many enterprises do not have the financial means, capacity or expertise in this difficult economic climate to ensure that their systems have adequate protection in place or to invest in readiness programmes."

However, the risk landscape has reached the point at which businesses can no longer afford to continue operating in a reactive mode.

"The good news is that the events of the last year, while they are to blame for weakened defenses and reduced ability to mitigate cyber risk, have also pushed cybersecurity up the agenda."

68%

According to the Resilience Barometer, more than 68% of respondents in South Africa indicated that cybersecurity has become a board-level issue as a result of COVID-19.

52%

With this, businesses have improved their approaches to managing the leak of sensitive internal information, with 52% of South African respondents reporting that they manage this risk proactively, compared to the 44% of G20.

Strengthening resilience on many fronts, particularly cybersecurity, will be critical to a successful recovery from the pandemic. An end to the crisis is in sight, but there is still a lot of work to be done.

From a cybersecurity perspective, there are several key risks and opportunities businesses in South Africa can address in order to improve their resilience in this new landscape. These include:

1. Digitalisation

Nearly all of the respondents in the Resilience Barometer survey are under extreme or significant pressure to integrate technology and innovate in the next 12 months. Yet only half as many expressed concern about post-pandemic risks such as external threats (47%) and securing new and emerging technologies (35%). While digitalisation and data analytics will provide significant advantages to becoming more efficient, differentiating from competitors and bouncing back from financial setbacks, businesses must place equal emphasis on addressing the spectre of increased cyber risks.

2. Supply chain disruption

Roughly 85% of Resilience Barometer respondents agreed that the pandemic is forcing them to reimagine their supply chain. As disruptions to supply chains, processes and working environments continue, businesses must be prepared to evaluate the additional cyber risks that accompany these changes. Businesses must recognise the evolution and emergence of cyber risk alongside the tremendous changes taking place across their processes.

3. Persistent remote work conditions

Most businesses will continue to keep their offices closed for day-to-day work. With many employees continuing to work from home through 2021 and perhaps indefinitely, businesses must continue to be vigilant regarding related vulnerabilities that first emerged in 2020. This includes addressing unsecured Wi-Fi networks, implementing controls around personal devices, setting policies for the use of third-party apps and collaboration tools and training and awareness programmes that help employees understand their role in preventing a cyber breach.

4. Resource allocation

It's critical to invest in cybersecurity readiness. While it may be difficult to secure budget for new tools, headcount and programmes this year, the business case for doing so is clear. The financial downsides of a cyber attack, regulatory violation due to loss of personal data or reputational fallout from a massive data breach, far outweigh the cost of implementing strong defences.

South African businesses are operating in an increasingly tenuous climate and must address the gaps in their approach to cyber resilience.

"The most successful businesses, and the quickest to recover from the pandemic, will be those that recognise cyber resilience as a vital source of competitive advantage, with cybersecurity bolstered as a key element of survival in the future of business."

GEOFF BUDGE
Managing Director
Head of Technology Practice
geoff.budge@fticonsuling.com
+27 (0) 76 400 6237
FTI Consulting South Africa

PAUL REILLY
Managing Director
EMEA Cybersecurity
paul.reilly@fticonsulting.com
+44 207 632 5013
FTI Consulting