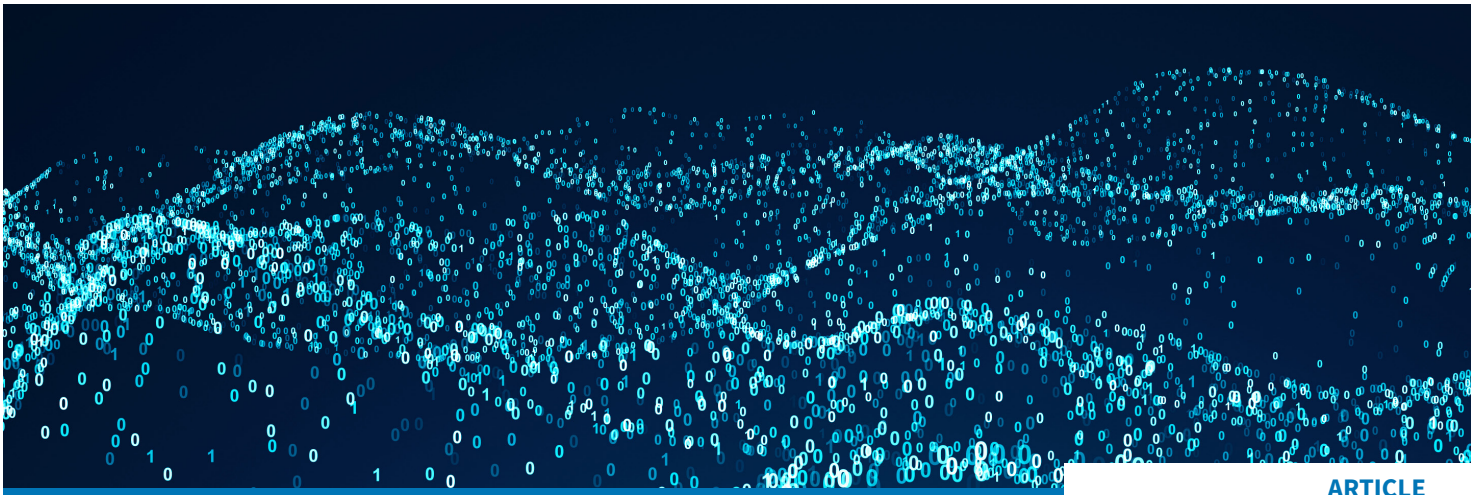

ARTICLE

# Building resilience post a cyber incident

## South Africa

Warren Buffett once said, “It takes 20 years to build a reputation and five minutes to ruin it.” Rarely can the ‘sage of Omaha’ be disputed, but on his point around timing, five minutes is a very long time in today’s real-time world when you’re dealing with a cyber attack.

Cybersecurity is one of the most critical commercial and reputational risks facing South African organisations today. No sector is immune, and no business can afford to be unaware of their vulnerabilities or have robust practices in place to manage them.

Globalisation, investor activism, regulatory change, political and cyber risk are all contributing to increased business vulnerability which is amplifying the need for companies to carefully consider their ability to respond effectively. These mounting risks coupled with the always-on nature of the news cycle mean that companies face round-the-clock scrutiny.

Cyber risk is no longer just a technical issue. Prevention and response need to be comprehensively embedded in people and systems. For it is how an organisation responds to an incident that often gets as much attention as the incident itself. If handled poorly, a crisis can cause deep and long-lasting damage to a company’s reputation. If handled well, it is an opportunity for a company to show its mettle to its stakeholders.

Today, cyber threat tops most corporate agendas. Research conducted as part of FTI Consulting’s 2020 Resilience Barometer amongst 2000 companies operating across the G20 countries at the beginning of the year shows that a cyber breach is the top concern for boards and management teams.

At least one in four G20 organisations has experienced a cyber attack where assets were stolen or compromised in the last 12 months. Worryingly in this region, that figure rises to one third with the most common breach a phishing attack, followed by a loss of customer or patent data and loss of third-party information.

During the course of this year, over a quarter of business leaders expect their business to be harmed by a cyber attack. Yet, less than half of are taking steps to manage cyber risk proactively. Most leaders in the region are aware of the risks with 84% surveyed acknowledging their cybersecurity gaps. However, only 40% have made investments over the last twelve months.

The 2020 FTI Consulting Resilience Barometer showed that 36% of South African businesses that experienced a cyber attack lost revenue as a direct result and 27% of South African business suffered a negative impact on their reputation.

## The scale of the problem

The global move towards increased digitalisation and cloud migration, combined with a regulatory and judicial environment pursuing greater effectiveness leaves us in an exposed position. The additional impact of COVID-19 means that many of us have been working from home for prolonged periods of time, presenting the cyber criminals with new opportunities to exploit weaknesses and breach our processes, systems and behaviours.

The fourth industrial revolution is fundamentally changing the risk environment and creates a new range of potential unintended consequences across corporate ecosystems. Unfortunately, Africa's pursuit to realise this potential is not equal to its efforts in cybersecurity and this is leaving the continent vulnerable to cyber attacks.

The Cyber Crimes Bill passed by the National Council of Province at the beginning of July will now go to the President for sign-off. The Bill, which is aligned to international laws consolidates existing legislation and implements more stringent laws to stop cyber criminals acting in the country without fear of reprisal, as well as regulating powers to investigate these crimes.

## Planning for the worst

The threats to today's cyber landscape are ever evolving across the digital ecosystem, with more advanced tactics. Moreover, cyber attacks are becoming increasingly sophisticated and targeted, therefore a proactive approach is essential.

> *"While a cyber breach can be over in seconds, its aftermath lasts much longer."*

Whilst companies cannot control whether they are the victim of a cyber attack, they can control how they respond. Proactivity is key, especially when an incident has the potential to both cripple organisations and permanently damage its reputation.

Information is at the core of a good crisis response plan, starting long before a hack ever takes place. Companies need to understand their threat profile, prepare a response plan, understand their weak points and harden their defenses in order to successfully navigate future disruptive events of their own. Having data governance in place as part of a crisis preparedness and scenario planning impacts the effectiveness of the response if, indeed, the worst happens.

## Understanding the risk

In FTI Consulting's recent Anatomy of a Crisis report, which analysed 300 publicly available cyber breaches over the last ten years, data breaches that did not contain the most sensitive data tended to have a relatively benign market reaction, especially compared to other types of crises such as fraud and accidents. On average, share price recovered within three months of the attack taking place. The takeaway from this is that while investors may be forgiving, customers and employees take such an incident far more seriously, therefore this is where a company's communications response should be focused.

As one would expect, a cyber attack thrusts a company into the spotlight as media interest intensifies. Our evidence suggests that media coverage increases by five times and social media by eight times in the month following a cyber breach. And the bigger the breach, the greater the media interest. So how do you manage this?

## Taking proactive action

An integrated, cohesive strategy is key, implemented across existing mission critical functions. And it is this that informs both internal and external communications working from the inside out every step of the way. This encompasses addressing the various phases of an emerging crisis, reviewing options and making consequential decisions at each juncture.

Culturally, it is important to shift mindsets to act as a first line of defense in creating proactivity in and preparedness from the inside out. This allows management teams to respond to cyber risks in their own time and in a more controlled manner.

Business preparedness is key. Waiting until an incident occurs to determine a response is too late. Every second counts and lost time equals lost information, resources and reputation. How companies react to and communicate regarding their cybersecurity incidents is critical and there is only one chance to get it right. Despite this, only 45% of companies we surveyed for our 2020 Resilience Barometer report that their business is preparing proactively to deal with a cyber attack, and only 39% of businesses are conducting crisis simulations on a regular basis. Only just over a quarter of these businesses have invested in crisis communications readiness.

There are a number of options available for businesses to take in the immediate aftermath of a cyber event. In the short-term, those tend to relate to how the business responds from a communications perspective transparently, to acknowledge the issue, outline what's happened and to explain the action being taken to manage the crisis. In many jurisdictions, companies have a very limited window to comply with legal requirements to report such incidents with relevant parties.

*"Companies should carefully consider their response plan in the eye of the storm of a cyber breach and the channels of communication within the business."*

It is imperative that if the company is going to respond appropriately and accurately that all the details of the hack can be understood. Too often, we see companies succumb to the pressure of reacting fast by getting their facts wrong and lose control of the situation.

They must react with speed, proportionality and accuracy to inspire confidence in their customers, employees, investors and regulators to demonstrate the situation is under control. The proliferation of social media is increasing the velocity and complexity of each crisis, making it all the more essential to react with speed or the situation can quickly escalate.

Recovery is every organisation's top priority, but this can only begin once the incident is contained and the risk eradicated. But this isn't the end.

One of the most important aspects of incident response is also the most often forgotten - learning from the event and improving processes. Companies must evolve from the experience and how they would respond to future incidents to reflect lessons learned, new threats and better technology.

The goal in the recovery process is to position the crisis as firmly in the past, emphasising the progress made to restore confidence and bridge to long-term business sustainability and greater resilience. Once the initial crisis has subsided and recovery is underway, it is crucial to understand, identify and apply the lessons learned, facilitating continuous improvement and assured management of future issues.

*"Rebuilding trust amongst clients and broader stakeholders is not a quick fix – it takes time to earn it back. A quick and effective response to a cyber attack can go a long way to limiting the damage."*

**CAROLINE PARKER**
Managing Director
Strategic Communications
caroline.parker@fticonsulting.com
+27 (0) 72 659 9255
FTI Consulting South Africa

**GEOFF BUDGE**
Managing Director
Technology Consulting
geoff.budge@fticonsulting.com
+27 (0) 76 400 6237
FTI Consulting South Africa

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. For more information, visit www.fticonsulting.com and connect with us on Twitter (@FTIConsulting), Facebook and LinkedIn. **www.fticonsulting.com**
©2020 FTI Consulting, Inc. All rights reserved.