Cybersecurity and Resilience in South Africa

The 2019 FTI Resilience Barometer ranked cyber attacks as a top concern for South African businesses in the G20.

SOUTH AFRICA THREAT LANDSCAPE

South Africa is a target firmly in the view of cyber threat actors today. The Country's move towards digital transformation, combined with a regulatory and judicial environment that is still grappling to achieve greater effectiveness, leaves it in a vulnerable position.

In the past few years, South Africa has experienced significant breaches across a range of industries. Its banks have been silently robbed of millions, hundreds of thousands of identities have been stolen, and corporates have been held ransom, demanding a payment of usually Bitcoin to grant them access to their own data. Adding insult to injury, the attackers even provide a 24/7 support desk to help make Bitcoin payment. This problem is not exclusive to South Africa.

DATA AND ACCESS HOSTAGE SITUATION

Cyber criminals targeting South African businesses are increasingly using ransomware as their weapon of attack. This was the case for an electricity supplier of Johannesburg, who recently was hit by a ransomware attack that left some customers without power. FTI Consulting has assisted several organizations who faced ransomware attacks, including an e-commerce billing platform. Weak customer credentials led to a highly successful, laterally moving attack that was able to successfully encrypt servers in a matter of hours. The FTI Consulting team deployed to the client site immediately and was able to quickly determine the strain of ransomware. The collaborative effort led to a successful negotiation with the malicious actor, saving the client hundreds of thousands of dollars and preventing significant customer and revenue loss.

SIMPLE METHODS, EFFECTIVE RESULTS

Despite the simplicity of phishing attacks, they are effective in achieving desired results. For South Africa, they present a significant issue, as a vast majority of the population uses online banking services and Android mobile phones in the region are among the most targeted globally for banking-specific malware.

In a current engagement investigated by the team, threat actors were able to create mirror email addresses of an organisation by using a new email address with a single-character change to the legitimate email addresses of the entity – this change was hardly perceptible when reading the email address. Using this fabricated, yet seemingly real address, the threat actor was able to "pretend" to be the legitimate organisation and issue instructions through various means to a major subcontractor to make substantial financial payments to new bank accounts in foreign jurisdictions with the ultimate goal of financial enrichment. As part of this the entire financial controls and governance protocols of the primary organisation were breached. FTI Consulting is currently investigating the exposure levels of other subcontractors operating under the franchise of the parent organisation.

MORE CONNECTIONS, MORE EXPLOITS

Globally, the increase in digitisation and cloud migration is happening at a speed that surpasses security enhancements, and this is no different in South Africa. As data and other valuable assets move to the cloud, it becomes a prime target for hackers. Businesses often make the fatal flaw of blindly agreeing to the cloud provider's terms without doing their due diligence to determine if proper security protocols are in place, which they often are not. Hackers view emerging economies as easy targets because businesses often are rapidly implementing new technology, which creates new vulnerabilities, while also not having an existing security structure that provides adequate protection. After a leading medical diagnostics information provider suffered a third-party vendor breach, FTI Consulting was brought in to advise the client as it disclosed the breach that impacted millions of patients' medical and personally identifiable information. This included message development, rapid-fire response, media monitoring, and partnering with legal counsel to help mitigate any reputational risk to the client.

REGULATION IS ON THE WAY

Passed by the National Assembly in November 2018, the Cybercrimes and Cybersecurity Bill aims to consolidate existing piecemeal cyber crime legislation in South Africa, while also implementing new laws. Businesses operating in the region will face increased scrutiny and requirements, such as deadlines to report a cyber incident. Raising public awareness to the potential dangers of careless security practices and bolstering enforcement for failing to maintain regulatory compliance should be the end goal of this bill once it becomes law later in 2019. Currently, cyber criminals view South Africa as a place to conduct their illegal operations freely without fear of reprisal. FTI Consulting is highly experienced in regulated markets. Our work includes Regulator regime design, investigations, communications, and quantification of losses.

NATIONAL SECURITY THREATS

Escalating manoeuvres between adversarial jurisdictions is part of a growing trend of state-backed offensive cyber operations. There are multiple motivations behind these offensive efforts, such as disrupting critical infrastructure, demonstrating a strong presence on the global stage, influencing geopolitical decisions, destabilising democratic processes, and stealing assets. South Africa was recently targeted by North Korea in an attempt to raise funds by allegedly attacking the SWIFT payment system and stealing/mining cryptocurrency. Cyber attacks initiated by nation states are especially dangerous because the criminals have the full support and resources of their government to conduct their activities.

THE POWER OF PROACTIVITY

Combatting the specific cyber risks facing South Africa requires taking a proactive approach.

Businesses without strategic cybersecurity policy are faced with difficult choices, including whether to expend resources upfront when they believe their current security is sufficient. Instead of operating in 'incident response mode' where weak security policies and processes can be exploited, a structured strategy must be developed so that threats can be negated, and losses can be avoided, before they ever occur.

With cyber attacks becoming more sophisticated and more targeted, a proactive approach is essential.

INCIDENT RESPONSE & CRISIS MANAGEMENT

Once a cybersecurity incident is detected, it is essential to take action. Combatting the full range of cyber threats requires not just risk mitigation processes but also a proper business continuity plan that has been implemented and tested in advance. Additionally, effective internal and external communication is imperative during every cybersecurity incident. After a breach, often times the company is left vulnerable to increased media, legal, and regulatory scrutiny, increasing the risk for undesired exposure. When stakes are high, it is imperative to know what to say, how and when to say it, and to whom.

An example of the importance of managing reputational damage through effective communication is illustrated by the assistance FTI Consulting provided to a South African financial institution that suffered a security breach in 2018, where the company's mailing service was illegally accessed.

Breach Response & External Communication for a Financial Institution

The Challenge

In 2018, a South African financial institution suffered a security breach. A malicious external party gained unauthorised access to its IT infrastructure and demanded payment as a result.

Our Input

FTI Consulting was hired to identify where the breach occurred and to secure the client's systems. Once secured, the focus shifted to external communication with customers and stakeholders. FTI Consulting assisted with breach notification via text, email, and the client website, in addition to establishing a call centre and training staff on tailored messaging to customers. Further, a statement regarding the breach was also proactively disseminated to media.

The Result

The effective communications approach meant that while initial media coverage focused on reporting, subsequent coverage then detailed the preparedness of the sector more broadly and the issue of cyber crime as a general corporate risk. After a week, the overseeing regulator confirmed that the client's breach was handled 'satisfactorily,' which was echoed by the media, and negative sentiment relating to the incident remained at manageably low levels.

Less than 50% of South African businesses in the G20 proactively manage risks related to cyber attacks.

–2019 FTI Resilience Barometer

ABOUT FTI CYBERSECURITY

FTI Cybersecurity's expertise includes proactive, independent cyber and risk management advisory services, cybersecurity incident response and investigation solutions, crisis management and strategic communications, and technology anchored investigations. Our experts work at the heart of the most critical events often in high-profile situations.

As part of this, we have more than 300 dedicated incident response and cybersecurity consultants, led by those with decades of experience at the highest levels of law enforcement, intelligence and global private sector institutions.

We have an integrated team of cybersecurity experts, developers and data analysts with extensive investigative experience. Drawing from both government and the private sector, our experts routinely tackle large-scale analytic challenges requiring complex, custom technical solutions. We regularly construct and leverage technical platforms to collect, analyse, and correlate data in demanding environments requiring precision and speed.

HOW FTI CYBERSECURITY CAN HELP

Building a robust security position is the best way to prevent a breach from occurring. You cannot control whether you will be the victim of a cyber attack or not, but you can control how to respond to one and you can mitigate the chances of being the target of an attack with robust policies, systems and response strategies and capabilities. Waiting until an incident has occurred to act is too late.

We help clients of any size address their most critical needs and integrate new solutions atop or alongside pre-existing policies and programs to address cyber threats. We build a safer future by helping organizations:

- Understand their own environments
- Harden their defenses
- Rapidly & precisely hunt threats
- Holistically respond to crises
- Recover operations and reputation after an incident

GLOBAL KEY CONTACT

Anthony J. Ferrante
Global Head of Cybersecurity
Senior Managing Director
ajf@fticonsulting.com
+1 202 312 9165

REGIONAL KEY CONTACTS

Joshua Burch
Head of Cybersecurity, EMEA
Senior Managing Director
+44 20 3727 1000

Jordan Rae Kelly
Head of Cybersecurity, Americas
Senior Managing Director
jordan.kelly@fticonsulting.com
+1 202 312 9140

Petrus Marais
Head of Forensic & Litigation Consulting, South Africa
Senior Managing Director, Cape Town
petrus.marais@fticonsulting.com
+27 21 487 9014

Geoff Budge
Cybersecurity
Managing Director, Cape Town
geoff.budge@fticonsulting.com
+27 76 400 6237

Max Gebhardt
Crisis Communications
Managing Director, Johannesburg
max.gebhardt@fticonsulting.com
+27 11 214 2402

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals

EXPERTS WITH IMPACT

About FTI Consulting

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.