TRUST

FELIX RiskTrainingConsultants

LEARNERSHIP NEWSLETTER | NOV 2019

South Africa has the third-highest number of cyber-crime victims worldwide

The South African business sector and the nation overall is developing into savvy technology users to meet their economic and social needs. As a result, cyber-attacks such as online identity theft, hacking, ransomware attack, internet fraud, and cyberstalking are threatening the safety and security of people and companies, irrespective of their size. Consequently, cyber-security has become a necessity.
Recently, the South African Banking Risk Information Centre (SABRIC), have confirmed that some public and private institutions have been hit by cyber-attacks. According to media reports the well-orchestrated cyber-attack attempts began on the 23 October and has been linked to the disruptions Standard Bank experienced. However, Standard Bank's cyber security preparedness and resilience foiled the attack and customers personal information was protected.

The worst victim was the City of Joburg Municipality website whereby the residents and businesses were unable to pay their e-bills or log queries online with the Municipalities support team. Media reports claimed that hackers behind that cyber-attack demanded R437 000 as ransom payable in Bitcoin failing which they threatened to release sensitive information on Johannesburg residents. Fortunately, SABRIC robust defensive strategies minimised the cyber-attack on Standard Bank and the City of Joburg Municipality.

Other attacks reported in the media during the month of October includes denial-of-service (DDoS) attack on Afrihost, Axxess, and Webafrica which affected the Digital Subscriber Line (DSL) and fibre subscribers.
Although cyber-attacks were publicly reported no information was provided to suggest that the cyber-attacks were linked to malicious data software that put people's personal details at risk.

According to the Global Cybersecurity Index (GCI) 2017, South Africa is amongst the 77 countries classified into the Maturing Stage, this means that it has developed complex commitments and is involved in cybersecurity programmes and initiatives. This explains why South Africa has managed to control some major cyber-attacks; however, the country still has the third-highest number of cyber-crime victims worldwide.

South Africa Africa's Cyber Security Status Quo,

Since 2003 South Africa has adopted Cybersecurity Awareness Month in October with the international community, as part of the government's long-term vision to address South Africa's cybersecurity skills shortage (Kahla, 2019).
In context of the country's need to deal with cyber security challenges, the Cybersecurity Awareness Month theme Own IT. Secure IT. Protect IT was an attempt get all South Africans to accept responsibility. In synergy with the theme the Cyber Security Innovations Conference hosted between the 30-31 October in in Fourways, Johannesburg advocated a shift in organizational culture to improve cybersecurity, privacy and business resilience.
The Comparitech assessment survey of privacy protection and state surveillance was conducted in 47 countries to understand where governments are failing to protect privacy. The findings on South Africa were as follows (Bischoff, 2019):

- Privacy rights are protected through the constitutional court
- The landmark case (amaBhungane Centre v Minister of Justice)in which bulk interception by the National Communications Centre was declared unlawful by the High Court
- Limits are placed on data sharing, even between agencies within the same sector
- The country is not part of any invasive international treaties (but it is involved in tax-sharing agreements)
- Biometrics are on the rise and the newly introduced South African ID card contains fingerprints

- The Protection of Personal Information Act (POPIA) was promulgated to further enforce privacy rights, however the commencement date of many of its sections is not fully operational, this creates many grey areas.

In an interview with: Daily Maverick journalist Chelsey Moubray; Murray Hunter (2019), a researcher on surveillance issues said, "South Africa's data protection law – the POPIA Act – is not yet in force and South Africa's privacy watchdog, the information regulator, doesn't have legal powers yet and is operating on a skeleton staff. Until these things change, you can't say that people's privacy is adequately protected."

While South Africa does legally protect privacy, the penetration of sophisticated technology in homes, business, social sectors and government makes it easy for cyber criminals to illegally access confidential data such as bank accounts, identity numbers, credit cards, addresses, mobile numbers and so on.

Businesses that are or were victims of stolen data through cyber fraud can recover their data; however, it is very unlikely that they will restore their reputation especially with regards to customer trust.

The Comparitech survey, the Cyber Security Innovations Conference, media reports and advice from cyber security experts, provides insight on South Africa's Cyber Security status quo and the need to urgently take action and implement security mechanisms or a framework to govern cyber security across all sectors.

However, according to Budnik (2018), "PwC's 2018 Global State of Information Security Survey (GSISS) and PwC's 21st Annual Global CEO Survey, CEOs and boards named cyber-attacks as the business threat they were most concerned about, yet in the GSISS survey, 44% of respondents said they did not have an overall information security strategy".

Creamer Media's Engineering News (2019) reported that the ongoing battle to control cyber security is challenging for the following key reasons:

- South Africa has the third-highest number of cyber-crime victims worldwide and loses about R2.2 billion a year to cyber-attacks according to SABRIC.
- Malware attacks in South Africa increased by 22% in the first quarter of 2019 compared to the first quarter of 2018, according to global cyber security company Kaspersky Lab.
- Most of the cyber security companies in South Africa only service information Systems (IT) and not Operational Systems (OT).
- There is a huge shortage of digital security skills in South Africa, which makes vulnerable the country to attack.

The most challenging aspect of cybersecurity management across organisations

In South Africa many executive decisions makers lack skills to prioritise risks, therefore, many organisations have not established a cyber security governance model. Thus, leaders may experience a difficult time determining how to mitigate and remediate cyber risks in their organisations.
The Deloitte 2019 Future of Cyber Survey, in partnership with Wakefield Research, polled 500 C-level executives who oversee cybersecurity at companies between January 9, 2019, and January 25, 2019. Included in the on-line survey participants were requested to select their cybersecurity management challenges. Below is the analyses of their responses:

- Data management complexities 16%
- Better prioritisation of cyber risks across the enterprise 15%
- Rapid IT changes 15%
- Lack of skilled cyber professionals 14%
- Lack of management alignment on priorities 14%
- Lack of adequate funding 13%
- Inadequate governance across organisation 12%

Most South African organisation across business sectors are experiencing similar cybersecurity management challenges as indicated in the Deloitte survey findings.
Hence, at the Cybersecurity Innovations Conference 2019 some of the critical aspects that affects cybersecurity management was discussed such as (KIWEB's, 2019):

- Implementing a Cybersecurity Skills Competencies Framework
- Protection of Personal Information Act (POPI) and the relevance of General Data Protection Regulation (GDPR)
- Creating the right cyber security culture
- Creating future-proof resilient businesses in an ultra-connected world
- How to Articulate the Value of Information Security to Senior Management
- How does Global Expansion Affect Cybersecurity Risk

To effectively address cyber security risks every organisation needs to develop an integrated governance model aligned to technical vulnerabilities, business strategy and daily operations, this will avoid spending unnecessary time and resources. Ultimately the most effective solution would be to produce more cyber security skills through educational programmes and meaningful awareness campaigns.

Refences

1. Bischoff Paul 15 October 2019 Surveillance States: Which countries best protect privacy of their citizens? https://www.comparitech.com/blog/vpn-privacy/surveillance-states/ [Accessed 04 .11. 2019]
2. Budnik Kris 30 October 2018 Building a united front on financial crimes in the financial services sector https://www.pwc.co.za/en/press-room/cyber-security.html [Accessed 04 .11. 2019]
3. Creamer Media's Engineering News 22 October 2019 Why is South Africa among the most vulnerable countries to Cyber-crimes? http://m.engineeringnews.co.za/article/why-is-south-africa-among-the-most-vulnerable-countries-to-cyber-crimes/ [Accessed 04 .11. 2019]
4. Deloitte 2019 The future of cyber survey 2019 PDF https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf/ [Accessed 04 .11. 2019]
5. Head Tom 25 October 2019 SA banks targeted by "cyber attack" – here's how it affects us https://www.thesouthafrican.com/business-finance/banks-cyber-attack-friday-25-october-can-i-use-my-card/ [Accessed 04 .11. 2019]
6. International Telecommunication Union 2017 Global Cybersecurity Index (GCI) 2017 PDF Geneva Switzerland https://www.itu.int/dms_pub/itu-d/opb/str/ [Accessed 02 .11. 2019]
7. Kahla Cheryl 26 October 2019 Cybersecurity Awareness Month – Here's how to stay safe online https://www.thesouthafrican.com/tech/cybersecurity-awareness-month-october-2019-importance/ [Accessed 04 .11. 2019]
8. KIWEB's October 2019 Cyber Security Innovations Conference 2019. 30- 31 October at Radisson Blu Hotel in Sandton, Johannesburg https://kiweb.co.za/cyber-security-innovations-conference-2019-at-the-maslow-sandton-in-johannesburg/ [Accessed 05 .11. 2019]
9. Moubray Chelsey 21 October 2019 Delays in privacy laws are costing South Africans money and security https://www.dailymaverick.co.za/-delays-in-privacy-laws-are-costing-south-africans-money-and-security/ [Accessed 02 .11. 2019]
10. My Broadband 28 October 2019 South Africa is under attackhttps://mybroadband.co.za/news/security/324989-south-africa-is-under-attack.html [Accessed 03 .11. 2019]

For more information, email Bernadette Felix at bernadette@frtc.co.za or call 031 207 3245.

CONTACT US

www.frtc.co.za
www.facebook.com/felixrisktraining
info@frtc.co.za

B-BBEE Recognition :
Level 1 contributor to BBBEE
BEE Procurement Recognition Level : 135%

Black Ownership : 100%
Black Women Ownership : 100%
Empowering Supplier : Yes