Sub-Saharan Africa third highest exposure to cyber fraud

By Krevania Pillay

18 Apr 2017

Given that sub-Saharan Africa has the third highest exposure to incidents of cyber fraud in the world (Global Fraud Report), the revised draft Cybercrimes and Cybersecurity Bill, tabled in Parliament on 21 February 2017, is a welcome addition to the prevention of cybercrime.

© Gleb Shabashnyi – 123RF.com

What is cybercrime? It is defined as "any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the internet or any one or more of them" in the Electronic Communications and Transactions Amendment Bill, 2012.

Heavy cost to industry, government

In the 2016 Cost of Data Breach Study, conducted by IBM and the Ponemon Institute, the costs incurred by 19 organisations from nine different industry sectors were examined, following the theft of protected personal data. On average, the total organisational cost of a data breach in South Africa is R20.6 million.

According to the study, incidences of cybercrime and cybersecurity breaches are rapidly escalating globally with 64% more security incidents reported in 2015 than in 2014. South Africa is a target for cybercrime on the African continent, due to comparatively high internet connectivity in relation to other African countries. Among the numerous threats posed to South African business by cybercrime is the unlawful acquisition or interference with sensitive data relating to their clientele or business operations, and cyber fraud, in particular wire transfer fraud.

The Global Fraud Report ranks data deletion due to system issues as the most prevalent form of interference with data. Wire transfer fraud accounted for 26% of cyber fraud in sub-Saharan Africa, far ahead of the global average of 14%. Other forms of cyber-attack included viruses, and email based phishing attacks.

South Africans are defrauded in excess of R2.2 billion each year through online scams and cyber related crimes, according to the South African Banking Risk Information Centre.

On 12 February 2016, the Government Communications and Information Services database was hacked by hacktivist group 'Anonymous', resulting in a leak of the names, phone numbers, email addresses and passwords of approximately 1500 government employees.

On 16 February 2016, the South African Department of Water Affairs was hacked by the same group, resulting in the leak of sensitive data including usernames, passwords, full names, identity numbers, highly sensitive data and details of projects undertaken by that department.

At the 2015 Security Summit, held in Johannesburg, it was revealed that South Africa suffered more cybercrime attacks than any other country in Africa during a six-week period leading up to the summit.

In response to the elevated threat of cybercrime, the South African Reserve Bank announced, on 23 August 2016, the establishment of a special forum of all South Africa's major financial institutions to put together contingency measures to protect critical financial infrastructure from a prolonged cyberattack.

According to Reserve Bank Governor Lesetja Kganyago, "As a central bank and a regulator in the financial sector, the bank would be remiss in its duty if it ignored the growing risks emerging from the financial services sector's increasing reliance on cyberspace and the internet."

Bill seeks to reduce cybercrime

The escalation of cybercrime in South Africa has elicited legislative intervention from government in the form of the draft Cybercrimes and Cybersecurity Bill. The Department of Justice and Constitutional Development was mandated to review the cybersecurity laws of South Africa to ensure that these laws provide for a coherent and integrated cybersecurity legal framework. On 28 August 2015, the Department invited public comment on the Bill.

Having regard to the commentary of the public, a revised version of the Bill was tabled in Parliament on 21 February 2017, which has created several new offences for unlawful cyber activity including 'revenge porn'.

In terms of the Bill, the following activities are criminalised:

- Unlawful securing of access to data, a computer programme, a computer data storage medium or a computer system
- Unlawful acquisition of data
- Unlawful acts in respect of software or hardware tools
- Unlawful interference with data or a computer programme
- Unlawful interference with a computer data storage medium or computer system
- Unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices
- Cyber fraud

- Cyber forgery and uttering
- Cyber extortion
- Certain aggravated offences
- Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence
- Theft of incorporeal properties
- Unlawful broadcast or distribution of data messages which incites damage to property or violence
- Unlawful broadcast or distribution of data messages which is harmful
- Unlawful broadcast or distribution of data messages of intimate image without consent

The Bill imposes an array of penalties on offenders on conviction, who will be liable for fines or imprisonment for up to 15 years. It also creates infrastructure, such as the Cyber Response Committee and 24/7 Point of Contact, to promote cybersecurity within South Africa.

The Portfolio Committee on Justice and Correctional Services will now process the Bill, prior to referral to the National Council of Provinces.

This Bill address the immediate and costly threat cybercrime poses to business in South Africa and is a positive legislative leap in the anti-corruption space.

ABOUT THE AUTHOR

Krevania Pillay, an associate at Hogan Lovells (South Africa)