COMMUNICATIONS ENSIGHT

TMT ENSight
27 February 2019

Cybercrime legislation on South Africa's horizon: Is your organisation ready?

click to print this article

by Mpho Manyala-Chitapi

The implementation of cybercrime legislation is a pressing issue given that South Africa has one of the highest numbers of cybercrime victims in the world. In addition, a number of unsuspecting individuals and organisations alike fell prey to the scourge of cyber scams which seemed to spike quite rapidly in the past year.

The Cybercrime Bill was adopted by the Portfolio Committee for Justice and Correctional Services in November 2018 and sent to the National Assembly for debate. The National Council of Provinces will be considering written submissions from the public until 8 March 2019. This comes after an extensive public participation process which commenced in 2015. The most notable difference from the previous drafts is the conscious removal of the provisions dealing with cybersecurity, some of which were highly controversial and a cause for much debate.

The objectives of the Cybercrime Bill essentially include the codification and imposition of penalties on cybercrimes. Chapter XIII of the Electronic Communications and Transactions Act, 2002 was South Africa's first attempt at legislating for the codification of cybercrimes and the related penalties. The Cybercrime Bill, however, contains a wider range of cyber offences than those contained in the Electronic Communications and Transactions Act.

The Cybercrimes Bill further provides for mutual assistance in relation to the investigation of cybercrime. This has an impact on electronic communications service providers ("**ECSPs**") as well as financial institutions. ECSPs or financial institutions, such as a bank, may be required to work with law enforcement, where applicable, in the investigation of cybercrimes. In certain instances, this may involve the handing over of data and hardware. In addition, electronic communications service providers and financial institutions must report cyber offences within 72 hours of becoming aware of them. This may have devastating reputational effects on organisations, especially where an offence results from a compromise of their internal systems.

Furthermore, such organisations will be under an obligation to preserve any information that will be of assistance to the investigation. It is therefore important for organisations to assess the impact of the Cybercrime Bill on their business and understand exactly what their obligations are in order to avoid contravening the Bill and incurring penalties.

Some of the proactive initiatives that organisations should adopt include reviewing and introducing policies related to, among other things, social media, password policies, incident response plans/ security compromise policies as well as ensuring that staff are educated on cyber security issues.

For a discussion on how the Cybercrime Bill may impact on you organisation, please contact ENSafrica's TMT department.

Reviewed by Ridwaan Boda, head of ENSafrica's TMT department.

Mpho Manyala-Chitapi

technology, media and telecommunications | senior associate

cell: +27 82 310 2652