CYBERCRIMINALS ALWAYS SEEM TO BE ONE STEP AHEAD: WHY SOUTH AFRICA'S CYBERSECURITY LAWS NEED TO PLAY CATCH-UP!

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Lucien Pierce | August 5, 2016

South Africa has at least four pieces of legislation and one policy that can be used to fight cybercriminals. It is for this reason that some information security industry players have argued that one more cybersecurity law, such as the Cybercrimes and Cybersecurity Bill, is just too much.

They argue that laws like the Electronic Communications and Transactions Act 2002, the Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002, the Protection of Personal Information Act and the National Cybersecurity Policy Framework, are sufficient to combat the growing scourge of cybercrime.

The reality is that whilst each of these pieces of legislation has elements that address cybercrime, they are just not adequate enough to deal with the highly complex and multijurisdictional methods that cybercriminals now use. It would take a seasoned lawyer to extract the relevant provisions of each of the above pieces of legislation and to craft a satisfactory charge sheet or summons for some of today's complex cybercrimes.

Consider a hacker who breaches a company's security systems, steals its intellectual property, sells its clients' personal information, makes its computers slaves in a botnet and incapacitates its computer network by using ransomware. The lawyer would have to be an expert on and rely on portions of each of the above laws to address each of the different types of crimes committed in this example.

This is precisely why our laws need to play catch up, and why we need to have one comprehensive law that is able to account for any of the scenarios set out above. The recent R300 million Standard Bank credit card "hack" is a prime example of the multijurisdictional nature of cybercrime. The bank could possibly have had its South African systems hacked to steal the credit card information. Small time criminals based in Japan may have withdrawn the cash. Hackers based anywhere from Turkey, to Russia, to Brazil or the United States may well have been the masterminds of the heist.

Without one comprehensive cybercrime and cybersecurity law, that is able to address the complex issues that arise out of cybercrime, organisations that are victims of cybercrime and the organs of state tasked with investigating them, are going to have a much more difficult job on their hands. This is why we need the Cybercrimes and Cybersecurity Bill, a piece of legislation that will be on par with other similar international statutes such as the Council of Europe's Budapest Convention on Cybercrime.

The Cybercrimes and Cybersecurity Bill intends providing one comprehensive piece of legislation that can address the realities of present day cybercrime. It does so by:

- creating offences and prescribing penalties related to cybercrime;
- regulating jurisdiction, as well as the powers to investigate, search and gain access to or seize items in relation to cybercrime;
- regulating aspects of international cooperation in respect to cybercrime investigations;
- promoting best practice which requires that points of contact exist in various countries to

provide speedy assistance and investigation of cybercrime; and
- providing for the formation of a number of public and private sector structures in South Africa, that are intended to collaborate and assist with addressing cybersecurity and cybercrime.

South African organisations would do well to acquaint themselves with, and embrace, the Cybercrimes and Cybersecurity Bill. Where possible, they should also make inputs and submissions as it makes its way through the legislative drafting process. It is a necessary piece of legislation and will go a long way to enhancing South African organisations' ability to fight cybercrime, wherever the criminals may be.