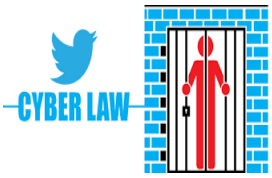
New Cybercrime Bill: Business must have a battle plan

In the light of the fact that the Cybercrimes Bill, now passed by Parliament, places obligations on financial institutions and service providers to report incidents to SAPS, it seems important that preparedness by business for a cybercrime incident needs to have a well-planned response plan in place.

Failure to report a serious incident of cybercrime, described quite clearly by definitions in the Bill after much debate, involves heavy fines. Follow-up involves investigative powers granted to SAPS, much of which would obviously involve the incident in question becoming a public matter, thus involving consumer affairs and invading share value.



Catch-up on crime

The knowledge that assets of the business can now be seized by investigators under defined circumstances, with the possibility of consequent damage to a balance sheet if not reported, is therefore a reality.

To a major extent, however, it is also realised by those who deal daily with the problems of invasive cyber fraud scams, clear definitions of what constitutes cybercrime and the capability of the state to join the fight, is agreed as being the outstanding main issue in combating the criminal element.

South Africa is high amongst nations where such crime exists and is a country where the profile of citizens is more subject criminal financial scams than most. An unsophisticated market place makes easy pickings for Internet criminal intentions, coupled with the fact that South Africa is fast becoming known as a gullible destination.

Alarm sounds

Urgent action against cybercrime has been called for over a number of years but this has been negated by plans of senior politicians over the same period to develop a response system that was seen as invasive. Inaction has been compounded by political interference, particularly as complainants saw the new control compounded by political interference.

With as much as R2,2bn being the estimated loss in terms of cybercrime annually in South Africa, Right2Know, coupled with a number of legal advisory firms and other interested bodies, have managed to constrain such state ambitions.

In fighting back, they seem to have managed to control the legislative build-up and a law that is acceptable to both parties arrived at, both at the same time acknowledging that South Africa urgently needs such legislation to combat cybercrime.

Lest we forget

In accepting the fact that the final Bill tabled is now more widely accepted, it might be seen as important to acknowledge the hard-fought process undertaken by civil society, those in the legal profession and importantly the Law Society of SA (LSSA. It has not been an easy walk in the park.

In a way, this battle reflects the times we live in, there being a lot more to the parliamentary statement

in 2018, which mildly read, “During its deliberations, the Portfolio Committee on Justice and Correctional Services has decided to only focus on cybercrimes issues, hence the change of the Bill’s name to the Cybercrimes Bill.” There is much more to this under the blanket, of course.

Many still believe that a sinister conflict of ideologies is still being fought out but for the moment this has been successfully overcome. There could be further legislation to come if the state does not undergo a change in its political profile, they believe.

Battle history

In early 2017, the then Minister of Justice and Constitutional Affairs, Jeff Radebe, published for public comment his Cybercrimes and Cybersecurity Bill, a broad and voluminous document, which was an update on an earlier 2016 draft, and which contained for example, an ominous Chapter 6 which ran for 30 pages with the title " Structures to Deal with Cyber Security". It read like a chapter of Animal Farm.

The Bill as proposed provided for the creation of no less than seven cyber security related state and para-state entities controlling information, the Bill being roughly divided in half between updated definitions as to what cybercrime was, the onus of businesses to report on same and with heavy penalties for failing to do so.

The really worrying half to the private sector, as put by the majors, was an extensive and lengthy section establishing cybersecurity institutions in government to counteract the spread of cybercrime.

Alarms sounding

The tone of the Bill deeply concerned all with its clear direction of political interference in communications. This initiated the LSSA into action, so much so that they said loudly, “It is also discomforting to note that this legislation emanates from the Justice, Crime Prevention and Security (JCPS) Cluster, so all is in essence a product of the State Security Agency.”

They added, “While the drafting of the Bill has been conducted under the auspices of the Minister of Justice and Correctional Services, it is nonetheless directed by the National Cybersecurity Policy Framework (NCPF), which is acting under the control of the State Security Agency in this instance.”

Big brother

The Law Society then immediately tackled the main reason for their objections. “Several aspects of the Bill reflect, in our opinion, an unacceptable bias towards law enforcement and national security at the expense of civil liberties and hard-won rights of our citizens. “At the least, this aspect requires closer attention and consultation.”

LSSA submitted that the 68 sections resulting in 128 pages of draft legislation was “not easy to digest” in legal terms and that the unnecessary duplication and incorporation of many common law principles in the Bill had contributed to their general decision that the Bill offended both common law and constitutional rights.

Second blast

American Chamber of Commerce in SA, a collective voice representing over 250 companies operating in the country, submitted that not only did the Bill offend the Bill of Rights but was totally unconstitutional in that "reverse onus of proof" was introduced by the proposed Bill.

They pointed to the "unacceptable fact" that any business entity or an individual had to show proof of innocence in failing not to report any alleged cybercrime, or otherwise be pre-judged as guilty, which would be a total contravention of their rights.

Amcham considered the Bill as vague and largely uninformed, pointing to the fact that the Bill as proposed also touched on copyright issues, which was a totally incorrect legal platform for such matters. They added that some of the proposals in the Bill directly contradicted international obligations.

All get together

They were joined on this issue by many civil society bodies, the legal profession and major IT and communications service providers, who all rejected the premise that for any cybersecurity agency not to provide evidential support of guilt and also impose very heavy penalties on this basis, was constitutionally unacceptable.

LSSA summed things up by concluding in their submission, "We believe that the (*Cybercrimes and Cybersecurity*) Bill goes some way towards extending the list of substantive cybercrimes that were initially limited in the Electronic Transaction Act of 2002."

Getting with it

However, they said, "Technology has progressed since the late 1990s and cybercrime is a much wider field contributed to by the unlawful use of personal and financial information to commit offences designed to steal confidential information." This draft Bill was silent on too many issues, they said.

In hearings which involved some one hundred other submissions from a cross-section of business and industry, LSSA warned in early 2017, "Any fast tracking of the Bill in its current form will have serious implications; may expose the Bill to constitutional challenges in Court; and may derail the bona fide intentions of the legislature to further regulate cyber criminality and aspects of cybersecurity."

This stance has paid off, it seems.

Getting it together

The revised version is now called the Cybercrimes Bill, named as such to make it obvious that the Bill is all about cybercrime and not about cybersecurity. It was tabled before Parliament in October 2018.

Deputy Minister of Justice, John Jeffery, said "The new Bill solves three problems, namely, by criminalising cybercrime conduct, dealing with the problem of 'the silo-based' approach to cybercrime law and aligning South African cybercrime laws with the international community."

Getting it right

LSSA noted the satisfactory inclusion in the final version of criminalising the distribution of malware with intent to commit acts of terrorism, espionage and extortion by ransom, having recommended a complete re-write of the Bill

Legal experts on IT, Michaelson's, said on the gazetting of the revised Bill, "We welcome the changes and they are something we have been asking for. The Department of Justice has resolved many contentious on government entities contained in the previous Bill", all of which was a polite way of saying that the Bill had been sandblasted from political interference.

They also noted that the crimes related to malicious communications are now expanded in the Bill but the section that makes fake news a crime has been removed, as have all the sections dealing with critical information infrastructures."

The sections dealing with intercepting communications and preserving evidence remain and were in order, they said, "as are the obligations on various organisations such as ECSPs and financial institutions to report cybercrime."

Media more relaxed

The sections offending the media were also changed. As outspoken Daily Maverick stated, "You may not have noticed, but in the final days of 2018 South Africa scored a win for internet freedom as legislators defanged the Cybercrimes Bill."

Cliff, Dekker, Hofmeyer has welcomed the Bill as well, noting recently that "all the substantive clauses regarding cybersecurity have been removed."

Set to go

Other key points in the final Bill approved are the inclusion in the definition of the word "computer" as also being "technologies which perform physical actions such as self-driving cars, devices attached to computers and also medical devices", all of which may possibly mean a giant leap by the Department of Justice towards embracing artificial intelligence.