Cybersecurity and Cybercrime

Background

The objective of cybersecurity is to reduce cybersecurity risks, to minimise successful cybersecurity attacks, and to build trust in and security of the internet. Cybersecurity includes the application of information security standards, the definition of appropriate cybersecurity organisations and the education of internet users.

Big and small enterprises, governments, as well as private internet users are facing similar threats in cyberspace.

Countries are setting up national cybersecurity strategies in order to protect their citizens, economy and environment. Critical infrastructure like telecommunications networks, power networks, (nuclear) power plants, and industrial complexes are potential targets of cyber attacks, which could have devastating consequences if not adequately countered. To counter this threat, countries are setting up Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs). The CERTs and CSIRTs coordinate planned and ad-hoc activities against threats to cybersecurity and ensure that there is international cooperation in this area.

The Current Legal and Regulatory Framework for Cybersecurity

The legal framework for cybersecurity matters is the ECTA of 2002. The ECTA provides for, inter alia, the following:

- Regulation of Public Key Infrastructure (PKI) and authentication and accreditation for electronic signatures;
- Legal, technical and operational framework for e-signature usage;
- Categories of electronic signatures;
- Preferred Authentication Service provider for government, namely the South African Post Office Trust Centre;
- Establishment of the South African Accreditations Authority; and
- Appointment of cyber-inspectors.

At an international level, the draft African Union Convention on cybersecurity spells out options for an AU-wide cybersecurity policy, lays the foundation for cyber ethics and deals with issues related to the use of electronic transactions, electronic signatures as well as an as institutional framework for the protection of personal data.

South Africa is also a signatory to international treaties such as the Budapest Convention and the SADC Model Law. The Budapest Convention remains the only international agreement that addresses cybercrime and is aimed at harmonising national laws and establishing international cooperation against cybercrime.

The SADC Model Law, which was produced 10 years ago, identifies offences that can be incorporated into national laws for the combating of cybercrime. These offences include illegal access, interception, data interference, espionage, forgery, fraud, pornography, xenophobic material and disclosure of details of an investigation.

Policy Reform & Trends

A draft cyber-security policy was published in May, 2011. The policy was developed under the DoC, but responsibility has now shifted to the State Security Agency. Today, the policy and implementation process related to the overall security framework is led by the State Security Agency. The redrafted policy was approved by Cabinet with the overall responsibility being given to the State Security Agency. This policy is currently not open for public consumption.

Gaps and critical success factors

The fragmentation of systems and non-alignment of law and polices still exist:

- While the ECTA recognises other forms of electronic signatures used between parties in an electronic transaction (for instance, a private agreement) these will not be recognised if the signature is required by law, such as signatures required in terms of the Companies Act 71 of 2008. To this end the Companies Act require advanced electronic signatures on issues such as signing of a memorandum of incorporation, financial statements, minutes of board meetings, and reservation of name notice.
- The Department of State Security, the Department of Justice and Constitutional Development (DoJ & CD) and the Department of Police are also involved in the curbing and prosecution of cyber crime. The DoJ & CD has the overall responsibility for cybercrime prosecution and court processes and is responsible for the implementation of the Regulation of Interception of Communications and Provision of Communications-Related Information Act (RICA).
- The Department of State Security is responsible for coordination, accountability and implementation of cybersecurity measures. It develops and implements regulations on cybercrime and collects intelligence and conducts relevant investigations. The Ministry of Police is responsible for the prevention, investigation, and combating of cybercrime.
- The Department of Defence and Military Veterans is responsible for the coordination, and implementation of cyber-defence measures. The Department of Science & Technology is responsible for the development, coordination and implementation of national capacity development programmes on a national cybersecurity research and development agenda for the country.
- Cybercrime and cybersecurity have become issues of national importance. In South Africa, the responsibility of policy making and implementation of measures to combat cybercrime and to enforce cybersecurity lies with government. However, research undertaken in this area highlights the fact that no single existing agency can claim a comprehensive understanding and a sufficiently wide authority to manage all facets of cybersecurity and cybercrime. Therefore effective coordination across government and its agencies, as well as co-operation at an international level are of paramount importance.

a) Data protection

The ECTA provided a legislative environment for secure electronic transactions in South Africa. The Act compelled the Minister of Communications to have due regard to international best practice when it comes to electronic transaction issues; introduced the concept of consumer protection by protecting individuals from unsolicited commercial communication, and set out principles that govern the protection of personal information.

Read together with the Consumer Protection Act (CPA) of 2008, the ECTA deals firmly with the issue of unsolicited communications. In this regard, the CPA reinforces the principles

espoused in the ECTA by empowering consumers to refuse to accept direct marketing through mechanisms that include registering a pre-emptive block of a marketer who manages a registry recognised by the National Consumer Commission (NCC).

Additionally, the Protection of Personal Information (POPI)Act will make it illegal for a direct marketer to market directly to any individual unless prior consent had been given, or unless that individual is an existing customer. The current vacuum from a policy perspective is the issue of the use of social media as a communication instrument. Users of social media are often not aware that there could be repercussions for their actions on social media. This area is not addressed anywhere in the ECTA and may need to be examined when new policies are developed.

b) Identify theft

Identity theft is very high in South Africa. The South African Fraud Prevention Service reported in 2008 that identify theft in South Africa could exceed R1 billion in annual losses. Traditionally, theft of personal identify happened when someone illegally obtained another person's hardcopy government-issued Identity Document (ID). As use of the internet rises, new forms of identity theft have emerged. Consumers' financial records can be highly impacted by persons who steal personal information through the use of computers and other devices. Typically these scammers target people using spam email, fake online banking websites and false online advertisements.

c) Online gambling and related activities

The National Gambling Act 2004 prohibited both offering interactive gambling services and engaging in interactive games (games on the Internet). Online sports betting, online horse race betting and the business of bookmaking is lawful in South Africa, provided that the person conducting such business holds the necessary provincial bookmaker's licence(s), or is using a website with proper licence(s).

d) Collection, preservation and production of e-evidence

Cybercrime is international by nature and therefore to combat it requires effective international cooperation of law enforcement agencies. This international cooperation rests on the harmonisation of law and the establishment of mutual assistance.

The internet is not restricted to any national border. While the victim of cybercrime may reside in one country, the offender might be in another country. This means that a multi-pronged strategy is required for the prosecution of cybercrime. Law enforcement agencies are confronted with additional challenges, including the fact that data tracks are elusive, which makes it difficult for these agencies to identify attacks and trace the offenders. The collection of electronic evidence needs to be supported by effective data collection processes and must be accepted in court as evidence.