Strengthening IT Security: Mastering the Key to Preventing Cyber Fraud

Cyber Crime in South Africa

Sizwe Lindelo Snail
Director, Snail Attorneys @ Law

E-mail: Ssnail@snailattorneys.co.za
Criminal Practice Issues:
Cyber Crime
1. Introduction

Computer crime or commonly referred to as Cyber Crime or ICT Crime (D van der Merwe (2008) 61) is a new type of criminal activity which started showing it’s ugly head in the early 90’s as the Internet became a common place for online users worldwide.

Cyber crime or also known as computer crime can be defined as any criminal activity that involves a computer and can be divided into two categories. One the one the it deals with crimes that can only be committed which where previously not possible before the advent of the computer such as hacking, cracking, sniffing and the production and decimation of malicious code (Ibid).
The other category of computer crimes are much wider and have been existence for centuries but are now committed in the cyber environment such as internet fraud, possession and distribution of child pornography to name a few.

In modern times there is more focus from protecting the “container” of valuables (the computer is merely the modern equivalent of a bank vault), only instead of money or gold it contains data) to protecting the real valuables in most ICT crimes, namely the data contained in the computer, the cell phone’s GPS device and so on. (D van der Merwe (2008) 63. The question then usually arises as to what types of criminal offences may be committed online and what laws one must apply to charge an offender to successfully get a prosecution.
Common law position: Prior to the ECT Act

2.1 Introduction

Prior to ECT, the common and statutory law at that time could be extended as widely as possible.

One can easily apply the common law crimes of defamation, indecency (Online child pornography, decimation of child porn), crimen injuria (also known as Cyber-smearing) fraud (Cyber fraud) (see the case of S v Van den Berg 1991 (1) SACR 104 (T)), defeating the ends of justice, contempt of court (in the form of publishing any court proceedings without the courts permission online or by other electronic means), theft (see the cases of S v Harper 1981 (2) SA 638 (D) and S v Manuel 1953 (4) SA 523 (A) 526 where the court came to the conclusion that money which had been dematerialized could be stolen in it immaterial form) and forgery to the online forms of these offences.
The applicability of the common law however has its own limitations and narrows significantly when dealing with online crimes involving assault, theft, extortion, spamming, phishing, treason, murder, breaking and entering into premises with the intent to steal and malicious damage to property.

When looking at the crimes of breaking and entering with intent to steal as well as the crimes of malicious damage to property two commonly known categories of Computer crimes come to mind. On the one hand, hacking and cracking and on the other hand the production and distribution of malicious code known as viruses, worms and Trojan Horses.
In *S v Howard* (unreported Case no. 41/ 258 / 02, Johannesburg regional magistrates court) as discussed by Van der Merwe, the court had no doubt whether the crime of malicious damage to property could apply to causing an entire information system to breakdown.

The Court also mentioned further that the crime no longer needed to be committed to “physical property” but could also apply to data messages of data information.

(D van der Merwe (2008) 70)
2.2 Interception and Monitoring Prohibition Act

The Interception and Monitoring Prohibition Act specifically governs the monitoring of transmissions including e-mail.

Section 2 states that: no person shall –

“intentionally intercept or attempt to intercept or authorize, or procure any other person to intercept or to attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission “

This means in simple terms that conduct that:

(a) Intentionally and without the knowledge or permission of the dispatcher to intercept a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line; or

(b) Intentionally monitor any conversations or communications by means of a monitoring device so as to gather confidential information concerning any person, body or organization,
2.3 Dangerous code

Dangerous code refers to any computer programme that causes destruction or harm and has been programmed in such a way with malicious intent.

Ebersoehn & Henning (JJ Henning & G J Ebersoehn (2000) 111) define a virus as:
“A piece of programming code usually disguised as something else that causes some unexpected and, for the victim usually undesirable event and which is often designed so that it is automatically spread to other computer users.”

They go on further and classify them as File infector viruses, system or boot record viruses and macro viruses. It must be noted that viruses can either be decimated or “contracted” by exchange of various media or by receipt in an e-mail.
Ebersoehn & Henning define a worm as:

“a type of a virus …. that situates itself in a computer system in a place were it can do harm” (JJ Henning & G J Ebersoehn (2000) 112)

The difference between a virus and a worm is the former has to be activated by the user and that worm on the other hand gains access to the computer and search for other internet locations infecting them in the process.
Ebersoehn & Henning define a Trojan as:

“A destructive computer programme disguised as a game, a utility or application. A Trojan horse does something devious to the computer system while appearing to do something useful”

It is submitted that with the court’s inherent power to develop the common law the creating and or decimation of the above dangerous codes could have resulted in successful prosecution relating to malicious damage to property.

The requirements of malicious intent and fault could easily be attributed in the form of dolus directus, dolus indirectus or even dolus eventualis and in some instances luxuaría (conscience negligence) could also be used were maybe the author of such a programme failed to take precautions to ensure that it does not fall in the public domain (even if it was for research purposes)
2.4 Child Pornography

Crimes such as possession and distribution of child pornography can be prosecuted in terms of the Films and Publications Act, Act 65 of 1996 which provided in its definition of publication that a publication is:

“(i) any message or communication, including visual presentation, placed on any distributed network including, but not confined to, to the internet. “

In terms of section 27 (1) and section 28 of the said legislation if anyone creates, produces, imports or is in possession of a publication or film which contains scenes of child pornography, he shall be guilty of an offence. Gordon also notes that the act may also extend to “pseudo-pornography” as found in animated pornography. (Barrie Gordon (2000) 439). Section 25 and section 26 also prohibit the decimation of child pornography in films or publications respectively.
2.5 Evaluation of e-Evidence at Common Law

Watney states that section 35(5) of the Constitution of South Africa finds application. Section 35(5) states that evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence render the trial unfair or will otherwise be detrimental to the administration of justice. (M Watney (2008) 2).

The constitutional court confirmed in the matter of Key v Attorney-General, Cape Provincial Division (1996 (6) BCLR 788 (CC)) ‘(b)ut there will be times when fairness will require that evidence, albeit obtained unconstitutionally, nevertheless be admitted.’ Issues of proof are traditionally classified under three headings namely: witnesses, objects (real evidence) and documents.
Technological advances have brought many new devices onto the market, some valuable in providing evidence. The products of these devices are sometimes regarded as real evidence and sometimes as documentary evidence. The current view is that it is real evidence unless it takes the form of paper or other material on which knowledge or thoughts are reproduced. (M Watney (2008) 3). Watney points out that In the S v Fuhri (1994(2) SACR 829 (A)) it was decided that the photograph of a vehicle whose driver had committed an traffic offence is real evidence, whereas in the S v De Villiers (1993 (1) SACR 574 (Nm)) the court found that a computer printout containing information, where the information had a human source, is a document. (M Watney (2008) 3)
Although *S v Ndiki [2007] 2 All SA 185 (Ck)* dealt with the admissibility of computer print-outs before the ECT Act, Van Zyl J made many relevant remarks pertaining to the admissibility of electronic evidence. The following remark was made by Van Zyl J in *S v Ndiki*:

‘It seems that it is often too readily assumed that, because the computer and the technology it represents is a relatively recent invention and subject to continuous development, the law of evidence is incapable or inadequate to allow for evidence associated with this technology to be admissible in legal proceedings. A preferable point of departure in my view is to rather closely examine the evidence in issue and to determine what kind of evidence it is that one is dealing with and what the requirements for its admissibility are’ [53].
Watney submits against the background of the Ndiki-case, one will have to look at the facts of a particular case and determine what type of evidence the data message represents.

Once the type of evidence has been determined, a two-phased procedure will be applicable namely:

(i) to determine the admissibility of the electronic evidence during a trial-within-a-trial and if the evidence is found to be admissible

(ii) the evidential weight of the evidence has to be determined.

Watney citing Hoffman states that questions relating to admissibility of electronic evidence must be decided in a ‘trial within a trial’. ‘A trial within a trial’ (Hoffman (2006) 1).
3. Cyber-crime in the Electronic Communications and Transactions Act
3.1 Background

In *Narlis v South African Bank of Athens 1976 (2) SA 573 (A)*, the Court held that a computer printout was inadmissible in terms of the Civil Procedure and Evidence Act 25 of 1965. It was also held that a computer is not a person. It was clear that the law regarding value of electronic data in legal proceedings required urgent redress.

This resulted in the premature birth of the Computer Evidence Act 57 of 1983. Section 142 of the said act made provision for an authentication affidavit in order to authenticate a computer printout. The Computer Evidence Act seemed to make more provision for civil matters than criminal ones. It created substantial doubts and failed the mark for complimenting existing statues and expansion of common principles. (M Kufa (2008) 18 -19)
3.2 The Electronic Communications and Transactions Act, Act 25 of 2002

- After many years of legal uncertainty, Parliament enacted the Electronic Communications and Transactions Act, Act 25 of 2002 (ECT) which comprehensively deals with Cyber-crimes in Chapter XIII and has now created legal certainty as to what may and not constitute Cyber-crime.

- One must however, note s3 of the ECT (its interpretation clause) which does not exclude any statutory or common law from being applied to, recognizing or accommodating electronic transactions – in other words the common law or other statues in place wherever applicable is still in force and binding which has the result that wherever the ECT has not made specific provisions for criminal sanction such law will be applicable. (S Snail (2008) 65)
Section 85 defines ‘cyber crime’ as the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorized to access that data and still continues to access that data (S L. Geredal (2006) 282).

Section 86(1) provides that, subject to the Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.
In the case of *R v Douvenga (District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2003, unreported)* the Court had to decide whether an accused employee GM Douvenga of Rentmeester Assurance Limited (Rentmeester) was guilty of a contravention of section 86(1) (read with sections 1, 51 and 85) of the ECT Act.

It was alleged in this case that the accused, on or about 21 January 2003, in or near Pretoria and in the district of the Northern Transvaal, intentionally and without permission to do so, gained entry to data which she knew was contained in confidential databases and/or contravened the provision by sending this data per e-mail to her fiancée (as he then was) to ‘hou’ (keep).

The accused was found guilty of contravening section 86(1) of the ECT Act and sentenced to a R1 000 fine or imprisonment for a period of three months. (S L. Geredal (2006) 282). Hacking has now been entrenched in our law in s86 (1) of the ECT which makes any unlawful access and interception of data a criminal offence. This also applies to unauthorized interference with data as contained in s86 (2) of the ECT.
Section 86 (4) and 86(3) introduces a new form of crime known as the anti-cracking (or anti-thwarting) and hacking law. In terms of Section 86 (3) the provision and, or selling and, or designing and, or producing of anti-security circumventing (technology will be a punishable offence. (GJ Ebersoehn (2003) 16)

In terms of section 86(4) it is requirement to be guilt of this offence if the offender uses and designs a programme to overcome copyright protection, with direct intent to overcome a specific protection data protection programme (GJ Ebersoehn (2003) 17).
Denial of service (DOS) attacks also popularly known as Disk Operating System attacks, are attacks that cause a computer system to be inaccessible to legitimate users.

Section 86(5) states that, “any person who commits any act described in Section 86 with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial of services to legitimate users is guilty of an offence”.

The act or conduct is fashioned in such a manner that it is widely defined and consist of any of the action criminalized in Sections 86(1) – Section 86 (4). The actions include unauthorized access, unauthorized modification or utilizing of a program or device to overcome security measures. (M Kufa (2008) 20)
Similarly one can deduce that e-mail bombing and spamming is now also a criminal offence as contained in the wide definition of s86 (5) and s45 of the ECT respectively.

Section 87 of the ECT also has introduced the Cyber crimes of E-Extortion as per section 87(1), E-Fraud as section 87(2) and E-Forgery as section 87(2). Section 87(1) provides an alternative to the common law crime of extortion. Kufa states that pressure is therefore exerted by threatening to perform any of the acts criminalized in section 86.

Kufa also criticizes this section as “wet behind the ears“as its common law equivalent applies to both forms of advantage of a propriety and non-propriety form. He suggests that this proviso is wanting and will require redress. (M Kufa (2008) 21)
3.3 Other statutory remedies

- Cyber crimes are not limited to the acts as contained in the ECT but there are also other statues that are applicable in the prosecution of Cyber crimes.

- For instance, in terms of the Prevention of Organized Crime Act (POCA) and FICA Act the prevention of all the crimes (as applicable to the cyber environment) listed is highlighted (but in an organized fashion) as well as the prohibition of money laundering and other financial related crimes which are these days done online which may also contravene the Exchange Control Regulations.

- Also noteworthy is the National Gambling Act and Lotteries Act. In terms of s89 of the National Gambling Act any form of unlicensed gambling is unlawful and may be imprisoned for period of 2 years. Similarly s57 and s59 of the Lotteries Act also states that “any unlicensed lotteries or anyone participating in a foreign lottery is liable to a criminal offence”.
Other statutory remedies cont.

• Notwithstanding Section 86 (4) which outlaws the cracking of anti-pirating and or security software. It is also important to state that the sale and or making available of illegal copies of movies or music online (in formats such mpeg4, Divx, mov, mp3, wav, mwa etc) an individual may be in contravention of the Copyright Act in terms of which s27 of the Copyright Act prohibits the unlawful copying, decimation and, or distribution of copyrighted works.

• The provisions of the Counterfeit Goods Act may also be applied were the sale of such counterfeit goods (in this context reference to goods is the illegal copy of the movie or song) was concluded online.
4. Procedural aspects of Cyber-crimes
Legal Aspects impacting on Law enforcement of Cyber crimes
(Procedural aspects of Cyber crimes)

4. 1 Admissibility and Evidential Weight of data Messages (ECT Act S 15)

- After much legal uncertainly as to the admissibility of a printout in Court in terms of the Old Computer Evidence Act, Section 15 of the ECT, now states that the rules of evidence must not be used to deny admissibility of data messages on grounds that it’s not in original form. A data message made in the ordinary course of business, or a printout correctly certified to be correct is admissible evidence. It constitutes rebuttable proof of its contents when it is produced in the form of a print-out.[1]

- The Act now states that Data messages shall be admissible giving due regard to reliability of manner of storage, generation and communication, reliability of admission manner of maintenance of message, manner in which originator is identified, and any other relevant factor. In other words the Act creates a rebuttable presumption of that data messages and or printouts thereof are admissible in evidence.[2]

[1] Also see the case of S B Jafta v Ezemvelo KZN Wildlife ( Case D204/07 ) where a e-mail used to accept an employment contract was regarded s conclusive proof the the said employment had been accepted.

[2] also see the controversial case of S v Motata where electronic information ( data in the form of images and sound) from cell phone was admitted into evidence in a trial within a trial ( the case has yet to be concluded )
The Act now states that Data messages shall be admissible giving due regard to reliability of manner of storage, generation and communication, reliability of admission manner of maintenance of message, manner in which originator is identified, and any other relevant factor. **Section 15(4) of the ECT Act** provides that data message made by a person in the ordinary course of business, or a certified copy, printout or extract from such data message **"is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract."**

The copy, printout or extract is to be certified to be correct by an officer in the service of the person making the data message. In other words the Act creates a **rebuttable presumption** of that data messages and or printouts thereof are admissible in evidence. (See also the controversial case of **S v Motata Johannesburg District Court case number 63/968/07 (unreported) at 622**, where electronic information (data in the form of images and sound) from a cellphone was admitted into evidence in a trial within a trial ).
When giving judgement, the court must decide what weight to attach to the evidence when evaluating the totality of the evidence. Guidelines and presumptions assist the presiding officer. The following guidelines will assist the presiding officer: (M Watney (2008) 7). 15(3) states in assessing the evidential weight of a data message the court must take regard to:

(a) the reliability of the manner in which the data message was generated, stored or communicated;
(b) the reliability of the manner in which the integrity of the data message was maintained;
(c) the manner in which its originator was identified; and any other relevant factor.’
4.2 Search and Seizure (ECT Act s82 (1))

The ECT has now created “Cyber-Inspectors” who, with the authority of a warrant, may enter any premises or access information that has a bearing on an investigation (into possible Cyber crime). Their powers have been well defined in the Act which includes the authority to search premises or information systems, search a person or premises if there is reasonable cause to believe they are in possession of article/document/record with bearing on investigation.

- Cyber inspectors may also demand the production of and inspection of any licences or registration certificates in respect of any law, take any extracts of books or documents on any premises or information system with a bearing investigation, and also the power to inspect any facilities on premises with a bearing on an investigation.

- To avoid issues of unnecessary red-tape which may hamper a prosecution, Cyber inspectors are also empowered to access and inspect the operation of any computer or equipment forming part of an information system - used or suspected to have been used in an offence and require any person in control of, or otherwise involved with the operation of a computer to provide reasonable technical assistance.
4.3 Jurisdiction (ECT Act s90)

- Jurisdictional challenges are probably the main challenge that cyber prosecutors face in prosecution of cyber-crimes.

- Sec 90 of the Act gives South African courts the jurisdiction to try offences arising from actions where an offence is committed in the republic, any act in preparation for the offence takes place in the republic, any part of the offence is committed in the republic, the result of the offence has effects in the republic, the offence is committed in the republic, by a person carrying on business in the Republic or when the offence is committed on board any ship or craft registered in republic.

- There is much legal debate however as to whether this provisions in line with International law and the effect of other international treaties on the prosecution of Cyber-crimes.
5. Lessons learnt from European Union and USA

European Union

In the European Union Cyber crime law is primarily based on the Council of Europe’s Convention on Cyber crime (November 2001). South Africa has signed but did not ratify the Convention. Under the convention, member states are obliged to:

• criminalise the illegal access to computer system,
• illegal interception of data to a computer system,
• interfering with computer system without right, intentional interference with computer data without right,
• use of inauthentic data with intend to put it across as authentic (data forgery),
• infringement of copyright related rights online,
• interference with data or functioning of computer system,
• child pornography related offences (possession/distribution/procuring/producing of child pornography).

The Convention’s broad coverage of offences has drawn extensive criticism. Critics argue that it should limit itself to protecting the global information infrastructure by criminalizing “pure” cyber crimes. Fraud and forgery, they argue, are already covered in existing international agreements and should not be included in the Convention as “computer-related fraud” and “computer-related forgery.”[1]

Recommendations and conclusions

• Most of the Cyber crime provisions in the ETC are noble endeavours, however their enforceability is still to be tested in our South African Courts.

• Given the boarderless nature of the internet and the challenges it poses in terms of jurisdictional questions, international co-operation and uniformity it is of utmost importance that states learn from each others efforts to deal with Cyber crime and create an international Cyber crime code to be applied universally if any significant success is to be achieved in the combating Cyber crime.
Contact Us:

Sizwe Lindelo Snail

E-mail : ssnail@Snailattorneys.co.za / Sizwe_snail@yahoo.com
www : www.snailattorneys.co.za
Tel / Fax : (012) 362 6087
Fax : (086) 617 5721
Cell : (083) 477 4377