Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

South Africa - Computer Misuse Act, Proposed

In 1997 a Commission was started to investigate computer-related crime in South Africa (SA). The Commission released a very exciting proposal, called Discussion Paper 99, which if adopted will change the way the SA law system deals with computer misuse. This paper looks at this proposed act as well as its application in today's computer environment.

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.
watchfire

South Africa – Computer Misuse Act, Proposed.

Michael Masters

June 14, 2001

Introduction

In 1997 a Commission was started to investigate computer-related crime in South Africa (SA). The Commission released a very exciting proposal, called Discussion Paper 99, which if adopted will change the way the SA law system deals with computer misuse. This paper looks at this proposed act as well as its application in today's computer environment.

…imprisonment for a period not exceeding 5 years.
…imprisonment for a period not exceeding 10 years.[1]

These are the promising proposed penalties of Discussion Paper 99 for different computer offences of a country that seems to be taking a stand on computer crimes in their different forms. With this type of proposed legislation and penalties one feels a lot more confident about technology performing critical functions in the different spheres of human life such as commerce, banking, health and government services.

One would think that SA would be far behind world trends with respect to looking at cyber crime and its legislation but after some Internet research with articles like those on the World Information Technology and Services Alliance's (Witsa) website, it seems that, apart from a couple of the first world countries like the United States (USA) and the United Kingdom (UK), most countries are still developing cyber laws and even the above-mentioned countries' laws are still changing to better suite the environment it is trying to protect. SA however still has the advantage of being able to investigating current misuse laws from other countries and looking at relevant cases that have been tried within these legislations and from this information building its own act that will successfully embrace the relevant issues and set a legal infrastructure through which the courts in SA can prosecute cyber crimes. An added help to SA's efforts to build proper legislation is its membership to organizations like the Council of Europe which among other things is trying to set a legal infrastructure standard which all member countries could follow and benefit from.

With these advantages in mind Discussion Paper 99 poses three questions that form the starting point of defining a policy on computer misuse and which will be examined below:

1) Should the unauthorized accessing of computers and the unauthorized modification of computer data and software applications attract a criminal sanction?
2) Is it necessary to create new offences to criminalize these actions?
3) What provision should be made for the investigation and prosecution of such offences, given the unique nature of electronically stored information?[2]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

What constitutes a crime?

A common sentiment expressed about the Internet is that it is borderless and free and this opinion seems to be one of the major reasons why it is so popular and has grown into the giant it is today. With this sentiment it is difficult to impose laws without the impression that a body wants to "control" this cyberspace. As with early civilizations, the need for a legal infrastructure to protect what is deemed "just" or "right" has become crucial, with respect to the Internet, so that individuals through to industries can lay their trust in this medium and use it as effectively as possible.

So with a basic idea of why we need legislation that can deter would-be offenders in cyber-space the question of what constitutes a punishable crime in the eyes of the proposed South African misuse act must be considered. If one looks at current legislations in other countries, a major issue being faced is the wide scope of ways to commit a computer offence and what is worse is that it is continually changing with each new technology wave. It would be very difficult to have specific legislation relating to each type of offence, so what has rather been suggested is to look for a common denominator in all these offences. That denominator seems to be that the offending party does not have the authority needed to do what he/she is doing and from this one can conclude that any unauthorized use with respect to computers should be a punishable crime.

With the conclusion that we definitely need some type of legislation to stop unauthorized computer misuse let us look at current South African legislation.

Current Acts

Looking at current laws, two questions arise. Firstly, can current laws be successfully applied to computer misuse in all its different forms, and secondly, if they can't be applied, can the current laws be practically extended to include computer misuse applications?

Let us sample three current laws that might practically be used in a computer misuse case.

Malicious injury to property

> The unlawful and intentional damaging of another's property. [3]

One of the restrictions to this law is that damaged property must be corporeal, or in other words it must be physical. One cannot therefore successfully apply this across the spectrum of computer misuse offences as computer offences normally deal with information in some form or another and information as stored on computers is by its nature abstract and not corporeal.

Housebreaking

> The unlawful breaking into and entering a premises with intent to commit a crime.[4]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Again one has to look to the definitions of terms used in these laws. An important one used here is “premises”. In SA’s legal system this word only has physical connotations and so, as in the above law, it is not applicable to the computer environment.

The Trespass Act

> entering or being present on fixed property without the requisite permission.[5]

In this law an important element is the necessity of a physical presence to commit the offence. From a computing perspective there will rarely be any physical presence where a breach occurs, so again it does not easily get applied to cyber-crime cases

The above-simplified examples put across the point that the current laws were written without knowledge of the computing world and the abstracts that come with it, and hence do not easily apply to it. We are therefore left with two possibilities. The first of which is to extend the current laws to deal with these new offences, and the second is to create a new act that defines new offences. The SA government will soon make an answer in this regard.

Procedural Aspects

As with the discussion of whether our current legislation is capable of handling computer misuse issues, we also have to consider whether our current procedural aspects of the law are suitable. Legal procedures basically consist of the gathering and handling of evidence and the legalities attached to this.

For this we look to The Criminal Procedure Act 51 of 1977. On close inspection of this act it is clear that it was not designed with the Internet in mind. The procedure around search warrants is a worthy example to demonstrate the inadequacy of current procedural legislations because for a warrant to be issued one is required to specify the location over which the warrant is applicable and in the majority of cases location cannot be determined. Once again, therefore, we are faced with either having to extend the current applications of the act, or to create a new act specifically written for this legal domain.

Two very contentious issues that fall in this area are “Admissibility of Evidence” and “Jurisdiction”.

Admissibility of Evidence

The current act that addresses this topic is the Computer Evidence Act 57 of 1983. However as detailed in “A Green Paper on Electronic Commerce for South Africa”, this act has already been investigated by the South African Law Commission and found to be inadequate.

Allowable as evidence. [6]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

This dictionary definition above captures the essence of evidence tendered for review but to extend the meaning for practical purposes one can say that the evidence must be relevant to the case in question and must be in a format accepted by the courts. Both these elements must be present before the court will consider the evidence as applicable to a case.

A simple example showing the difficulties involved with the application of the above laws is as follows. The courts when looking at the admissibility of evidence generally require two aspects from the format of the evidence tendered which are originality and authenticity. This means that the courts require originals of the evidence, or if the original is not available then the copy must be proven to be a true copy. When dealing with information from a computer system the problem arises as to how to prove that the information is original and, if it is a copy, whether it is in fact a true copy. As mentioned in the paper, "A Green Paper on Electronic Commerce for South Africa",

In the electronic environment, the distinction between original and copy becomes blurred. [7]

Jurisdiction

One of the large advantages to a standards organization like the European Council, mentioned earlier, is that if it can form some type of legal standard across multiple countries then cases where jurisdiction issues arise should be far easier to handle efficiently and timeously. Two current legal issues as explained below demonstrate this problem.

The first deals with the litigation of a company known to the public as Napster. The successful litigation of this company by five large record companies in the USA was welcomed in the business sector, as this was a classic case of infringement of US Copyrighting Laws. The justice system in the USA successfully stopped this abuse but the question raised was that if a Non-US company were to host a similar type of service as Napster and that country's laws were not similar to those of the USA, would there be a different outcome and could the offenders be brought to justice?

The second case, which is still ongoing as I write this paper, involves France suing Yahoo for selling Nazi items on its website, because under its legislation these Nazi items can be litigated under the "anti-hate speech" laws. Yahoo, based in the USA, maintains several websites that cater for multiple nationalities and in regard to each relevant nationality they make sure that the laws of that nationality are adhered to but they cannot stop people from one nationality from looking at websites designed for another nationality.

I'm sure the world will be watching the outcome of this case with interest as it will be cases like these that forge the future with respect to international jurisdiction laws.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

After looking at the impact both cases above could have, it brings to mind the more serious cyber-offences such as viruses like “Melissa” or “I Love You”. If the specifics of enforcing laws across international boundaries with respect to cyber-crimes cannot be clarified and agreed upon it opens up Internet abuse for future generations and compromises the future success of the Internet.

Looking at the above issues one can see the importance of defining laws to cater for the procedural issues that arise with computer misuse acts.

Culpability

Deserving blame. [8]

The last aspect I will cover in this paper is the important aspect of culpability as defined above. With all the advantages that the Internet has brought it has brought along with it the disadvantage of lowering the criminal entrance level. In other words, currently it is far easier to perpetrate serious and petty offences in the cyber world and get away with it than in the physical world. It is also far easier to hide behind “ignorance” when having caused damage or mischief and say you weren’t aware of what you were doing. Obviously the creation of specific legislation as discussed in this paper goes a long way to solving this problem but what about the grayer areas where it is not obvious that the perpetrator meant what he/she did? The decider here according to Discussion Paper 99 depends very specifically on what the perpetrator meant to do or even what he/she knew they were going to do by performing the offence and also that they knew it was unauthorized. In legal terms this is called “intent” and one can therefore summarize as follows. Unauthorized “intent” is what provides culpability and should be punishable by law.

Conclusion

In today’s computer world where most industries have realized the benefits of changing physical process flows into computer-managed process flows it is imperative, if the Internet is to be used to its fullest extent, that proper legal systems be put in place to deter misuse. If countries like SA are taking such a positive stance in this arena it makes for a very exciting “e-future”.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Quotes:

[1] Discussion Paper 99, p.67
[2] Discussion Paper 99, p.3
[3] Milton 765; Snyman 544
[4] Milton 792; Snyman 550
[5] Discussion Paper 99, p.11
[6] The Concise Oxford Dictionary of Current English
[7] A Green Paper on Electronic Commerce for South Africa, p.29
[8] The Concise Oxford Dictionary of Current English

References:

South African Law Commission. "Discussion Paper 99". August 2000
URL: http://www.gov.za/documents/01sublist.htm (28 June 2001)

Department of Communications, SA. "A Green Paper on Electronic Commerce for South Africa". November 2000
URL: http://www.ecomm-debate.co.za/greenpaper/index.html (28 June 2001)

http://www.law.wits.ac.za/salc/discussn/discussn.html

http://securityportal.com/articles/limits20010618.html

McConnell International. "Global Cyber Crime… and Punishment? Archaic Laws Threaten Global Information". December 2000
URL: http://www.witsa.org/papers/ (28 June 2001)

McConnell International. "Ready? Net. Go! Partnerships Leading the Global Economy". May 2001
URL: http://www.witsa.org/papers/ (28 June 2001)

http://www.coe.int/

http://www.cert.org/tech_tips/FBI_investigates_crime.html

Milton
Milton J R L South African Criminal Law and Procedure vol 2 3rd edition Cape Town: Juta 1996

Snyman
Snyman C R Strafreg 3rd edition Durban: Butterworths 1992

The Concise Oxford Dictionary of Current English; Eighth Edition

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced