Cyber Crime Influencing Businesses in South Africa

Marlien Herselman
PE Technikon, Pretoria, South Africa

Matt Warren
Deakin University, Geelong, VIC, Australia

HerselmanM@techpta.ac.za

mwarren@deakin.edu.au

Abstract

This study shows that cyber crime is a recent addition to the list of crimes that can adversely affect businesses directly or indirectly. This phenomenon was not directly prosecutable in South Africa until the enactment of the ECT Act in July 2002. However this Act also prevents businesses to fully prosecute a hacker due to incompleteness. Any kind of commercially related crime can be duplicated as cyber crime. Therefore very little research appears or has been documented about cyber crime in South African companies before 2003. The motivation to do this study was that businesses often loose millions in cyber attacks, not necessarily through direct theft but by the loss of service and damage to the image of the company. Most of the companies that were approached for interviews on cyber crime were reluctant to share the fact that they were hacked or that cyber crime occurred at their company as it violates their security policies and may expose their fragile security platforms.

The purpose of this study was to attempt to get an overall view on how South African businesses are affected by cyber crime in the banking and short term insurance sector of the South African industry and also to determine what legislation exist in this country to protect them.

The case study approach was used to determine the affect of cyber crime on businesses like banks and insurance companies and higher education institutions. Each case was interviewed, monitored and was observed over a period of a year.

This study discloses the evaluation of the results of how cyber crime affected the cases, which were part of this study. The banks and higher education institutions felt that they were at an increased risk both externally and internally, which is likely to increase as the migration towards electronic commerce occurs. The insurance industry felt that they are not yet affected by external cyber crime attacks in this country.

Keywords: Cyber crime in South Africa, business, banking and insurance sector

Introduction

While the affects of cyber crime are well documented on overseas (particularly American, Australian, British and some European) companies, very little research appears to be available about South African companies. Research needs to be done on how badly South African companies are affected by cyber crime (if at all) and whether the newly promulgated laws will aid in preventing and prosecuting these crimes.

Material published as part of this journal, either on-line or in print, is copyrighted by Informing Science. Permission to make digital or paper copy of part or all of these works for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage AND that copies 1) bear this notice in full and 2) give the full citation on the first page. It is permissible to abstract these works so long as credit is given. To copy in all other cases or to republish or to post on a server or to redistribute to lists requires specific permission from the publisher at Publisher@InformingScience.org

Therefore the following research questions can be applied:

- How does cyber crime affect business in South Africa?
- To what extent do the laws (new and old) protect business in this regard to prevent cyber crime?

Case study research was chosen as the methodology. Yin (1998, p. 23) defines a case as *an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident and in which multiple sources of evident are used*. In this study, although sorely lacking in the South African context, legal cases are a matter of public record and may provide insight into how the various laws are and would be implemented. Attention will also be paid to information available from other sectors in South Africa (for example Banks, Insurance and some higher education institutions). The participants for this study were banks (2) and insurance agencies (2) in South Africa as well as Higher Education institutions (2). The data was collected through interviews and observations.

Cyber Crime Concepts

Crime is an aspect of society that adversely affects us all. Cyber crime is a recent addition to the list of crimes that affect us, whether directly or indirectly. Until recently much cyber crime was not directly prosecutable in South Africa due to the lack of applicable controlling legislation. That which was prosecutable often relied heavily on the judgment under common law or statutory legislation under non-related (i.e. not computer related) acts. Business is adversely affected by crime, regardless of the type. Cyber crime can be any kind of crime, ranging from hacking (seen as spying) to more serious damage of intellectual property (Defacing websites). Almost any kind of commercial related crime can be duplicated as cyber crime. Businesses often loose millions in cyber-attacks, not necessarily through direct theft but by the loss of service to customers and damage to the company's image.

Cyber crime is little different to any other kind of crime; the defining difference between cyber crime and traditional crime is that cyber crime is committed with the use of a computer (Whether it be a Desktop PC or an ATM machine). Almost all the kinds of traditionally accepted crimes could be performed with the aid of a computer (Gordon, 2000, p. 423). Crimes such as fraud and forgery are relatively easy to perform and occur very frequently however; crimes such as murder can also be attributed to cyber crime. For example: If a person broke into and damaged or affected the network that controls the lights and junctions of Railway tracks and two trains happened to collide killing twenty people, that could be construed as murder. Another (which studies have shown to be a fairly common) crime is Hacking. Hacking can be likened to espionage since the people hacking into systems are often just going in to have a look around (spying) without intending to do any damage to the system or its integrity (this is not always the case, some cases of hacking , usually called cracking also occurs). According to Long & Long, (1999, p. C215) cracking can be quite malicious and cause sever damage to systems and data integrity) this crime can be performed or executed from within or external to the organisation (Gordon, 2000, pp. 425-426).

Intellectual Property

The introduction of the Internet was seen by many as the beginning of the end for intellectual property rights (Hartnick, 1998). The growth of technology in this area has far outstripped the growth of the law in copyright issues (Bencivenga, 1997). The international nature of the Internet makes the regulation of intellectual property particularly difficult since each country has its own laws governing trademarks, copyright, patents trade names, etc. (De Villiers, 2000, p. 67). The

majority of South African regulations of international intellectual property rights issues are governed by several conventions and agreements that have been ratified by the South African Government. These include conventions such as the Berne convention and the Paris convention with the *Trade Related Aspects of Intellectual Property Rights (TRIPS)* and *World Intellectual Property Organisation Treaty* covering the protection of trade of intellectual property. South African law covers most internal issues under the following Acts: Copyright Act 98 of 1978; Trade Marks Act 194 of 1993; Patents Act 57 of 1978 and Designs Act 195 of 1993. The Copyright Act makes no provision for protection under common law. The reason that even the older acts cover the Internet is because the Internet is seen merely seen as an alternative medium of communication (De Villiers, 2000, p. 39).

Internationally, several international Treatises deal with Intellectual Property issues such as copyrights. The treatise were arrived at by the World Intellectual Property Organisation (WIPO) and all member countries signed (South Africa been among them). These treatises govern how international issues should be dealt with.

Copyright

A problem with the ownership of websites is that the content and intellectual property may be owned by one or more persons, the designer and the owner of the website (domain name) may be different people. The different aspects are covered by different sections of the act, which may not yield a definitive answer to such an issue. An important aspect of the copyright act in Section 27 (Copyright Act 98 of 1978) makes it very clear that in order to infringe on a copyright that infringement must be intentional. An example is that if a person downloads a computer program to a computer is South Africa, but is unaware that it is a copy that infringes on someone else's copyright, he has not committed a crime. If however after he finds out he has violated the copyright and continues to use the said program he will be committing a crime (Gordon, 2002, p. 436).

Trademarks and Domain Names

Registered trademarks are protected by statutory regulations as well as by common law. A trademark is any mark used or, proposed to be used, by a person (legal entity) in relation to goods or services for the purpose of distinguishing that person's goods or services from those of another, Section 2(1)(xxiii) of the Trademarks Act (1993). Section 2(1)(xxiii) of the Trademark Act defines a registered *trademark that may include a device, name, signature, word, letter, numeral, shape, configuration, pattern, ornamentation, colour, container for goods or any combination of these.*

South African common law recognises that a person has rights acquired as goodwill, which attaches to a trademark. If a party attempts to use the goodwill of another party this is called passing off (Viljoen, du Plessis, & Vivier, 2000, p. 73). According to section 33 of the Trademarks Act, any statutory protection is offered in addition to any protection afforded under the Common Law.

An area of the Internet causing a large amount of conflict is the area of domain names, the reason been its conflict with trademarks. Two particular problems come to the fore when domain name registration needs to take place. Firstly, domain names must be unique (Internet Corporation for Assigned Names and Numbers), this in itself is not a problem, however in its relationship to trademarks, where multiple identical trademarks can coexist on the register, is poses the problem of only one proprietor is able to use their trademark in the corresponding domain name. Secondly, almost any domain name may be registered, including domain dames that are very similar (possibly even confusing) and the Trademark Act prohibits the use of confusingly similar trademarks.

Criminal Law

Just one decade ago, the realms of email were enjoyed only by a select few; today almost every person in the company from tea-girl to the General Manager uses it. It would be hard to imagine business today without the "connectedness" we get from email. This connectedness as well as the value of computer equipment has made it a target for computer-based crime. Crime that uses or affects computers can be divided up into three basic categories (Gordon, 2000, pp. 423-424) namely:

- Physical computer crimes – such as the theft of a printer or screen;
- "Ordinary Crime" traditional crimes been committed in new ways – such as online fraud or pyramid schemes;
- "New Crimes" Crimes that can be committed only with the use of a computer – such as hacking.

New Crimes

New computer crimes are crimes that can be committed solely with the aid or use of a computer. While some of these crimes are dealt with under ECT Act (ECT Act of 2002) and others under Common Law, others are dealt under other Acts. The most common and probably one of the few uniquely computer related crimes is hacking, hacking is commonly defined as "the unauthorised access of a computer system or network" (Gordon, 2000, p.425). Until the enactment of the ECT Act at the end of last year hacking was not a criminal offence.

Another uniquely computer related crime is the Denial of Service Attack (DOS) (Section 86(5) of the ECT Act (2002). This occurs when the perpetrator sets up a computer program (possibly a virus) that exploits the handshaking routine of requesting. The standard handshaking routine can be as follows:

- User's PC: Sends request to see if Server Active;
- Server PC: Sends Reply of Active;
- Users PC: Requests required page;
- Server PC: Sends required page.

Now in a denial of service attack the perpetrators program repeatedly (as often as possible – several hundred or more times a second) requests to see if the server is active, the server then sends the reply. The server then becomes so busy replying to the attack that it is unable to reply to genuine requests. The server may also eventually malfunction and eventually crash. Another method is to confuse the web server by sending it data it does not expect to receive, for example data packets of an unusual length. This may result in the server rebooting and thus denying service to legitimate users (Gordon, 2002, p. 48).

Electronic Communications Transaction Act

The Electronic Communications Transaction (ECT) Act is a statute designed to combat and prevent the rise and spread of cyber crime in South Africa. When President Thabo Mbeki enacted ECT Act in August 2002, it repealed the previous Computer Evidence Act. The only section of the ECT Act to deal with criminal activities directly relating to computers is Chapter XIII that deals with computer crime in two main sections. Section 86 deals with unauthorised access to, interception of, or interference with data. Section 87 deals with computer-related extortion, fraud and forgery. Section 88 deals with attempt, and aiding and abetting, and Section 89 with the penalties. The most important definition made in this chapter is the definition of "access". *"Access*

includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access the data and still continue to use that data" (ECT Act of 2002, Section 85)

The ECT Act does not cover crimes that are protected under other laws (whether Common law or statutes) but where there is a possible *lacuna* in the law, power is transferred from the ECT Act to the other Acts.

The ECT Act mainly protects companies or individuals against:

- Theft, Interception or Interference of Information;
- Theft, Fraud, Forgery and Extortion;
- Aiding and Abetting cyber crime;
- The ECT Act also provides for the penalties of contravening the act.

Significant numbers of states in the world have undertaken the effort to criminalize certain patterns of malicious behaviour online. Irrespective of the differences in the scope of the laws, the basic understanding of key terms and procedural obstacles with the enforcement, it seems that there are certain conducts which are included in all criminal studies against cyber crime in the world (Drozdova, 1999). The Drozdova survey comes to the finding that some thirty countries can be identified as having laws against computer and network misuse. Of these thirty countries each prohibits, in some way all, or most, of the following offences (Drozdova, 1999, p. 23):

- Unauthorized (illegal access);
- Illicit tampering with files or data;
- Computer or network sabotage;
- Use of information systems to commit or advance 'traditional' crimes (e.g. fraud, forgery, terrorism);
- Computer-mediated espionage;
- Violations against privacy by acquisition of computer-stored data;
- Theft or damage of computer hardware or software

Most countries deal with cyber crime in a way similar to South Africa, since many of the crimes (such as fraud) are already covered by existing law, the main purpose of "cyberlaws" is to help patch up any loopholes in the law and make specific provisions (such as the relevance of extradition).

Cyber Terrorism

A Merrill Lynch survey, released in July 2002, indicated that security is the number two concern of all Chief Information Officers (Betts, 2002, p. 1). According to Rusine Mitchell-Sinclair (In Betts, 2002, p. 1), the reasons for this are the September 11th events as well as the realisation that people need to protect their assets. With Cyber terrorism it would be possible for a terrorist to destroy real-world lives and properties by taking control of the floodgates of a dam, or the 300,000 Volts of power a substation handles (Gellman, 2002, p. 1).

After the September 11th terrorist attack against the USA, hackers used the medium of the Internet to voice their outrage. A group called the Dispatchers announced that they would destroy Web servers and Internet structures in Afghanistan and other countries that supported terrorism. They defaced hundreds of web sites and launched Denial of Service (DOS) attack against Iranian min-

istries and the Afghanistan presidential palace. A group called Young Intelligent Hackers Against Terror (YIHAT), claimed that they managed to break into two Arabic banks with ties to Osama bin Laden, officials of these banks deny any security breaches (Gaudin, 2002, p. 1).

Above is just one example of how Cyber terrorism is committed and what can be done (in a mild form). One way to attempt to curb Cyber terrorism is to pass anti-terrorism acts such as Great Britain's Terrorism Act 2000, which is a step in the right direction since it includes Cyber terrorism within the ambit of conventional terrorism. According to Nagpal this is not the ideal situation and Cyber terrorism should be dealt with as a separate issue (2002, p. 1).

Vatis (2001, p. 9) points out that cyber attackers are attracted to "High Value Targets"; he goes on to define high value targets as network infrastructures whose disruption would have a symbolic, financial, political, or tactical consequences. Palestinian group attacks on Israeli banking and financial institutions' web sites are a warning for potential attacks on the U.S economy (Vatis, 2001. p. 9). The white paper of the Center for the Study of Terrorism and Irregular Warfare ("Cyber terror," 1999) identifies three types of hypothetical cyber terrorist groups classified in accordance with their cyber terror capability:

- **Simple-unstructured**: The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control or learning capability.
- **Advanced-structured**: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control and learning capability.
- **Complex –coordinated**: The capability for coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defences (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organizational learning capability.

The study also determined that hacker groups are psychologically and organizationally ill suited to cyber terrorism, moreover they would have no interest in global scale disruption of Internet infrastructure ("Cyber terror," 1999).

There are striking similarities between the relationship of organized crime to the potential of cyber space and of global inter-networking, and the relationship of terrorists to the same potential. In their cyber-dimensions, none of the two exists or can exist as a stand-alone phenomenon. Both are rather the result of the attempt of facilitating traditional forms of organized crime. In this sense terrorism uses the Internet for encrypted communications, for recruiting supporters and for coordinating actions. But this places cyber terrorism in a completely different spot in the security priorities list than the one which is commonly being attributed to it (Milanovitch, 2003, p. 55). In this sense, it is still crime that is the problem to be targeted, not the cyber space. It is still terrorism, which endangers lives, not a malicious code or a denial of service attack. This could be taken further as a warning for all countries to be aware of the possibility of cyber attacks as a potential new terrorist tool.

South African Case Study Findings

The following research question will be addressed in this section: How does cyber crime affect business in South Africa?

The question was asked to ascertain whether businesses in South Africa are affected by cyber crime and to what extent. In order to answer this question the following data collection techniques were used:

- Interviews;
- Legal Case Studies.

Bank

Table 1 is a compilation of the questions asked during an interview with two bank managers in SA (Gordon, 2002). The answers giving were used to answer the question: How cyber crime affects businesses in South Africa?

Table 1: Bank Interview (Research Question 1)

No	Question	Answer
1.	With the increase of cyber crime occurring worldwide, do you think that the banking sector is at a risk of been affected?	Definitely. Bank losses from crime occur in two ways: branch robberies, where physical acts result in physical cash being taken from the premises; secondly, electronic crime, which is non-physical, and involves cash being taken only after monies have been transferred electronically and fraudulently.
	Do you think that the cyber crime would most likely be committed Internally (by staff) or Externally (people outside of the bank)	Bank fraud has been 50% external, and 50% internal, roughly speaking. Often there is collusion between insiders and outsiders. I have no reason to believe that cyber crime is/will be any different. In fact, because it is sophisticated and requires know-how, I wouldn't be surprised if cyber crime in banks becomes MORE dependent on help from inside (Gordon, 2003).
2.	Are Banks in South Africa been affected by cyber crime already and to what extent?	Definitely, if you include electronic crime/fraud. As I said, as banks move more and more to electronic transactions, fewer tellers, no cash, and internet banking, so cyber crime will take root. Crooks will HAVE NO CHOICE but to use cyber facilities.
3.	Given the current crime rate in South Africa, do you think crime will spread electronically (to cyber crime) and affect business in South Africa?	The above answer applies to business in general, in future. If you think how more and more business is being done on the internet, cyber crime will become inevitable.

4.	As people around the world move towards internet banking and away from a "hard cold cash" and the need for people to go to bank branches decline - how would cyber crime affect the transaction types and services offered by the bank be affected (for example home loans - would it be possible to do them online? What about documents the banks require like certified copies of ID's), in short what restrictions would cyber crime impose on these kinds of services.	All the big banks already have an internet home loan APPLICATION facility, and ABF APPLICATION facility (asset based finance, i.e. finance for vehicles, aircraft, factory equipment), but an individual or company still has to sign the agreement with the bank, and sign for having taken delivery of the asset. I'm not sure how the banks will get around not requiring a client's signature, but in future perhaps they'll find a way. The point is, Internet applications for bank finance is particularly vulnerable to fraud because it makes verification more difficult. The more you remove the human interface, the greater the opportunities for fraud. I'm afraid cyber crime has the potential to thrive unless banks and business in general remain a step ahead of increasingly cyber-literate crooks.
5.	Of what benefits is it for the banks to move towards a cashless society (EFT type transactions)?	Major benefits, esp. in RSA: Less admin intensive/less expensive, improved security, new product opportunities e.g. smart cards, lower insurance premiums.
6.	What are your feelings about cyber crime and banking?	Banking is a fertile ground for cyber crime by its nature, and I think it will become a major issue, here and internationally. Cyber crime will know no borders or physical boundaries; it will have no import/customs, or Forex constraints (Gordon, 2003).

Banks have always been targeted for crime. The concentration of wealth in one place makes it a fertile ground for crime. Banks have been exposed to cyber crime (if you consider the electronic fraud taking place from within the banks) and they expect it to increase. While bank fraud has been about 50% internal and 50% external many of the external jobs have relied on insider assistance (Gordon, 2002). It is thought that with the increase in sophistication of modern banking systems the collusion between insiders and outsiders will increase because outsiders will have more difficulty defrauding the system. One of the reasons banks expect cyber crime to increase is that as banks, business and individuals move away from cash based transactions and towards electronic transactions physical crimes will become more difficult to commit and thus a movement towards cyber crime is inevitable.

Cyber crime has no borders or physical boundaries, it is also not subject to import/customs or Forex constraints thus making it a target by any one from anywhere in the world (Gordon, 2002). Some of the major reasons for moving towards electronic banking in the Republic are that it is cheaper (due to been less admin and labour intensive), more secure (it is easier to protect electronic money than physical money) and the opportunities that can be explored such as smart cards.

While it is possible to use digital signatures as provided for under the ECT Act (ECT Act of 2002) legally, the risk of fraud, lack of personal interaction and Internet banking security risks remain significant stumbling blocks to be overcome.

Insurance

Table 2 is a compilation of the questions asked of the insurance agencies in the interview (J. Conradie, and F. Van Zyl, Personal interview conducted in 2003 at the insurance agency in Pretoria, South Africa). The answers giving were used to answer the question: How cyber crime affects businesses in South Africa?

Table 2: Insurance Interview (Research Question 1)

No	Question	Answer
1.	With the increase of cyber crime occurring worldwide, do you think that the insurance sector is at a risk of been affected?	With the advent of policies etc being available online, organisations would have access to policies and would be able to use the information illegally i.e. marketing, offering cheaper premiums obtaining personal info on-line.
2.	Do you think that the cyber crime would most likely be committed Internally (by staff) or Externally (people outside of the company)	There is probably more chance of cyber crime being committed internally as insurers do have strict access controls in place with passwords etc. it would be easier for an employee to access the info as they have the ability to obtain the info during the course of their duties. e.g. mutual and federal allow us to access our client's policies however we cannot access any clients that are not on our brokerage. Furthermore, we cannot "work" in the policies only view
3.	Is Insurance in South Africa been affected by cyber crime already and to what extent?	Possibly only with regards to the claims - this has been a continual problem for insurers for many years and the internet has probably made it worse
4.	Given the current crime rate in South Africa, do you think crime will spread electronically (to cyber crime) and affect business in South Africa?	At some point, cyber crime will probably start having an affect on business in South Africa as more and more people have access to computers and become "computer literate". This will probably affect certain sections of business i.e. banking, financial services etc. I do feel Insurance is not likely to be affected significantly by external crime in the near future.
5.	With the advent of Internet banking and a slow transition towards a cashless society (particularly the business sector) what kind of limitations does cyber crime impose on insurance?	Insurance companies both life and short term did away with the cash payment of premiums many years ago. it is only possible to pay for your premiums by means of a monthly debit order or any annual payment up front. Insurers at this stage will not entertain a policy that is paid monthly by the insured by means of an EFT transfer, claims settlements however are paid out by means of a cheque or EFT'S and this is where the weakness is for insurers.

6.	Of what benefits is it for insurances to move towards a cashless society (EFT type transactions)?	It would be impossible for insurers to administer premium payments by means of EFTS. It would be an administration nightmare! It is doubtful that insurance companies would ever go this route. Claims settlements, refunds etc are much safer being done by means of an EFT - posting cheques has become a thing of the past
7.	What are your feelings about cyber crime and insurance?	As with any other business in South Africa, the insurance industry is just as vulnerable to cyber crime - internally and externally. Of course this has an affect on insurance premiums as companies have to put extensive and expensive securities in place. Ultimately the man in the street ends up paying the price for this crime. Insurance is unlikely to move towards been internet based in the near future because of the complexities of underwriting a policy, this still needs human intervention and risk analysis.

Insurance has not significantly been affected by cyber crime until now (except for internal fraud), they do feel hover that they are unlikely to be affected in the short term- but definitely in the long term. None of the insurance companies in the country allow clients to take out insurance over the Internet, as of yet, however it is possible to get quotes. With the new ECT act in place this may however change now that electronic contracts are admissible in a court of law. The Insurance brokerage felt that they do not see a move towards Internet insurance in the foreseeable future (particularly for non domestic clients) because the process of underwriting accounts is a complex one that still needs to performed manually. The insurance agency did feel however that they are at an equal risk as any other financial services company to fraud, particularly of the internal kind.

Legal Cases

No legal cases directly attributed to cyber crime have been concluded in courts located within the Republic of South Africa yet. In 1998 there was a case that would now be possible to prosecute but at the time there was *lacuna* in the legislature. In 1998 in Port Elizabeth a man allegedly placed child pornography on his website (Gordon, 2000, p. 45). The Attorney General was unable to prosecute because legislation at the time did prohibit the offence (Storm Impact Inc Vs Software of the month club). One of the reasons been the *Films and Publications Act* was not yet enacted.

As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security. The present *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* were adopted as a recommendation of the OECD Council at its 1037th Session on 25 July 2002. The Security Guidelines were first completed in 1992 and were reviewed in 1997. The current review was undertaken in 2001 by the Working Party on Information Security and Privacy (WPISP), pursuant to a mandate from the Committee for Information, Computer and Communications Policy (ICCP), and accelerated in the aftermath of the September 11 tragedy (OECD, 2002, p. 4).

These Guidelines aim to (OECD, 2002, p. 5):

- Promote a culture of security among all participants as a means of protecting information systems and networks.
- Raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation.
- Foster greater confidence among all participants in information systems and networks and the way in which they are provided and used.
- Create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks.
- Promote co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures.
- Promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.

The implications of these "Guidelines" for South Africa are that these apply to all participants in the new information society and suggest the need for a greater awareness and understanding of security issues and the need to develop a "culture of security". Promotion of a culture of security will require both leadership and extensive participation and should result in a heightened priority for security planning and management, as well as an understanding of the need for security among all participants. Security issues should be topics of concern and responsibility at all levels of government and business and for all participants. These Guidelines constitute a foundation for work towards a culture of security throughout society. This will enable participants to factor security into the design and use of all information systems and networks. They propose that all participants adopt and promote a culture of security as a way of thinking about, assessing, and acting on, the operations of information systems and networks.

However if South Africa were to follow international precedence, then the courts would not tolerate the defence that the crime was committed online and that law does not specifically exclude cyber crime. Ignorance is not an excuse under the law. This has serious implications for South African cyber crime problems. Many cases of cyber crime were issued in the newspapers, but not yet fought in the courts:

- South African Universities were under attack of a hacker (University of Natal on May 21 2003, University of the North on April 18, 2003; Rhodes University on August 05, 2003; University of the Witwatersrand on August 07, 2002) ("New security for Standard Bank," June 2003, p. 1);
- Banks were under attack (African Bank on May 23, 2003; ABSA Bank on May 15, 2003) ("New security for Standard Bank," June 2003).

Further Findings on Cyber Crime

The South African Consumer Union (SACU) has called for a possible government intervention to protect clients against Internet banking fraud (Lombard, 2003). Smullen, director of operations at Active Card, an international company whose technology has been employed by European banks, indicated that the cyber crime events that happened recently with banks would speed up the process where banks will employ technology to ensure customers are protected. This would happen in spite of the fact that in terms of the ECT Act (2002), banks cannot be held liable for Internet

Banking fraud if the breach occurred on the side of the customer (Lombard, 2003). On 17 July 2003, hackers defaced more than 60 South African web sites. This is a new daily record and significantly higher that the previous record of 52 web sites defaces in one 24-hour period. On 20 July 2003 the Sunday Times reported that a 'hacker' cleaned out a number of ABSA bank accounts. According to the police and bank officials the 'hacker' used spyware to obtain usernames and passwords, essentially engaging in identity theft in siphoning off funds from unsuspecting users (“New security for Standard Bank,” June 2003).

Increased hack activity is not of course limited to South Africa. When police arrested Brooklyn, NY, busboy Abraham Abdallah in March 2002, he had Forbes magazine's issue on the 400 richest people in America, plus Social Security numbers, credit card numbers, bank-account information and mothers' maiden names of an A-list of intended victims drawn from the issue, including Steven Spielberg, Oprah Winfrey and Martha Stewart. Abdallah is accused of using websites, e-mail and off-line methods to try to steal the celebrities' identities and make off with millions in assets. One scheme that was caught in time: he allegedly sent an e-mail purporting to come from Siebel Systems founder Thomas Siebel to Merrill Lynch, directing that $10 million be transferred to an offshore account (Lombard, 2003).

Abdallah's high-profile arrest brought national attention to identity theft, which the FBI says is the nation's fastest-growing white-collar crime. An estimated 500 000 Americans have their identities stolen each year. A sign of the times: at least four insurance companies now offer ID-theft policies (Lombard, 2003).

The Privacy Rights Clearinghouse, which works with victims, says it takes an average victim of identity theft two years to clear his credit rating. A growing worst-case scenario: “criminal-identity theft” in which thieves use the stolen identity when they are arrested, leaving their victims with a criminal record that can be difficult to expunge.

South African businesses can certainly expect the profile of identity theft to increase in the years to come, as the country becomes a more integrated part of the global economy, essentially a world without borders.

The African Bank website was hacked onto by an unknown party but no permanent damage was done to the site and the home page was replaced within few hours. African Bank was looking at method of securing the website further, in cooperation with the service provider (“New security for Standard Bank,” June 2003). According to The Cape Times, the 7up hacker had invaded their website and defaced the site. 7up removed all the content from the bank's home page and left the following message: “7up owns African Bank.” 7up then hacked into more than 52 SA websites - mostly in the Western Cape - in less than 18 hours, however there is no evidence to suggest that the hacker gained access to bank accounts (Betts, 2002).

South African universities have come under attack before. On July 2, the IT Services website at the University of Cape Town was defaced by a hacker referred to as "h4ck3rsBr" (Lombard, 2003). Before that the University of Natal fell prey to attacks on May 21 and August 20. The University of the North was hacked on April 18, UCT on April 18 and the Medical University of South Africa on October 20 2002 (“New security for Standard Bank,” June 2003).

The ECT Act only covers business with respect to cyber crime in the following way:

- Theft, Interception or Interference of Information;
- Theft, Fraud, Forgery and Extortion;
- Aiding and Abetting cyber crime;
- The ECT Act also provides for the penalties of contravening the act.

It is thus evident that South Africa needs to learn from and apply the mentioned OECD guidelines in order to safeguard businesses and their vulnerabilities to cyber crime. Otherwise the customer will never be fully protected. To say a country has cyber crime laws but that these laws do not fully protect the customers who are the most vulnerable in all transactions on the Net.

Recommendations

Based on findings the following recommendations can be made:

1. International convention (treaty) across the globe could be a viable option.
2. Spreading the system rights amongst various proxies was a lesson learned as the hacker used single login to hack into the entire system.
3. Continuous training is required for the business clients in order to share the responsibility in a fight against cyber crime.
4. As indicated above, as the technology advances, so is the rate cyber crime, subsequently new cyber laws should emerge to counter attack rapid changes.
5. Reactive and proactive security measure should run in parallel in the cyberspace to strike a balance in fight against cyber crime.
6. There should be a continuous research and development in IT security.
7. Since the institutions vary, it is important to ensure the relevance of the security measures that are to be adopted depending on the line of business and common type of cyber attacks.

Conclusion

Findings indicate that cyber crime has not affected business in the Republic of South Africa yet, although it is expected to in the future. Technology is a double-edged sword; good for the good guys, good for the bad guys. This means steps need to be taken to ensure innocent parties are protected regardless of their geographic are. Many countries have taken the initial steps on introducing legislation to protect innocent people. However until the international nature of cyber crime is matched by the no-so-international nature of law protection can be offered against cross-border crimes. Whilst the laws of South Africa appear to be sufficient to protect against cyber crime, and expectations are the courts will follow in similar footsteps as their foreign counterparts, the proof is in the pudding and that will only happen when the courts are faced with cases to be heard. Governments around the world have recognised the threat of cyber crime and many have been pre-emptive in attempting to bring out legislation protecting against cyber crime. How effective these legislations are…. will still have to be put to the test.

References

Betts, M. (2002, July 15). IBM's view of the hot trends in IT security. *Computerworld*. Retrieved 27/08/2002 from http://www.computerworld.com/securitytopics/security/story/0,10801,72571,00.html

Bencivenga, C. (1997). Protecting copyrights. *The New York Law Journal. Internet*. Retrieved from http://www.ljx.com/internet/1016cpdig.html

Copyright Act 98 of 1978. Republic of South Africa.

Cyber terror. Prospects and implications. (1999, October). Retrieved 12/09/2003 from http://www.nps.navy.mil/citw/files/cyberterror%20Prospects%20and%20Implications.pdf

De Villiers, R. (2000). *CyberLaw @ SA*. Pretoria, South Africa: Van Schaik.

Drozdova, E. (1999). International responses to cyber crime. Retrieved 13/09/03 from http://hoover.stanford.edu/publications/books/fulltext/cyber crime/35.pdf

Electronic Communications and Transactions (ECT) Act of 2002. Republic of South Africa.

Gaudin, S. (2002). Security Expert: U.S. Companies Unprepared for Cyber Terror. Retrieved 29/08/2002 from http://itmanagement.earthweb.com/secu/article.php/1429851

Gellman, B. (2002, June 27). Cyber-attacks by Al Qaeda feared. *Washing Post*, p. 1.

Gordon, B Adv. (2000). *CyberLaw @ SA*. Pretoria, South Africa: Van Schaik.

Gordon, B Adv. (2002, August). Hacking, denial of service and the Electronic Communications and Transaction Act. *Servamus.*

Hartnick. (1998). Copyright & trademarks on the Internet. *The New York Law Journal.*

Leggat H, 2003. Hackers have a free ride in SA. Internet: www.buys.co.za Access date: August 2003.

Lombard, E. (2003, September 21). Alleged Absa hacker's secrets revealed in court. *Sunday Times*.

Long, L. & Long, N. (1999). *Computers*. New Jersey, USA: Prentice Hall.

Milanovitch, M. (2003). *Cyber crimes and spy games: Threats and dangers, but from whom?* Unpublished Masters dissertation, Diplomatic Academy of Vienna, University of Vienna.

Nagpal, R. (2002). Defining Cyber Terrorism. A paper submitted at the *National Seminar on Human Rights and Terrorism*. 9 and 10 March, 2002 at Nagpur, India.

New security for Standard Bank after Absa hacking, June 25, 2003. Retrieved 2003/08/11 from, www.sabcnews.com, 17:30. http://www.sabcnews.com/economy/business/0,2172,62864,00.html

Organization for Economic Co-Operation and Development (OECD). (2002). *OECD guidelines for the security of information systems and networks: Towards a culture of security*. Retrieved 25/09/03 from http://www.oecd.org

Trademarks Act 194 of 1993. Republic of South Africa.

Van Zyl, F. 2003. *Personal interview* with insurance agency as on 20/08/03 in Pretoria, South Africa.

Vatis, M.A. (2001). *Cyber attacks during the war on terrorism: A predictive analysis*. Hanover: Dartmouth College Printers. (Published Report).

Viljoen, Du Plessis, & Vivier. (2000). *CyberLaw @ SA*. Pretoria, South Africa: Van Schaik.

Yin, R. (1998). *Case study research: Design and methods*. United Kingdom: Sage Publications.

Biographies

Prof. M. E. Herselman is the Research Professor: Faculty of ICT at Technikon Pretoria. In this position she assists lecturers and post-graduate students with their research projects, NRF projects, articles and other research related activities. Since 1997 she has published several articles in various national and international journals and has presented papers at several international conferences. She has also been the team leader in a team research project in writing of a technical report funded by the NRF. Currently she has two NRF funded research projects and assists over 50 postgraduate students with their research projects. Her master's and doctoral students work on industry related projects especially focusing on ICT provision in disadvantaged communities in SA. Her field of expertise: All aspects of ICT in rural areas and HEI in South Africa.

Prof. M. Warren is the Dean of the School of Computing and Mathematics at Deakin University in Geelong in Victoria, Australia. He has been publishing articles since 1995 and has focused his research mainly on Information Technology crime. He has also assisted in writing the cyber crime laws pertaining to Australia.