CYBER CRIME AFFECTING SOME BUSINESSES IN SOUTH AFRICA

BY

MARTHA ELIZABETH HERSELMAN (BAEd, BEd, MEd, PhD)

Submitted in partial fulfilment of the requirements for the degree
Magister Technologiae Business Information Systems in the Faculty of Computer Studies at the Port Elizabeth Technikon

Date of submission
November 2003

Study leader:
Dr M Warren
ACKNOWLEDGEMENTS

The successful completion of this task would been impossible without the support, advise, assistance and encouragement of others.

I should like to record my sincere thanks and appreciation to the following:

Dr Matt Warren for his efficient guidance and continued encouragement from the beginning of this task to its completion.

Prof Rossouw Von Solms for constructive comments and inspiration to see this task through.

Elsa Strydom for her administrative support, efficiency and guidance.

Peggy Arendse for her meticulous proofreading and editing.

My husband (Phillip) and daughter Arlene for their encouragement and continued support as well as their understanding and patience.

My Lord and Saviour: “The Lord is my Shepherd”.

Marlien Herselman

Pretoria

November 2003
SUMMARY

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 2003.11.21

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. 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 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.
# TABLE OF CONTENTS

1.1 INTRODUCTION........................................................................................................... 1
1.2 PROBLEM STATEMENT............................................................................................... 3
1.2.1 Research objectives.......................................................................................... 3
1.3 METHODOLOGY....................................................................................................... 4
1.3.1 Case studies ..................................................................................................... 4
1.3.2 Data collection techniques................................................................................ 4
1.3.3 Participants ....................................................................................................... 5
1.4 IMPORTANCE /BENEFITS OF THIS STUDY............................................................. 5
1.5 PRELIMINARY LIST OF CHAPTERS ......................................................................... 6
1.6 DEFINITIONS OF CONCEPTS IN THE TITLE ......................................................... 7
1.6.1 The concept of "cyber crime"............................................................................ 7
1.6.2 The concept of "influencing" ............................................................................. 7
1.6.3 The concept of "business" ................................................................................ 7
1.7 CONCLUSION ......................................................................................................... 7

2. INFORMATION ABOUT CYBER CRIME AND THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT IN SOUTH AFRICA .................................................. 8
2.1 AIMS OF THIS CHAPTER ........................................................................................ 8
2.2 INTRODUCTION....................................................................................................... 8
2.3 DEFINING CYBER CRIME ..................................................................................... 8
2.4 INVESTIGATING CYBER CRIME ........................................................................... 9
2.5 INTELLECTUAL PROPERTY ISSUES ............................................................... 9
2.5.1 Current legislation ........................................................................................... 10
2.5.2 Copyright......................................................................................................... 10
2.5.3 Trademarks, domain names, patents ............................................................... 11
2.5.3.1 Registered trademarks.................................................................................... 11
2.5.3.2 Unregistered trademarks ................................................................................ 12
2.5.3.3 Domain names................................................................................................ 13
2.5.3.4 Patents ............................................................................................................ 13
2.6 CRIMINAL LAW ................................................................................................... 14
2.6.1 Physical computer crimes ............................................................................... 15
2.6.2 Ordinary crimes ............................................................................................... 15
2.7 NEW COMPUTER CRIMES .................................................................................... 17
2.8 ELECTRONIC COMMUNICATIONS AND TRANSACTION ACT ....................... 18
2.9 CONCLUSION ................................................................................................ 20

3. CYBER CRIME IN OTHER COUNTRIES AND THE EFFECTS ON SOUTH AFRICA ........................................................................................................... 22
3.1 AIMS OF THIS CHAPTER.............................................................................. 22
3.2 INTRODUCTION............................................................................................. 22
3.3 INTERNATIONAL ISSUES.............................................................................. 23
3.3.1 Intellectual Property ........................................................................................ 23
3.3.2 Criminal law ..................................................................................................... 24
3.3.3 International law .............................................................................................. 25
3.3.4 Extradition ....................................................................................................... 26
3.3.5 Cyber terrorism ............................................................................................... 27
3.4 CONCLUSION ................................................................................................ 29

4. CASE STUDY FINDINGS............................................................................... 30
4.1 INTRODUCTION............................................................................................. 30
4.2 RESEARCH PROBLEM ................................................................................. 30
4.3 RESEARCH METHODOLOGY ...................................................................... 31
4.3.1 Case study as a research method ................................................................. 31
4.3.1.1 Purpose of a case study ................................................................................. 31
4.3.1.2 Why do we carry out case study research?.................................................... 32
4.3.1.3 Planning a case study..................................................................................... 34
4.3.1.4 Advantages of the case study approach....................................................... 35
4.3.1.5 Disadvantages of the case study approach................................................... 36
4.3.2 Data collection techniques/sources of evidence............................................. 36
4.4 PARTICIPANTS ............................................................................................. 37
4.4.1 Legal case studies ........................................................................................... 37
4.4.2 Bank ................................................................................................................ 37
4.4.3 Insurance agencies ........................................................................................ 38
4.5 FIRST RESEARCH QUESTION ..................................................................... 38
4.5.1 Bank ................................................................................................................ 38
4.5.2 Insurance ........................................................................................................ 40
4.5.3 Legal cases ..................................................................................................... 41
4.5.4 Findings........................................................................................................... 46
APPENDICES

APPENDIX A: CASE STUDY – BANK INTERVIEW 60
APPENDIX B: CASE STUDY – INSURANCE INTERVIEW 63
LIST OF FIGURES

Figure 2.1: ECT Act domain of control 20
Figure 2.2: Structure of law 21

LIST OF TABLES

Table 2.1: ECTA related Acts 18
Table 2.2: ECT schedule 1 19
Table 2.3: ECT schedule 2 19
Table 4.1: Research Questions 30
Table 4.2: Legal cases 37
Table 4.3: Bank interview (Research question 1) 38
Table 4.4: Insurance interview (Research question 1) 40
Table 4.5: The OECD guidelines and discussions 43
Table 4.6: Bank interview (Research question 2) 47
Table 4.7: Insurance Company interview (Research question 2) 49
Chapter I

INTRODUCTION AND BACKGROUND

1.1 INTRODUCTION

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 what was prosecutable often relied heavily on the judgement 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) [Gordon, 2002b]. Almost any kind of commercial related crime can be duplicated as cyber-crime. Businesses often lose millions in cyber-attacks, not necessarily through direct theft but by the loss of service to customers and damage to the company’s image.

According to the 2002 Computer Security Institute’s computer crime and security survey on security trends and issues, 90 percent of respondents detected computer security breaches within 12 months with 80 percent acknowledging financial losses from these violations [Computer security institute, 2003; ITlink 2003: 26]. A Merrill Lynch survey, which was released in July 2002 [Betts 2002: 1], indicated that security is the number two concerns of all Chief Information Officers (CIO’s). One reason according to Rusine Mitchell-Sinclair, general manager of safety and security protection services at IBM [in: Betts 2002:1], is the September 11th events as well as the fact that people recognize that security is important to protect assets. In South Africa too cyber crime is on the increase as was evident from the ABSA Bank fraud case [Lombard, 2003:1]. Therefore risk assessment is high on the agenda. People want to know how good their security is in order to close the gaps that they have [Computer security Institute, 2003]. Therefore the critical infrastructure protection issue in information security is the real focus here. United States analysts also believe that by disabling or taking command of flood gates
in a dam, or of substations handling 300,000 volts of electric power, an intruder could use virtual tools to destroy real-world lives and properties [Gellman 2002:1]. The director of the FBI’s National Infrastructure Protection Centre, (Ronald Dick) has the same concerns. He fears a successful cyber-attack on respondents 911 or on a power grid more than a physical attack [Gellman 2002:2].

The latest Computer Crime and Security Survey from the Computer Security Institute (COMPUTER SECURITY INSTITUTE, 2003) and the Federal Bureau of Investigation (FBI), indicates that cyber-crime was on the rise for the third year in a row (Computer security institute, 2003: 5). This is the seventh annual Computer Crime and Security Survey, which aims to raise security awareness and discover the score of computer crime in the United States [Hollis 2002:1].

The survey is conducted by Computer Security Institute in conjunction with the San Francisco FBI’s Computer Intrusion Squad. The 2003 survey is based on responses from 503 computer security practitioners working in U.S. corporations, government agencies, medical and financial institutions and universities [Computer security institute, 2003:3, USA].

Most of the respondents—90 percent—had to experience computer security breaches in the past year, most of them large corporations and government agencies. Eighty percent experienced financial loss due to those security breaches. Of those, 223 respondents quantified their financial losses, reporting $455,848,000 in financial losses due to security breaches. The most serious financial losses were the result of theft of proprietary information and financial fraud. More of the respondents are reporting intrusions to law enforcement than in the past. In 1996, only 16 percent of respondents said they reported intrusions to law enforcement, while in the 2002 survey, 34 percent did so [CIW Community 2002:2; Computer security institute, 2003:5].

For five years running, more respondents said that their Internet connection is a frequent point of attack than said that their internal systems are a frequent point of attack. Seventy-four percent of respondents claimed their Internet connection was a frequent point of attack, compared to 33 percent who said their internal systems were a frequent point of attack. The survey revealed various types of attacks and abuses [Hollis 2002]:

---
• 40 percent of respondents reported system penetration from the outside.
• 40 percent reported denial of service attacks.
• 78 percent reported employee abuse of Internet access.
• 85 percent reported they had detected computer viruses.

According to Patrice Rapalus [in: Hollis 2002:2], the director of Computer Security Institute, the survey reveals that technology by itself can’t stop cyber-attacks and that there is still a need for cooperation between the private sector and government. It is indicated by Guadin [2002:1] that that threats from within organizations are greater than the threats from outside and “juveniles on joy-rides in cyber-space” perpetrate most cyber-attacks.

These factors together with the above statistics and devastating results of September 11 were the reason why this investigation into cyber crime and its effects on certain business in South Africa are important to pursue [Gaudin 2002].

The purpose of the study is to attempt to get an overall view on how South African businesses are affected by cyber crime and what legislation exists to protect them.

1.2 PROBLEM STATEMENT

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.

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) in South Africa protect business in this regard to prevent cyber crime?

1.2.1 Research objectives

The following objectives will be pursued in this study:
• Determine what areas of business are most affected by cyber-crime, which business sectors they fall in.
• Determine how effective our laws are in preventing cyber-crime (in comparison to International laws on cyber-crime).

1.3 METHODOLOGY

The research will be done with a qualitative method that will be used for collecting data from various sources. Qualitative methods are defined as methods that provide detailed and in-depth information. Qualitative data gives outside audiences an understanding of what a target population may think or feel about specific issues or a specific project in their community [Yin, 1989:6] Two methodologies will be used, the first been a literature study, the reason for this is to ascertain the current and proposed laws and to understand the in way the law is intended to work. The second methodology to be used is case studies (particularly legal cases).

1.3.1 Case studies

Yin [1989:23] 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. Landsberger [2000:13] defines A case study is a formal report based on the examination of a prearranged subject. 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).

Information will be collected through the following data collection techniques:

1.3.2 Data collection techniques

The following data collection techniques will be used in this study:
• Interviews: One insurance agency and one Bank in South Africa will be interviewed to obtain information regarding cyber crime and insurance contracts via the Internet.
• Observations: The researcher will read through and map various literature information about legal case studies and cyber crime as well as observation of business interviews.

1.3.3 Participants

Interviews will be conducted with the following people at the mentioned agencies:

• Insurance Agency 1: Branch Director and one member.
• One bank managers who were willing to participate.

The sample size of this research project is 2 persons at an insurance company and one bank manager. More participants could not be found, as the managers did not want to involve more people who may expose too much detailed information of the companies involved. Confidentiality problems associated with this type of investigation necessitated the researcher to focus more on legal case studies. Most of the banks and companies, which were approached for interviews, 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. Therefore only one insurance agency and one bank were willing to participate in the interviews. For the sake of confidentiality the names of these companies or the names of the participants cannot be revealed.

1.4 IMPORTANCE/BENEFITS OF THE STUDY

It is hoped that this study will help give insight into how cyber crime affects business in the Republic of South Africa within their respective business sectors. With this insight it would be possible for one to review the laws of this country and see how effective they are at protecting business and perhaps even give insight into where the weaknesses of the law are and how they can be addressed.
1.5 PRELIMINARY LIST OF CHAPTERS

The focus of each of the chapters is listed below:

Chapter 1: Introduction

This chapter is generally an introduction to cyber crime and highlights what the subsequent chapters will contain as well as he literature study.

Chapter 2: Information about ECT Act and cyber crime in South Africa

This chapter has a more detailed definition of cyber crime as well as an explanation of the ECT Act.

Chapter 3: Cyber crime in other countries and the effects on South Africa

This chapter focuses on cyber crime in other countries and the ripple effects of these crimes; issues such as extradition and double criminality are also dealt with. International issues such as cyber terrorism are also explored.

Chapter 4: Case Study findings

This chapter summarises the findings based on the case studies.

Chapter 5: Findings based on the research

Chapter 5 looks at the findings based on the research competed.

Chapter 6: Review, conclusion and recommendations

This chapter is a conclusion, which summarises the previous chapters in a far more detailed manner. Any recommendations arrived at during the study are given here.
1.6 DEFINITIONS OF CONCEPTS IN THE TITLE

1.6.1 The concept of “Cyber crime”

Any crime committed with the aid or use of a computer (Personal Computer, Laptop, PDA, etc). Crime is defined as any contravention of statutory laws and common laws [Gordon, 2002(a): 7].

1.6.2 The concept of “Influencing”

Any action physical, metaphysical or psychological that causes another action or process to deviate from its intended path [Thorndike and Barnhart, 1987:7].

1.6.3 The concept of “Businesses”


1.7 CONCLUSION

This chapter focuses on the introduction and background to the phenomena of cyber crime. The concept was identified and defined, the research problem with the objectives was indicated and the predicted chapters were provided. In chapter two of this study the problem of cyber crime will further be highlighted and discussed as well as the influence of certain laws which are presently in the Republic of South Africa and which pertains to cyber crime in one way or the other.
Chapter II

INFORMATION ABOUT CYBER CRIME AND THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT IN SOUTH AFRICA

2.1 AIMS OF THIS CHAPTER

The aim of this chapter is introduce cyber crime and to show how the laws and statutes of the Republic deal with such crimes.

2.2 INTRODUCTION

Cyber crime is not dealt with under any one specific act but rather under a multitude of acts that govern that area of transgression. The only act that deals with computer related (internet, EDI, etc) crimes is the Electronic Communications and Transactions act of 2002, however this act only deals with crimes that do not fall under other acts (such as theft of information and Virus’) [The Electronics and Transactions Act- ECTA, 2002:4].

2.3 DEFINING CYBER CRIME

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, 2000a: 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 linked 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). According to Long & Long, [1999:C215] cracking can be quite malicious and can cause damage to systems and data integrity) this crime can be performed or executed from within or external to the organisation [Gordon, 2000b:425-426]. One of the most problematic areas of cyber crime is its investigation.

2.4 INVESTIGATING CYBER-CRIME

Cyber-crime is a very difficult transgression to investigate since by its very nature it leaves the bare minimum of a trail and the trails it does leave are often considered “soft” evidence since it may indicate something, which cannot be proved conclusively. One of the few “hard” evidences, which cyber-crimes may leave, is a log held by reliable sources [Gordon 2002c:18]. The new ECT Act provides for the appointing of cyber-inspectors to help aid the protection of the rights of companies, organisations and individuals (this will be discussed further under the ECT bill section 2.8; [ECT Act 2002]. Normal police can investigate many crimes with some special training [Gordon 2000b:444]. The Scorpions is a police investigating body in South Africa that has been well trained into using computers to investigate crimes such as fraud. They have mainly been involved in fraud and corruption cases and tax evictions and so far had success in arresting the ABSA bank hacker who hacked into the accounts of the clients at this bank [Gordon, 2000c].

Intellectual property is one of the most difficult crimes to prove since it is to a large degree subjective; fortunately however in the context of cyber crime existing laws already cover it.

2.5 INTELLECTUAL PROPERTY ISSUES

In this section in this chapter the issues of intellectual property namely; copyrights, trademarks, domain names and patents and how the law protects them are highlighted. 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, 2000:67].

2.5.1 Current legislation

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 (See references). The Copyright Act makes no provision for protection under common law. The reason for this is that the Internet is seen merely seen as an alternative medium of communication [De Villiers, 2000:39], however the Internet does present some unique problems that the acts do not cater for.

An important aspect to remember (an aspect, which the Copyright Act does not deal with) is that by the very nature of the Internet when an owner of copyrighted work places work on the Internet (for public access) he grants (implicitly) the right for a transient copy of the work. The transient copy is stored in Random Access Memory or on the Hard Drive (cache) of a users PC to enable the data to be displayed [De Villiers, 2000:39].

2.5.2 Copyright

The Copyright Act [Copyright Act 98 of 1978; Section 2(1)] protects specifically listed works in Section 2(1) and defines them in Section 1 this includes the following (of relevance to this paper):

- Literary, musical and artistic works;
- Sound recordings, cinematographic films, television broadcast and programme-carrying signals;
- Computer programs.
Databases are covered under literary works [paragraph g of The Copyright Act, Copyright Act 98 of 1978].

Since websites are often multimedia products, they fall within different sections of the copyright act and thus may have different rulings. 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 2002a:436].

Something that further complicates the issue of intellectual property is the conflicting issue of trademarks and domain names.

2.5.3 Trademarks, domain names, patents

This section will first address the trademarks, then domain names and finally end with the patents.

2.5.3.1 Registered trademarks

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 [Trade Marks Act 194 of 1993].
Section 2(1)(xxiii) of the Trademark Act [Trade Marks Act 194 of 1993] 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.

The general consensus is that, in principle, if a third party uses a trademark which is identical or so similar (so as to be confusingly so) to an existing trademark without the proprietors consent this amounts to trademark infringement [Section 34 (1)(a) of Trademarks act, Trade Marks Act 194 of 1993].

To date no cases have appeared in South African courts where the uses of trademarks in say metatags have needed to be ruled upon; however such a ruling would depend heavily on the circumstances. If for example an online store sells electronic goods and lists the trademark names of goods in metatags (to assist in searching) this could be considered fair practice and would not be prosecutable, if however a competing electronics company listed trademarks in its metatags, which would draw searches for competitors towards itself (i.e. a competitors trademark), this could be grounds for prosecution since it is unlikely that such a practice would be considered fair practice [Viljoen, Du Plessis, Vivier, 2000:73].

2.5.3.2 Unregistered trademarks

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, 2000:73]). The principle of passing off was defined in the case of Capital Estate & General Agencies (Pty) Ltd v Holiday Inn, Inc as follows:

“The wrong known as passing-off consists in a representation by one person that his business (or merchandise, as the case may be) is that of another, or that it is associated with that of another, and, in order to determine whether a representation amounts to passing-off, one inquires whether there is a reasonable likelihood that members of the public may be confused into believing that the business of the ones is, or is connected with, that of another”. 
According to section 33 of the Trademarks Act (Trade Marks Act 194 of 1993), 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.

2.5.3.3 Domain names

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 names that are very similar (possibly even confusing) and the Trademark Act prohibits the use of confusingly similar trademarks.

An Example:
There are numerous proprietors using the trademark STERLING (but for different goods or services). However only one of them would be able register the domain name sterling.co.za. Competitors would be able register stirling.co.za although trademark laws prohibit this (because it can be seen as confusingly similar) [Viljoen, Du Plessis, Vivier, 2000:74].

2.5.3.4 Patents

According to the South African Patents Act 57 of 1978 in order for an invention to be patented it must be “new” and it must also involve an inventive step. An inventive step means it must not be obvious to a person of ordinary skill in that art [Section 25(10) of the Act]; [The Patents Act 57 of 1978]. Section 25(2) of the Act excludes among other things, presentation of information, mathematical method and computer programs. However in Section 25(3) of the Act [The Patents Act 57 of 1978] the exclusion is qualified “only to the extent to which a patent or an application for a patent relates to
that such thing”. This means a computer program in itself may NOT be patented, however this exclusion does not include the methods and processes that the software package carries out, nor does it exclude any combination of hardware and software [Viljoen, Du Plessis, Vivier, 2000:91].

South African patent applications do not require exhaustive examination, they do however undergo a formal examination to ensure that all the documentation requirements have been satisfied; because of this no patent has been rejected to date, on the basis of being software. South African law does however allow for a third party to apply for a patent to be revoked. In such a case the courts would then have to decide as to whether an invention is patentable.

To date there have been no cases in the Republic of South Africa dealing with section 25(2) and section 25(3) [Viljoen, du Plessis, Vivier, 2000:91]. South African Patent Law is largely based on UK Patent Laws and thus it would be reasonable to assume that South African courts would follow British approaches [Viljoen, Du Plessis, Vivier, 2000:94].

Not all aspects of crime are covered by common law; these areas of law are legislated and fall under the heading of criminal law.

2.6 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 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 2000c: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.

These examples will now be further highlighted.

2.6.1 Physical computer crimes

In this type of crime, the computer is not been used to commit the crime but is rather the object of the crime, for example: if somebody had to throw a printer out of a double storey window and it shattered on the floor, that would be malicious damage. South African law already covers these kinds of crimes (Mostly under Common Law).

2.6.2 Ordinary crimes

Ordinary Crime can be divided up into two main categories the first been crimes covered by our Common law, these crime include crimes such as fraud, murder and theft. In later years we added the second category this been statutory crimes [Gordon 2000a:424]. Statutory crimes are crimes that are specifically forbidden by Acts and Laws imposed by the government, for example drug trafficking and child pornography.

Most crimes committed today fall into the category of ordinary crime, these crimes have been in existence for a long time and criminals merely use a computer to aid them in their criminal activities. Therefore all the legal proceedings, laws and principles are already in existence and just need to be applied to the area of computers. According to the Internet Fraud Watch in 2000, 78% of Internet fraud came from auctions while a mere 10% from merchandise (Online shopping) fraud [The National Consumers League National Fraud Information Centre, 2002:2].

With the above information it can be seen that police for the most part need only to follow the normal procedures for investigating crimes when investigating computer based crimes, because the majority of these crimes will be prosecuted under non-specialised laws.
However, an example of a computer crime that would pose problems is that of theft of information, South African law states that in order for theft to occur three basic criteria must be met and they are [Buys 2000:45]:

A) The object must be corporeal (tangible);
B) The object must be appropriated;
C) The perpetrator must have the intention of permanently depriving the owner of the said object.

The courts of the Republic have ruled in the past that the criteria of an object needing to be corporeal is not hard and fast, and that intangible objects such as shares (not only share certificates) can also be stolen. This does leave the question though of does the object need an intrinsic value? The question of whether an object must be appropriated is also difficult, since if a person was to steal a CD-ROM with important information, he could be charged for the theft of the CD (which has a low value) but not for the information stored on the CD. To complicate further: if someone steals the CD, makes a copy of it, returns the original that object has not been appropriated. Lastly with regards to intention, if the perpetrator returns the CD after making a copy of it he is not permanently depriving the owner of the object, however that point is arguable on the grounds that the owner no longer has exclusive use of the object [Gordon 2000a:433].

Having said that, the ECT Act, which was enacted at the end 2002, has made enormous strides in the field of computer and Internet related crimes. Section 86(1) of the Act says “A person who intentionally accesses or intercepts any data without the authority to do so, is guilty of an offence” [ECT Act of 2002]. While this doesn’t directly address the situation of stealing information it at least deals with people accessing information without permission. The Act [ECT Act of 2002] goes on to say in Section 86(4) says that “A person who utilises any device or computer program mentioned is subsection (3) in order to unlawfully overcome any security measures designed to protect said data or access thereto, is guilty of an offence” The Act [ECT Act of 2002] also goes on to say in Section 87(2) that the production of intentionally false data that could mislead a person to prejudice of another is also guilty of an offence.

Certain crimes are unique to the world of computers and could not have occurred before the occurrence and require the use of computers. These “new computer crimes” will be described first, then the ECT Act, which was brought in to help curb these new crimes.
2.7 NEW COMPUTER 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, and yet others appear not to be dealt with at all. 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 2000b: 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 [ECT Act of 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 2002b: 48].

Knowing that these acts already protect intellectual property, copyright, trademarks, domain names, patents and computer crimes the new ECT Act 25 of 2002 was enacted. The details of this act will now be discussed.
The purpose of the ECT Act [ECT Act of 2002] is provided in its opening paragraph as:

- “To provide for the facilitation and regulation of electronic communication and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access to electronic communications and transactions and the use of electronic transactions by SMEs; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected therewith.”

The only section of the ECT Act [ECT Act of 2002] 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].

In several places the ECT ACT [ECT Act of 2002] does not deal directly with an issue itself but instead transfers power to other Acts; a summary of Acts referred to by the ECT Act [ECT Act of 2002] is given below in table 2.1.

**Table 2.1: ECTA Related Acts**

<table>
<thead>
<tr>
<th>ECTA Section</th>
<th>Acts Referred To</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 31(2 (d))</td>
<td>Promotion of Access to Information Act 2 of 2000 (Section 11 or 30)</td>
<td>ECTA does not apply here</td>
</tr>
<tr>
<td>Section 32 (1)</td>
<td>Intelligence Services Act 38 of 1994</td>
<td>ECTA does not apply here</td>
</tr>
<tr>
<td>Chapter X</td>
<td>Companies Act 61 of 1973</td>
<td>Setting up of a Domain Name Authority (Section 21 Company)</td>
</tr>
<tr>
<td>Section 82 (4) Section 83(1)</td>
<td>Criminal Procedure Act 51 of 1977</td>
<td>Allows the referred act to include information system and data messages</td>
</tr>
</tbody>
</table>
Section 86(1) Monitoring Prohibition Act 127 of 1992 Allows the referred act to include illegal Access of data
Section 92 Computer Evidence Act 57 of 1983 The Referred Act is Repealed.

Compiled from ECTA 2002

Table 2.2 refers to the Schedule 1 of the ECT Act [ECT Act of 2002]; it is a summary of Acts NOT affected by Sections of the ECT Act [ECT Act of 2002]:

Table 2.2: ECT Schedule 1

<table>
<thead>
<tr>
<th>No.</th>
<th>Act Referred To</th>
<th>ECT Act Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wills Act, 1953 (Act No. 7 of 1953)</td>
<td>11, 12, 13, 14, 15, 16, 18, 19 and 20</td>
</tr>
<tr>
<td>3</td>
<td>Bills of Exchange Act, 1964 (Act No. 34 of 1964)</td>
<td>12 and 13</td>
</tr>
<tr>
<td>4</td>
<td>Stamp Duties Act, 1968 (Act No. 77 of 1968)</td>
<td>11, 12 and 14</td>
</tr>
</tbody>
</table>

Schedule 1 of the ECT Act

Table 2.3 refers to the Schedule 2 of the ECT Act [ECT Act of 2002]; The ECT Act [ECT Act of 2002] must not be construed as giving validity to transaction mentioned in Schedule 2 [ECT Act of 2002 Section 4(4)].

Table 2.3: ECT Schedule 2

<table>
<thead>
<tr>
<th>No.</th>
<th>Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An agreement for alienation of immovable property as provided for in the alienation of Land Act, 1981 (Act No. 68 of 1981).</td>
</tr>
<tr>
<td>3</td>
<td>The execution, retention and presentation of a will or codicil as defined in the Wills Act, 1953 (Act No. 7 of 1953).</td>
</tr>
</tbody>
</table>

Schedule 2 of the ECT Act

The following figure 2.1, which was developed by the researcher, illustrates the areas, which the ECT Act covers as well as those it does not cover:
2.9 CONCLUSION

The laws in the Republic of South Africa form a hierarchy with laws depending on each other and others superseding each other. The intellectual property laws namely: Copyright, trademarks and patents, are all designed to work together to offer the best possible protection. The laws mentioned above as well as the ECT Act are known as Statutes.

The ECT Act therefore stipulates many Acts but also specifically does not cover all acts as Table 2.2 indicates.

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.

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 following figure 2.2 illustrates how the law is structured in South Africa.

![Figure 2.2: Structure of Law](image)

In Chapter 3 cyber crime in other countries will be discussed as they affect South Africa.
Chapter III

CYBER CRIME IN OTHER COUNTRIES AND THE EFFECTS ON SOUTH AFRICA

3.1 AIMS OF THIS CHAPTER

The aim of this chapter is to briefly view how other countries have dealt with cyber crime by looking at their relevant legislation. The countries covered in this section are Great Britain, United States of America and Europe. It is mostly these countries laws that have affected laws passed in South Africa.

3.2 INTRODUCTION

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 [1999:23] 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, 1999:23]:

- 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). South African cyber laws were dealt with in
chapter 2. This chapter will address the same laws as in chapter 2, namely: Intellectual Property, but from an international perspective. Issues such as international criminal law, extradition and Cyberterrorism are also dealt with in this chapter.

3.3 INTERNATIONAL ISSUES

In the next few sections the laws that govern different countries will be discussed. International Law is a set of laws that most countries adhere to. In international law it is recognised that individual countries are sovereign, and as a result a particular country has the exclusive right to govern its nationals as it sees fit [Gordon 2000a:44].

Following the structure used in Chapter 2, the first issue to be dealt with is the one of intellectual property.

3.3.1 Intellectual property

Bencivenga tells us how technology is progressing too fast for the law [1997:1]. The international nature of the Internet and the fact that each country has its own laws makes international protection of intellectual property very difficult. The very nature of the Internet will force world governments to standardise law [De Villiers 2000:37].

In July 1995 the European Commission Green Paper “Copyright and related rights in the Information Society” was published, as well as the “Report on Intellectual property rights” which was published in September 1995 by the US Administrations Information Infrastructure task force [EU Green Paper, 1997:13]. The result of these two initiatives resulted in the World Intellectual Property organisation (WIPO) arriving at two treatises, which were concluded on 20 December 1996. South Africa being a member country of the WIPO has signed the treatise. The WIPO copyright treaty according to Milanovitch (2003:43) extends to “expression and not ideas, procedures, methods of operation or mathematical concepts as such” [Milanovitch, 2003:21]. Section 6 of the Copyright treaty brings in the notion of an “exclusive general right of distribution of copies of a work by its copyright owner” [De Villiers 2000:38]. However the Agreed statements concluded at the same time as the WIPO treatise state that this right applies only to
“fixed copies that can be put into circulation as tangible objects”. This apparently does not include distribution via the Internet [De Villiers 2000:38].

The copyright treaty introduces a general right of communication of a work by the copyright owner. This explicitly excludes distribution of works and explicitly includes interactive on-demand acts, which would cover the downloading of files and viewing of content on a web site [De Villiers 2000:38].

The Agreed statements provide for the availability of facilities that enable communication does not amount to communication itself. “This means that bulletin board operator and network operators will not be liable for copyright infringement in respect of the works they source” [Milanovitch, 2003:22].

As the South African (Patents) Act is closely based on the UK (Patents) Act, it is to be expected that our courts will follow a similar approach [De Villiers 2000:94].

Since each country has its own laws and what may be a criminal activity in one country is not in another the topic of criminal law needs to be discussed.

3.3.2 Criminal law

In the USA the Computer Fraud and Abuse Act deals with dangerous Code (Viruses) as well as computer fraud issues [Betts 2002:2]. According to this act a person will be guilty of an offence if he transmits any destructive code or command to a computer system without the authorisation of the persons or entities who own the system or who are responsible for it, or if he causes loss or damages to the amount of $1000 to the computer or computer system [18 USCS, 2000 § 1030 (4)(5)]. On conviction of such an offence the perpetrator can be fined, or imprisoned for a maximum period of five years [18 USCS, 2000 § 1030 (A)(6)(C)(3)(A)]. In Great Britain the Computer Misuse Act of 1990 deals with any form of dangerous or destructive code. However to be held criminally liable it must be clear that there must be an intention to cause damage by the introduction of the code [Computer Misuse Act, 2000:4].
The Internet is an international animal with no regard towards boundaries and borders and since there is such a variance in law, the common dominator or most countries law is the concept of International Law.

3.3.3 International law

A major problem of the Jurisdiction of the Internet is its international nature. If a crime is committed in one territory but affects another, who has the right to prosecute? These issues and others have still to be dealt with. If the USA passes judgement on a case and that case needs to be implemented in Italy how will this be enforced (see Playboy enterprises Vs Chuckleberry Publishing Inc in chapter 4)? The concept of Jurisdiction as we currently know, relates to a Sovereign country with well mapped out boundaries. Cyberspace disregards these boundaries totally [Gordon 2000a:441]. The Australian Computer Crime Law (2001:3) states that computer crime is of no assistance unless adequate evidence is available which law enforcement agencies can rely upon to obtain a conviction and that businesses must be aware of the potential evidence that must be collected, preserved and archived. Each of the states, territories and Commonwealth have their own rules of evidence and include the following [Australian Computer Crime law, 2001:5]:

- The Commonwealth Evidence Act 1995;
- New South Wales has the Evidence Act 1995 which essentially mirrors the Commonwealth Act.
- Australian Capital Territory applies the Commonwealth Evidence Act 1995 in its courts
- Queensland, Victoria, Western Australia, South Australia, Tasmania, Northern Territory Acts of different years.

The Attorney-General in Australia has quoted that cyber crime is costing companies $3 trillion each year [Australian Computer Crime Law 2001:7]. This document gives examples of risk assessment and also highlights the effects on e-commerce. Currently the only way to deal with criminals who commit crimes in another country is to have them extradited to the country where the crime took place.
3.3.4 Extradition

Extradition is not covered under the ECT Act, however it is important because as the volume and severity of cyber crime increases countries may demand to have criminals extradited. An example would be: If a terrorist in the United Kingdom hacked into the Air Traffic Control (ATC) of Johannesburg International Airport and caused two planes to collide killing everybody onboard. The South Africa Authorities may wish to have the terrorist extradited from the United Kingdom to South Africa to stand trial.

Gordon [2000c:948] define extradition as “the delivery of an accused or a convicted individual to the state where he is accused of, or has been convicted of, a crime, by the state whose territory he happens for the time to be”. If a perpetrator flees one country and takes refuge in another a request must be made to return said perpetrator to the country where the crime was committed. According to the principles of international law a country does not have a duty to extradite a fugitive [Gordon 2000a:442]. Therefore in order to make it easier for countries to extradite (or request an extradition) criminals’ countries enter into extradition treatise with each other.

In South African extradition is governed by the Extradition Act as well as treatise entered into with countries. According to section 2(2) of the South African Extradition Act extradition limited to cases “which if committed in the Republic would be punishable therein as an offence” – this means in order for a person to extradited the offence must be a crime in both South Africa and in the country requesting the Extradition. This is called Double-criminality.

Since each country has different laws about internet criminality it can be surmised that obtaining extradition orders for internet based crimes (cyber crime) could be quiet difficult. The principles of extradition are likely to be put to the test when called upon to deal with the new and difficult problem of Cyber terrorism.

Cyber terrorism needs to be looked at due to its extreme danger as well as relative ease to perform. “It is important to distinguish cyber crime, a domestic issue that may have international ramifications and Cyber terrorism, an international issue that may have domestic ramifications” [Nagpal 2002:1].
3.3.5 Cyber terrorism

Cyber terrorism can be defined as “… the premeditated use of activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives” [Nagpal 2002:1].

In July 2002 a Merrill Lynch survey, which was released, indicated that security is the number two concerns of all Chief Information Officers [Betts 2002:1]. According to Rusine Mitchell-Sinclaire [in: Betts 2002:1] is the September the 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 2002:1].

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. The defaced hundreds of web sites and launched Denial of Service (DOS) attack against Iranian ministries 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 2002:1].

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 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 [Nagpal 2002:1]. According to Nagpal this is not the ideal situation and Cyber terrorism should be dealt with as a separate issue [2002:1].

Vatis [2001:9] 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 2001:9]. 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, 2003:55]. 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.
3.4 CONCLUSION

The variance of laws between countries makes the prosecution of international crimes extremely difficult. In order for countries to deal with cross boundary crimes most countries have entered into either treatise with each other or group treatise (such as the WIPO treatise). Most countries base inter-country laws on the principles of international law, however cross border jurisdiction is not dealt with in international law. Extradition is a means to overcome the international jurisdiction however the concept of double-criminality is required and this poses a problem without a standard international law designed to deal with cyber crime. Cyber terrorism is a new and growing threat that has not yet tested the laws regarding terrorism; most countries are overhauling terrorism laws to allow for Cyber terrorism.

In chapter 4 the various case studies that where discussed in chapter 1 are presented along with any findings that may be applied to the case studies.
CHAPTER IV

CASE STUDY FINDINGS

4.1 INTRODUCTION

This chapter deals with the research methodology (case study research) as well as the findings based on the case studies discussed in chapter 1. The findings are applied to the research questions asked in chapter 1. The purpose of this chapter is to present and analyse the research data obtained through the following collection techniques:

- Interviews;
- Literature Study;
- Legal Case Studies.

4.2 RESEARCH PROBLEM

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 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. Table 4.1 shows the research questions and the participants used in the collection of the data.

Table 4.1: Research Questions

<table>
<thead>
<tr>
<th>Research Questions</th>
<th>Bank</th>
<th>Insurance</th>
<th>Legal Case Studies</th>
<th>Literature Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. How cyber crime affects businesses in South Africa?</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>2. How laws Prevent Cyber crime?</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
</tbody>
</table>
4.3 RESEARCH METHODOLOGY

The research will be done with a qualitative method that will be used for collecting data from various sources. Qualitative methods are defined as methods that provide detailed and in-depth information. Qualitative data gives outside audiences an understanding of what a target population may think or feel about specific issues or a specific project in their community [Landsberger, 2000:6]. Two methodologies will be used, the first being a literature study, the reason for this is to ascertain the current and proposed laws and to understand the way in which the law is intended to work. The second methodology to be used is case studies (particularly legal cases). “Generally speaking, one will prefer a multiple-case design, because this will facilitate comparisons between cases contributing to your conclusion” [Olivier 1999:122].

4.3.1 Case study as a research method

Yin [1998:23] defines a case study as an empirical study that investigates a contemporary phenomenon within its real-life context; when the boundaries between the phenomenon and context are not clearly evident; and in which multiple sources of evidence are used.

Case studies also allow a researcher to ‘reveal the multiplicity of factors [which] have interacted to produce the unique character of the entity that is the subject of study’ [Yin, 1998:82].

Case study typically involves the observation of an individual unit, e.g. a student, a delinquent clique, a family group, a class, a school, a community, an even, or even an entire culture. It is useful to conceptualise a continuum of unit size from the individual subject to the ethnographic study [Landsberger, 2000:259].

4.3.1.1 Purpose of a case study

Denscombe [2001:30] argues that a case study approach has certain features associated with it and when brought together they form a broad approach with an underlying rationale for the direction and planning of the investigation that separates it from the other research methods.
Hereunder are some of the identified features of a case study [Denscombe, 2001:30]:

- **Spotlight on the instance.** One distinct feature and starting point of the case study approach is that it focuses on just one instance of the thing that is to be investigated than other approaches that focuses on a wide spectrum. This will bring a better understanding of the thing that is being studies.

- **In-depth study.** The prospects of getting some valuable and unique insight depends on being able to investigate things in a way that is different from, and in some senses better that, what is possible using other approaches. A case study affords the research an opportunity to study things in detail and also a greater concentration on an instance of a thing studied.

- **Focus on relationships and processes.** Case studies are more holistic thus give and complete picture of a thing being investigated. It allows for identification of relationships that exist among the various aspects of the case being studied. It makes the researcher to concentrate on the outcomes and results of the processes that make the case to be as is.

- **Natural setting.** The case being investigated is not something, which is created artificially for the purpose of research; it is something that already exists.

- **Multiple sources and multiple methods.** The case study approach allows the research to apply multiple sources, use variety of data and a variety of research methods as part of the investigation.

All of these purposes are addressed in this research study on cyber crime.

### 4.3.1.2 Why do we carry out case study research?


- Firstly, he claims that they are valuable as preliminaries to major investigations as they generate intensive and rich data that may suggest themes for more intensive investigation.
• Secondly, he claims that since case studies 'have the aim of probing deeply and analysing intensively', the many phenomena that make up the activities of the unit under study, then generalisations to the wider population may be possible.
• Thirdly, he indicates that case studies may generate anecdotal evidence that can illustrate general findings.
• Fourthly, case studies may serve to refute generalisations.
• Fifthly, a case study approach is preferred when pertinent behaviours cannot be manipulated.
• Finally, a case study may be the best possible description of a unique historical event.

In this study cyber crime in certain organizations in South Africa will be investigated which covers all the aspects or reasons mentioned above. Additionally, the behaviours and perceptions of people to be interviewed could not be manipulated as would be required for an experimental study. Thus this research project fits five of Burns [2000] suggested reasons for carrying out case study research, except for the historical event. Furthermore, Denscombe [2000:33] states that a good case study requires the researcher to justify the choice of using this approach. The selection can be justified on the following bases:

• Selection on the basis of suitability

The researcher needs to defend the decision by arguing the suitability of the particular case for the purposes of the research by broadly speaking the following four grounds of justification:

1. **Typical instance.** The typicality of the chosen case suggests the logic that the particular chosen case is similar in crucial respects with others that might have been chosen, and that the findings are more likely to apply elsewhere.
2. **Extreme instance.** Apart from typicality, a case should provide something of a contrast to the norm.
3. **Test-site for theory.** The logic for the selection of a particular case can be based on the relevance of the case for previous theory and thus resulting in theory testing and/or theory-building.
4. **Least likely instance.** Following the idea of test-sites for theory, a case might be selected to test the validity of ‘theory’ by seeing it occurs in an instance where it might be least expected.

- **Selection on a ‘pragmatic’ basis**

  If the face of all the limitations of time and resources in the practical world of research the researcher has to select an alternative within his/her means and the one that involves less travelling, less expenses and the difficulty of gaining access.

  The research should decide on something that he/has interest and is exciting to pursue.

- **Selection on the basis of ‘no real choice’**

  If the research study is funded by a certain organisation and prescribes a case study method, the researcher will have no leeway on deciding about another method.

  The occurrence of an event may present a lucrative and unique opportunity for the researcher to take advantage of the once-off chance. In this regard the researcher has no choice but to grab and utilize the opportunity as he/she has to power to bring back or suspend the opportunity.

4.3.1.3 **Planning the case study**

According to Burns [2000:464] case studies have four main components to the research design. These will now be indicated:

- **Initial case study questions**

  These are (W4H) who, what, where, where and how, which must be answered from the onset of the research project. This is actually what the case study is seeking to answer and proves the focus for the whole research project. Hence my project is to identify how cyber crime influences businesses in South Africa.
• **Study proposition**

The proposition identifies something at which attention is to be directed within the scope of the study, so that specific evidence can be obtained. Cyber crime affects businesses all over the world and especially in South Africa.

• **Unit analysis**

This aspect is concerned with defining and determining the crux of the case. This helps the researcher to collect data, which is only pertinent to and applies specifically to the real matter and context of the research project scope. As indicated earlier in chapter one about the objectives and scope of this research, data will be collected from the identified business in relation to cyber crime, which affected their processes.

• **Linking data to propositions and criteria for interpreting findings**

This component relates to the actual data analysis step, which will culminate in the formation of certain conclusions about the case or the matter under research. These components help to scale down the research scope and create a better understanding of the case to be researched. This further brings a better flow and harmonisation of the research activities.

4.3.1.4 **Advantages of the case study approach**

Denscombe [2001:39] identifies the following benefits of applying a case study in a research project:

- The ability to focus on one or a few instances allows the research to deal with the subtleties and intricacies of complex situations. In way it also makes it possible for the researcher to grapple relationships and social processes that cannot be treated the same with other approaches.

- Case study allows the usage of a variety of research methods for capturing the complex reality under scrutiny.

- In parallel with the use of multiple methods, the case study approach fosters the use of multiple sources of data. This in turn, facilitates the validation of data through triangulation.
• The case study approach is particularly suitable where the researcher has little
• There is no pressure on the researcher to impose controls or change
  circumstances. This allows the researcher to concentrate on the investigation
  phenomena without any coercion.
• A case study can fit well with the needs of small-scale research through a
  concentrated effort on one research site.
• Theory building and theory testing research can both use the case study
  approach to good effect.

4.3.1.5 Disadvantages of the case study approach

Denscombe [2001:39] identifies the following disadvantages of applying a case study in
a research project:

• The credibility of generalisations made from case study findings is questionable.
• Case studies are often perceived to produce soft data
• The boundaries of a case can provide difficult to define in an absolute and clear-
  cut fashion.
• Negotiating access to case study settings can be a demanding part of the
  research process.
• IT is hard for case study researchers to achieve their aim of investigating
  situations as they naturally occur without any effect arising from their presence.

4.3.2 Data collection techniques/sources of evidence

The following data collection techniques were applied in this study to obtain the data:

• Interviews

  Meetings/interviews will be organised with the managers of the insurance
  agency as well as with the Bank to solicit information pertaining their
  perceptions about cyber crime and establish their view of cyber crime into
  their business operations.
• **Observations**

The operations and possible cyber crime offences will be observed at the insurance agency and the bank.

A case study is a very useful approach when it comes to the scaled-down investigation since it affords the opportunity to concentrate on one site or organisation under study in order to acquire detailed and clear facts about a phenomenon. However the researcher has to be cautious about the limitations of a case study and the final interpretation of the outcomes and results of the case study findings. Furthermore generalisation concluded from a case study may not be applicable on every individual, organisation or event.

### 4.4 PARTICIPANTS OF CASES

The three kinds of participants namely Legal Cases, Bank an Insurance Agency are listed below.

#### 4.4.1 Legal case studies

The following table summarizes the different legal case studies and the infringement, which applies to each.

<table>
<thead>
<tr>
<th>Case</th>
<th>Infringement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storm Impact Inc Vs Software of the month club</td>
<td>Copyright Infringement</td>
</tr>
<tr>
<td>Capital Estate &amp; General Agencies (Pty) Ltd Vs Holiday Inn, Inc</td>
<td>Unregistered Trademark Infringement</td>
</tr>
<tr>
<td>British Telecom plc &amp; Others Vs One in a Million &amp; Others</td>
<td>Trademark Case law – Domain Name registration</td>
</tr>
<tr>
<td>Playboy Enterprises Inc Vs Chuckleberry Publishing Inc</td>
<td>International Jurisdiction of trademark infringement</td>
</tr>
</tbody>
</table>

#### 4.4.2 Bank

Only one bank was used during this study, as the other banks did not want to take part. For the sake of confidentiality the name of the bank will not be revealed. The interviewee will be known as Gordon (2002c). Only one major bank in South Africa and the branch manager at this bank was a participant in this study.
4.4.3 **Insurance agencies**

Only one insurance agency in South Africa: SGJ Brokers in Benoni and its branch manager Mr Van Zyl (2003) and one employee (Mr D Conradie) were participants for this study.

4.5 **FIRST RESEARCH QUESTION**

The following research question will be addressed in this section: How cyber crime affects 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.

4.5.1 **Bank**

Table 4.3 is a compilation of the questions asked during an interview with the bank manager (Gordon, 2002b). The answers giving were used to answer the question: How cyber crime affects businesses in South Africa?

**Table 4.3: Bank Interview (Research Question 1)**

<table>
<thead>
<tr>
<th>No</th>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>With the increase of cyber crime occurring worldwide, do you think that the banking sector is at a risk of been affected? Do you think that the cyber crime would most likely be committed Internally (by staff) or Externally (people outside of the bank)</td>
<td>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. 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).</td>
</tr>
<tr>
<td>3</td>
<td>Are Banks in South Africa been affected by cyber crime already and to what extent?</td>
<td>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.</td>
</tr>
</tbody>
</table>
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?

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.

6. 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.

7. 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.

8. 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, 2002c).

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, 2002c). 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, 2002b). Some of the major reasons why moving towards electronic banking in the Republic are that it is cheaper (due to been less admin and labour intensive), more security (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.

4.5.2 Insurance

Table 4.4 is a compilation of the questions asked of the insurance agency in the interview (Van Zyl, and Conradie, 2003). The answers giving were used to answer the question: How cyber crime affects businesses in South Africa?

Table 4.4: Insurance Interview (Research Question 1)

<table>
<thead>
<tr>
<th>No</th>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>With the increase of cyber crime occurring worldwide, do you think that the insurance sector is at risk of been affected?</td>
<td>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 online.</td>
</tr>
<tr>
<td>2.</td>
<td>Do you think that the cyber crime would most likely be committed Internally (by staff) or Externally (people outside of the company)</td>
<td>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 &quot;work&quot; in the policies only view</td>
</tr>
<tr>
<td>3.</td>
<td>Is Insurance in South Africa been affected by cyber crime already and to what extent?</td>
<td>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</td>
</tr>
<tr>
<td>4.</td>
<td>Given the current crime rate in South Africa, do you think crime will spread electronically (to cyber crime) and affect business in South Africa?</td>
<td>At some point, cyber crime will probably start having an effect on business in South Africa as more and more people have access to computers and become &quot;computer literate&quot;. 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.</td>
</tr>
<tr>
<td>6.</td>
<td>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?</td>
<td>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.</td>
</tr>
<tr>
<td>7.</td>
<td>Of what benefits is it for insurances to move towards a cashless society (EFT type transactions)?</td>
<td>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</td>
</tr>
<tr>
<td>8.</td>
<td>What are your feelings about cyber crime and insurance?</td>
<td>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</td>
</tr>
</tbody>
</table>
Insurance has not significantly been affected by cyber crime until now (except for internal fraud), they do feel however 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.

4.5.3 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 2000c: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 2002:4]. These Guidelines aim to [OECD 2002:5]:

- 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.

These following table highlights these guidelines (OECD 2002:15-17):
Table 4.5: The OECD guidelines and discussions

<table>
<thead>
<tr>
<th>Guideline</th>
<th>Discussion</th>
</tr>
</thead>
</table>

| Awareness | Participants should be aware of the need for security of information systems and networks and what they can do to enhance security. Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures might significantly harm systems and networks under their control. |
| Responsibility | All participants are responsible for the security of information systems and networks. Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. |
| Response | Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents. Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation. |
| Ethics | Participants should respect the legitimate interests of others. |
| Democracy | The security of information systems and networks should be compatible with essential values of a democratic society. |
| Risk assessment | Participants should conduct risk assessments. Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. |
Security design and implementation

Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation’s systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

Security management

Participants should adopt a comprehensive approach to security management. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security.

Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

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”. The ECT Act [ECT Act 2002]. 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) [Maree & Bray, 2003a:1];
• Banks were under attack (African Bank on May 23, 2003; ABSA Bank on May 15, 2003) [Maree & Bray, 2003b].

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

As was evident from Chapter 2 and Chapter 3 in South Africa 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.

4.5.4 Findings

Therefore the answer to the research question is that cyber crime has been affecting businesses for a long time, particularly in the area of fraud. Until recently almost all of
the cyber crime was committed internally (internal fraud). The banks feel that they are at an increasing risk of been affected by cyber crime from external sources while the insurance agency feels that they are at no immediate risk of external attack due to the fact that insurance is not yet handled over the internet. The insurance agency does recognise the fact that they are at the same risk as anyone else when it comes to internal fraud.

4.6 SECOND RESEARCH QUESTION:

The second research question is: How laws prevent cyber crime?

This question was asked to ascertain business feels that the current laws protect them from cyber crime. In order to answer this question the following data collection techniques were used:

- Interviews;
- Legal Case Studies;
- Literature Review.

4.6.1 Bank

Table 4.5 is a compilation of the questions asked of the bank manager in the interview (Gordon, 2002c). The answers giving were used to answer the question: How laws prevent cyber crime?

Table 4.6: Bank Interview (Research Question 2)

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>According to research done, South Africa is a haven for money laundering (via the internet); do the laws adequately protect the banks and consumers from been affected by money laundering?</td>
<td>New legislation regarding money laundering was recently promulgated. It has been based on overseas experience, esp. USA and Europe. It affects Forex agencies, banks, car dealers, estate agents and travel agents, whereby such organizations are obliged to report all suspicious cash transactions over a certain amount.</td>
</tr>
<tr>
<td>5</td>
<td>Do you feel that the new Electronic Communications and Transactions Act (or any other existing acts) offer protection to people (and organizations) from cyber crime?</td>
<td>Don’t know enough about it to answer this question.</td>
</tr>
<tr>
<td>6</td>
<td>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</td>
<td>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</td>
</tr>
<tr>
<td>**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.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>7. Of what benefits is it for the banks to move towards a cashless society (EFT type transactions)?</strong></td>
<td><strong>Major benefits, esp. in RSA: Less admin intensive/less expensive, improved security, new product opportunities e.g. smart cards, lower insurance premiums.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>8. What are your feelings about cyber crime and banking?</strong></td>
<td><strong>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.</strong></td>
<td></td>
</tr>
</tbody>
</table>

Banks and similar financial services institutions are required by law to report any suspicious transactions over a certain value; the new anti-laundering laws have been based on overseas experience, especially the United States of America and Europe. It is hoped that these new laws will help prevent financial service institutions from becoming involved (either intentionally or accidentally) in fraud and to make it as difficult as possible to commit fraud and money laundering. It is hoped that current legislation is adequate, however it needs to be flexible enough to adjust quickly to the changes that occur on the technological front.

The ECT Act (As explained in Chapter 2) allows for controlled cryptography and digital signatures, which helps to protect banks, clients and merchants from criminals stealing transaction information and performing their own transactions with the stolen data at a later stage.

### 4.6.2 Insurance

Table 4.6 is a compilation of the questions asked of the insurance agency in the interview (Van Zyl and Conradie, 2003). The answers giving were used to answer the question: How laws prevent cyber crime?
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Do you feel that the new Electronic Communications and Transactions Act (or any other existing acts) offer protection to people (and organizations) from cyber crime?</td>
<td>The protection is probably limited. Unfortunately criminals at this level are very sophisticated and would have little or no regard for any acts that are enforced. Also the requirement of Financial Institutions to report any suspicious transactions should help alleviate fraud (especially the minor ones)</td>
</tr>
<tr>
<td>6.</td>
<td>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?</td>
<td>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.</td>
</tr>
<tr>
<td>7.</td>
<td>Of what benefits is it for insurance to move towards a cashless society (EFT type transactions)?</td>
<td>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.</td>
</tr>
<tr>
<td>8.</td>
<td>What are your feelings about cyber crime and insurance?</td>
<td>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.</td>
</tr>
</tbody>
</table>

The new anti-fraud laws that require financial service institutions to report any suspicious transactions above a certain amount (as discussed above) should help to curb fraud in this area. The new requirement that all financial service institutions must register with the Financial Services Boards is widely believed to reduce fraud and crime by allowing the board to regulate and monitor for unscrupulous business practices, this would apply to cyber crime as well. Since Insurance has not really begun the move towards e-commerce it is difficult to predict as to whether current laws would protect insurance agencies and clients from cyber crime, however the application with other financial service institutions should provide a fairly accurate guide.

### 4.6.3 Legal cases

Since no cases of cyber crime have yet been brought before the courts in the Republic, current laws have not yet been tested in respect of cyber crime. In chapter 2 an
explanation of the South African laws and how they should apply in the case of cyber crime.

4.6.4 International case

In the case of Playboy Enterprises Inv, Vs Chuckleberry Publishing Inc, in 1981 Playboy was granted an interdict against Chuckleberry for a publication titled “Playmen” which is similar to the “Playboy” trademark. In January 1996 Chuckleberry created a web site based on a server in Italy promoting its “Playmen” publication. Playboy Enterprises proceeded to take Chuckleberry to court for violating its 1981 interdict. The court found in Playboy Enterprises favour and ruled that Chuckleberry may not target its publication to customers from the United States of America (Gordon, 2000).

Unfortunately the court did not mention how the ruling was to be implemented. This case highlights how difficult implementation of rulings would be when cyber crime is committed internationally.

4.6.5 Findings

Therefore the findings for the research question can be seen as follows:

Current laws appear to protect against cyber crime by virtue of the fact that most cyber crime is merely a new means of committing an existing crime. However some ruling on some cases are not clear. The ECT Act [ECT Act of 2002] helps to protect against some of the unique cyber crimes. It would appear that due to the lack of knowledge about the ECT Act in the banking sector and Insurance that companies are unaware of the advances and changes having taken place in the law. It is hoped that the compulsory registration of financial institutions with Financial Services Board will help to monitor for fraudulent activities.

4.7 CONCLUSION

Businesses have been affected by cyber crime for a while with respect to internal fraud. The different business sectors feel that they are varying levels of risk of been affected further by cyber crime. While the laws appear to offer protection against cyber crime
these laws will only be put to the test when cases appear before the courts of law. In chapter 5 a review of the research, a summary and recommendations are to be made.
Chapter V

REVIEW, CONCLUSION AND RECOMMENDATIONS

5.1 INTRODUCTION

It is hoped that this study will help to give insight into how cyber crime affects business in the Republic of South Africa within their respective business sectors. With this insight it would be possible for one to review the laws of this country and see how effective they are at protecting business and perhaps even give insight into where the weaknesses of the law are and how they can be addressed. This chapter summarises the findings and gives recommendations.

5.2 SUMMARY OF FINDINGS

Findings of the research summarised according to the research questions.

5.2.1 First research question: How cyber crime affects business in South Africa?

Thus far it would appear business in South Africa has not been seriously affected by cyber crime. The only form of cyber crime that appears to be rife is internal fraud. This can been seen by the fact that no cases have appeared before the courts. The banks do however feel that they are at an increased risk both externally and internally, which is likely to increase as the migration towards electronic money occurs. The Insurance industry feels that they are not yet affected by external cyber crime and are unlikely to be so in the near future.

5.2.2 Second research question: How laws prevent cyber crime?

The laws specific to cyber crime, namely the ECT Act, have not yet been tested in the courts of Southern Africa. However existing laws particularly those pertaining to intellectual property issues are well established and should be applied to cyber crime without too much difficulty. The aspects of common law remain the same and are not affected by the way (whether the internet, physically, or otherwise) in which they are committed. Both the Banks and Insurance Agency feel that the legal requirement
requiring them to report suspect transactions should go a fairly long way in helping to reduce fraud.

5.3 RECOMMENDATIONS

Based on the findings in Chapter 4 the following recommendations can be made.

- Laws need to be standardised across countries;
- The South African Government needs to address the ECT Act [ECT Act 2002] in order to protect the customer better and to incorporate all lessons learned from the hacking of the banks and Higher Education institutions;
- An international cyber court to judge serious cyber crime and mediate disputes;
- Police and investigators need special training to aid the investigation of cyber crime and possibly even set-up a specialised investigations unit;
- Flexible laws that can match the rapid changes in technology to prevent lacuna in the law appearing.

5.4 FURTHER RESEARCH

Further research can be done on the above recommendations, particularly the aspects of standardised law and an international court in a worldwide context. Computer forensics in relation to the police force is also an area, which can be investigated. Locally research into improved policing techniques for cyber crime would go a long way. More research can be done on the following issues:

- The influence of the ECT Act in South Africa on businesses and the way they counteract cyber crime;
- Readdressing certain neglected issues in the ECT Act [ECT Act 2002] like theft, fraud, extortion and the incorporation of all OECD guidelines;
- The cyber crime in Europe and measures to counteract these;
- Laws on cyber crime internationally;
- Determining the establishment of a cyber crime court to specialize on these issues per se.
- Security measures to prevent cyber crime;
- Training of people in companies to know how to deal with cyber crime attacks.
5.5 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 area. 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…. Time will only tell.
REFERENCES

Australian Computer Crime Law. 2001. [Online]. Available at:

Available at:

[Online]. Available at:
http://www.computerworld.com/securitytopics/security/story/0,10801,72571,00.html.

Available at: <http://www.computeruser.com/news/02/07/27news2.html>. Accessed:
26/08/02.


CERT/CC Statistics. 2002. [Online] Available at:

CIW COMMUNITY. 2002. CIW addresses cyber security. [Online]. Available at:
Accessed: 27/08/02.

COMPUTER MISUSE ACT. 1990. Great Britttian. [Online]. Available at:


Conradie, J. 2003. Personal interview conducted at the insurance agency in Pretoria,
South Africa.


*The Copyright Act* 98 of 1978, Republic of South Africa.


*The Trademarks Act* 194 of 1993, Republic of South Africa.

*The Patents Act* 57 of 1978, Republic of South Africa.


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


APPENDIX A: CASE STUDY – BANK INTERVIEW

1. With the increase of cyber crime occurring worldwide, do you think that the banking sector is at a risk of been affected? Do you think that the cyber crime would most likely be committed Internally (by staff) or Externally (people outside of the bank)

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. The cyber vehicle is just another, albeit sophisticated new vehicle to commit bank crime, and falls into the second category. Every time there is new technology, it will be a double-edged sword: it's good for the good guys, and good for the bad guys. It's a new way of stealing money. 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.

2. According to research done South Africa is a haven for money laundering (via the internet); do the laws adequately protect the banks and consumers from been affected by money laundering?

New legislation regarding money laundering was recently promulgated. It has been based on overseas experience, esp. USA and Europe. It affects forex agencies, banks, car dealers, estate agents, travel agents, whereby such organisations are obliged to report all suspicious cash transactions over a certain amount.

3. 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.
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?

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.

5. Do you feel that the new Electronic Communications and Transactions Act (or any other existing acts) offer protection to people (and organizations) from cyber crime?

Don't know enough about it to answer this question.

6. 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.
7. 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.

8. 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.
1. With the increase of cyber crime occurring worldwide, do you think that the insurance sector is at a risk of being 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. Do you feel that the new Electronic Communications and Transactions Act (or any other existing acts) offer protection to people (and organizations) from cyber crime?

The protection is probably limited. Unfortunately criminals at this level are very sophisticated and would have little or no regard for any acts that are enforced.

6. 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.

7. 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

8. 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 being Internet based in the near future because of the complexities of underwriting a policy, this still needs human intervention and risk analysis.

Also the requirement of Financial Institutions to report any suspicious transactions should help alleviate fraud (especially the minor ones)