GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

New Zealand Information Technology Security Legislation

(Background Information for New Zealanders in IT)

© SANS Institute 2004, Author retains full rights.

Scott Walsh
Auckland, New Zealand, 19 July 2004
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b Option 1

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract 1

New Zealand Legislative Framework Overview 2

Background 3

Introduction 5

Security Implications of the 'Electronic Transactions Act 2002' 7

Security Implications of the 'Crimes Amendment Act 2003' 10

Conclusions 14

Appendices 15

- References 15
- Abbreviations and Acronyms 17
- Crimes Amendment Act 2003, Sections 248-253 18
- Credits 21

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

Within the global IT industry New Zealand makes up one of the smaller nations with a population comparable to a large city. Being a smaller country, information on IT Security written with a New Zealand focus is limited compared with information written with a focus on other countries.

In most areas of IT this does not present itself as an issue as the same technologies, applications and protocols are used by most English speaking countries. However the legislative and ethical framework in which IT operates can vary greatly from country to country.

As a New Zealander it is typically easier to find out how an IT Security issue stands within the United States' legislative and ethical framework than New Zealand's own one, this essay attempts to address this by providing an overview of how New Zealand legislation effects IT Security and some of its issues.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

New Zealand Legislative Framework Overview [1]

As this essay makes reference the New Zealand Legislative Framework and uses terms such as 'Bill' and 'Acts of Parliament', a basic understanding of these terms and how laws are created in New Zealand is required.

The following provides a short overview. This is a summary of the information provided on the 'Office of the Clerk of the House of Representative' website. For a more detailed overview their page on the Legislative Procedure is recommended (http://www.clerk.parliament.govt.nz/Publications/Other/Booklet/2+-+Legislative+Procedure.htm).

New Zealand's 'Parliament' consists of the Sovereign (who is the Queen of England) and the House of Representatives. The House of Representatives comprises all the elected members of Parliament. Unlike some other jurisdictions, there is no upper or lower House. Law is created through the passing of an 'Act of Parliament'

Before an Act can be passed, it must first be introduced to Parliament as draft legislation called a 'Bill'. A Bill can be introduced by any member of Parliament.

After a Bill is introduced it goes through three 'readings' where it is debated by the members of Parliament. After the second reading, the members decide whether the Bill is agreed to in principle and should proceed. Most Bills are also referred to a Select Committee, who calls for and considers public submissions, as well as reports from Government departments. The Select Committee may recommend amendments to the House and if the recommendations are accepted, they are incorporated into the Bill.

Any last minute amendments to the text of the Bill can be made by the House prior to the third reading. After its third reading, some formalities are completed, which include the Bill being signed by the Governor-General (New Zealand's representative of the Queen), then the Bill becomes law.

[1] Legislative Procedure - http://www.clerk.parliament.govt.nz/Publications/Other/Booklet/2+-+Legislative+Procedure.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Background

Even as recent as this early century, New Zealand has had lack of Acts of Parliament that provide laws relating to IT crimes. Without the appropriate legal framework of Acts IT Security professionals were limited in their requests to the Police and the Crown for prosecutions of what would ideally be clear cut IT crimes.

Before the introduction over the last 24 months of more appropriate Acts, prosecutions were attempted using laws that were designed before computers were common place and did not adequately address the advancements of Information Technology.

For example the defendant in a case tried in the late 90's had the follow charge, for what most IT professionals would simply call electronic fraud (the defendant was using a program for 'Blue Boxing' telephone systems):
"…with intent to defraud, obtained a document, namely a computer program named scavenger, by electronic file transfer protocol, which was capable of being used to obtain a benefit or pecuniary advantage"[2]
With a charge of this nature the defense was able to argue that a computer program is not a document. In this case it was an unsuccessfully, however there have been other cases where the defense has been successfully due the law not clearly handling IT based crimes both in New Zealand and other counties.

With arguments like the above in New Zealand case law, there was doubt within the New Zealand business community (whether founded or not) of the legal status of IT based crimes[3]. At the time, this left IT Security professionals concerned as there was limited legal recourse for when the technical defenses of IT systems are attacked or breached. In 1997 the New Zealand Law Commission began a project studying international trade[4], as part of this project the NZ Law Commission produced four reports to Parliament on the subject of 'Electronic Commerce'[5].These reports summarized a number of the legal issues surrounding, Electronic Commerce in New Zealand and made recommendations.

Most of the issues the Law Commission covered could, as well as being described 'Electronic Commerce' issues, be described as the legal issues of IT Security in New Zealand. A number of the recommendations made by the NZ Law Commission have now become New Zealand law.

---

[2] The Queen v Borislav Misic [2001] CA454/00 - http://www.brookers.co.nz/legal/judgments/Default.asp?doc=2000\ca454.htm#Number1

[3] Ecom 2, Paras 61-62 - http://www.lawcom.govt.nz/documents/publications/R58.pdf
[4] Ecom 1, Preface - http://www.lawcom.govt.nz/documents/publications/R50.pdf
[5] Ecom 1-3 and Computer Misuse

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This has mostly been covered through two Acts. These Acts are the greatest legal change to NZ IT security to date. These Acts are, the 'Crimes Amendment Act 2003'[6] and the 'Electronic Transactions Act 2002'[7]. These Acts have been backed up through clarifications in the 'Interpretations Amendment Act 1999'[8] of terms such as 'document'.

© SANS Institute 2004, Author retains full rights.

[6] Crimes Amendment Act 2003
[7] Electronic Transactions Act 2002
[8] Crimes Interpretations Act 1999

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Introduction

Between 1998 and 2000 the New Zealand Law Commission presented four reports to Parliament[9]. These reports have helped shape New Zealand's IT related laws with two Acts of Parliament including some of the recommendations.

The first of these two Acts, the 'Electronic Transactions Act 2002'[10] (ETA) is intended to clarify the legal status of business & legal transactions that that occur in an electronic format. As noted earlier in this essay, this was partly to ensure contracts and the like that were agreed by email or other electronic techniques are binding. Prior to the ETA, businesses had some level of doubt in electronic based contracts.

> Nobody's really sure whether or not electronic documents are binding (some Kiwi lawyers say yes, some no), or to what degree commercial and consumer protection laws apply to Internet transactions as well as 'normal' trade and commerce.[11]

With most IT professionals being aware of this uncertainty, some form of legislation was required.

The ETA is also intended to act as enabler for prior laws that were written in a way that did not allow for electronic methods to be used to satisfy the requirements of the laws. In Ecom 2[12]it was noted that a number of the requirements of existing laws could only be fulfilled through the use of paper, conventional mail systems or the physical attendance of people, e.g.: The Auctioneers Act 1928 requires the presence of at least six people; this does not cover on-line actions well.

As well as these clarifications introduced by the ETA, the Act also introduced the ideas that would be considered of great relevance to IT security professions, for example section 24 of the ETA[13] deals with the reliability of electronic signatures and documents. Although the technologies and techniques behind the electronic signing of documents have evolved over time (and will continue to evolve), the law makers behind the ETA have had the foresight to allow for changes of technologies by using wording that does not lock the public into one technology in order to satisfy the law. This befit of the wording in the ETA has even been noted in reports from government departments[14].

---

[9] Ecom 1-3 and Computer Misuse
[10] Electronic Transactions Act 2002
[11] When governments attack - http://www.pcworld.co.nz/pcworld/pcw.nsf/UNID/866A0C23A4355BA2CC256879000FCA03?OpenDocument&Highlight=2,Juha,Saarinen
[12] Ecom 2 - http://www.lawcom.govt.nz/documents/publications/R58.pdf
[13] Electronic Transactions Act 2002, Section 24
[14] ETA 2002: Plain Language Section by Section Explanation, Section 21 - http://www.med.govt.nz/irdev/elcom/transactions/explanation/eta-explanation.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The second of these two acts, the 'Crimes Amendment Act 2003'[15] introduced a number of new sections to the principal Act (the Crimes Act 1961[16]) under the title "Crimes Involving Computers" (sections 248-254).
These new sections clearly allowed prosecutions for the types of case the average IT security professional would term Un-Authorized Hacking/Cracking (or Black Hat Hacking/Cracking) and also the use of a computer for committing another crime (allowing for the case where the crime was not already covered in existing laws). Also introduced later in the Amendment Act were changes to the existing interception laws (that enabled legal interception in certain cases) to bring electronic communications (e.g. email) in line with more traditional communications (e.g. telephone).
The sections introduced have been broadly defined to help avoid them becoming dated as technologies more on with time.

Both of these two Acts came into effect in the later part of 2003 and have been a good starting point in building a basic legal framework for the security of the New Zealand IT industry. Although these Acts have been a solid starting point for laws around IT Security they do have a number of implications for those working in IT and potential issues.

© SANS Institute 2004, Author retains full rights.

[15] Crimes Amendment Act 2003 Sections 248-254
[16] Crimes Act 1961

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Security Implications of the 'Electronic Transactions Act 2002'[17]

One of the broad issues highlighted by the four reports produced by the New Zealand Law Commission between 1998 and 2000[18] was that that the existing laws were not well equipped to handle the use of electronic means to carry out requirements of New Zealand's laws. The reasons were summed up in Ecom 1, "the law which New Zealand inherited from England at the turn of the twentieth century was designed to facilitate paper-based transactions."[19].The type of impact this had on e-commerce and electronic transactions was noted in the Introduction of this essay.

For a country that strives to be at the top of technology, having laws that do not lead themselves to being e-commerce enabled was not desirable. This lead to the introduction of the Electronic Transactions Act 2002[20], this Act was largely based on the NZ Law Commission's reports.

As New Zealand was one of the later countries to introduce laws relating to 'e-commerce', the NZ Law Commission was in a position where it was able to draw heavily from the United Nations Commission on International Trade Law (UNCITRAL) Model Law[21] and also it was able to look to the laws of a number countries (and US states) in an attempt to define laws that would best work for New Zealand. For example Ecom 1 noted that the 'Digital Signature Act 1995 (Utah)' is "technology specific in that only digital signature technology using public key cryptography receives legal recognition"[22]. It was intended that the NZ Law Commission's recommendations avoid these issues.

The resulting Electronic Transactions Act 2002 is primarily aimed at clarifying that electronic transactions do have legal recognition. As well as this, the ETA also contains a number of Sections that are of interest to IT staff securely implementing solutions for electronic transactions, be they legal or commercial.

What is most likely pleasing about this Act to most IT professionals is the technology neutral approach it takes. Considering that Act came from reports that were began in 1998, if it had taken technology specific approach, New Zealand may have ended up with a law that came into effect late 2003 stating 56-bit DES was legal requirement for e-commerce despite it being surpassed as a suitable encryption method for many transactions.

---

[17] Electronic Transactions Act 2002
[18] Ecom 1-3 and Computer Misuse
[19] Ecom1 para E1 - http://www.lawcom.govt.nz/documents/publications/R50.pdf
[20] Electronic Transactions Act 2002
[21] Ecom 1- http://www.lawcom.govt.nz/documents/publications/R50.pdf
[22] Ecom 1, para 325 - http://www.lawcom.govt.nz/documents/publications/R50.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Act avoids these technology specific issues by using board definitions stating what a technology should achieve as apposed to how, for example the Act defines an Electronic Signature as a "method used to identify a person and to indicate that person's approval"[23].

Using this approach the ETA achieves many of the requirements an IT security professional would impose on an e-commerce system with locking it to 'todays' technology. In board terms the ETA achieves:

- Authentication[24]
- Integrity of Data[25]
- Non-repudiation by providing both Authentication & Integrity

Additional the Act covers Times of Dispatch & Receipt[26] to allow for time critical transactions.

As noted above the Act is quite workable and should serve New Zealand well for a number of years with changing technologies, however it does have at some drawbacks. In using these board technology neutral terms throughout the Act, there has been little guidance provided to IT security professionals as to what is considered acceptable by law when implement systems that comply with the ETA.

Much of the of guidance that has been provided to decide if an implementation meets the requirements of the Act, is that the implementation must be adequate. For example the legal requirement for an electronic signature states that it "must adequately identify the signatory"[27].

This then raises the issue of what is adequate. MED noted that this largely follows the common law approach[28] and also indicated that this will be clarified through case law by stating that this "does result in open-textured tests"[29]. MED has indicated what is considered adequate would depend on the circumstances that it is used[30]. This potently creates a wide range of what is 'adequate'.

This does form a practical approach of defining technical requirements of secure implementations as time goes on. It does also leave a risk, people involved in process of deciding case law are not always technically skilled, their skills are in the legal process. This leaves them relying heavily on IT expect wittinesses, if a

[23] Electronic Transactions Act 2002 Section 5
[24] Electronic Transactions Act 2002 Sections 5, 22, 23, 24
[25] Electronic Transactions Act 2002 Sections 17, 24ss(1)(d)
[26] Electronic Transactions Act 2002 Sections 10, 11
[27] Electronic Transactions Act 2002 Sections 22
[28] ETA 2002: Plain Language Section by Section Explanation, Section 21 - http://www.med.govt.nz/irdev/elcom/transactions/explanation/eta-explanation.pdf
[29] ETA 2002: Plain Language Section by Section Explanation, Section 22 - http://www.med.govt.nz/irdev/elcom/transactions/explanation/eta-explanation.pdf
[30] ETA 2002: Plain Language Section by Section Explanation, Section 22 - http://www.med.govt.nz/irdev/elcom/transactions/explanation/eta-explanation.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

compelling IT expect wittiness is not suitably versed in IT security, they may be lead to make poor decisions which will undermine NZ's new e-commerce law.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Security Implications of the 'Crimes Amendment Act 2003'[31]

Overall computer security related laws are of befit to the New Zealand IT industry and New Zealand in general. In fact it was highlighted during the Parliamentary debates of these amendments the importance computers play in the day to day lives of the average person. Even if a person does not directly use a computer system, they may in-directly use computer as passenger of an aircraft that makes use of computer systems[32].

Like the with the introduction of the ETA, New Zealand was one of the later countries to introduce laws around computer crimes. Many computer professionals at the time were aware of the potential issues the lack of laws raised, this was even noted by the 'House of Representatives' during the third reading in order to emphasized the importance of the Act.
"New Zealand is one of the few counties in the world that does not provide for computer crime"[33].

Although the process was slow, it most like befitted the Bill through forcing carefully consideration. Even with this consideration, it was noted early in the drafts stages that this Bill maybe be more encompassing than was intended.[34] Even with these issues the 'Crimes Involving Computers' sections made it to the Act with few changes.

Also like the ETA, this Act worded it in a way that avoids it being updated for a number of years by using board terms. The wording of this Act would allow it to apply as well 20 years ago as it does now and it should apply suitably as time goes on (for the foreseeable future at least). Although this board wording befits the public by avoiding constant amending of the Act to keep the law current, it has some implications to IT security professionals and the wider IT users.

The 'Crimes Amendment Act 2003'[35] broadly defines four new computer related crimes in sections 248 – 254.
The new crimes briefly are:

- "Accessing [a] computer system for a dishonest purpose"[36].
- "Damaging or interfering with [a] computer system"[37].

[31] Crimes Amendment Act 2003
[32] Brian Connell, 12 June 2003, NZ Parliamentary Debates page 6239
[33] Marc Alexander, 17 June 2003, NZ Parliamentary Debates page 6326
[34] Meeting with Hon Swain - CAB #6, Telecommunications Bill, Digital Copyright Discussion Paper - http://www.internetnz.net.nz/issues/issues010919PaulSwain.html
[35] Crimes Amendment Act 2003
[36] Crimes Amendment Act 2003, Section 249
[37] Crimes Amendment Act 2003, Section 250

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- "Making, selling or distributing or possessing software for committing a crime"[38].
- "Accessing [a] computer system without authorization"[39].

At first glance these laws seem reasonable; however an IT security person would pick up on issues around these, such as section 251 and the impacts on dual use software.

Most cases along these lines of legitimate use have been covered in the sections of the Act. In the case of Section 251, the law applies if the person intends to use software for a crime or promotes using it for a crime. This allows security professionals to use dual use tools, while still making it's use for unauthorized hacking illegal.
Although most cases of legitimate have been covered, not all have. Section 251 does potentially raise some interesting issues around concepts that many security professionals are supportive of, the sharing of information and full disclosure.

For example if a IT security professional wrote a report of how a dual use 'hacking' tool was used to attack a server they maintain, then went on to describe how servers in general could be protected from the tool and provided a link to the 'tool' so that others could study it, they would fall foul of this law. This law applies if "…he or she promotes [the tool] as being useful for the commission of a crime (whether or not he or she also promotes it as being useful for any other purpose)"[40]. By reporting on the attack in details, the security professional is inadvertently promoting the ways the 'tool' could be used for a crimes and by linking to it assisting in it distribution.

At a stretch, if in the above, a popular dual use tool had be named to use as an example and the Reference section of this essay linked to it's website, this essay would have breached the Act.

It is unlikely the State would chose to prosecute in a case like this, but it should be noted that the potential is there and the law fits better than the successful prosecution in the Background section of this essay.

A number of the other the implications that the sections of this Act have on IT security and wider the IT industry have been picked in a range of articles. A Computer World article by Saarinen[41] covered a number of these when the Act

[38] Crimes Amendment Act 2003, Section 251
[39] Crimes Amendment Act 2003, Section 252
[40] Crimes Amendment Act 2003, Section 251
[41] When governments attack - http://www.pcworld.co.nz/pcworld/pcw.nsf/UNID/866A0C23A4355BA2CC256879000FCA03?OpenDocument&Highlight=2,Juha,Saarinen

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

was still in the Bill stages (and these still apply). Saarinen's article[42] noted that probing for open mail relays for creating spam blocking lists is an unauthorized use of a mail server.
The activity of maintaining an open mail relay would be seen by many people as a case where the 'greater good' of the computer industry (and of the end-user that receives the spam) outweighs the unauthorized access required to probe the mail server. The Act as it stands makes no allowance for this type of access and it would breach Section 252 as the maintainer of an open relay list has no authorized access.

The defense that a person could have in a case like this is if they were able to argue that accessing a mail server on the Internet (even when not sending mail to the users of it) can be considered authorized because it is available. Of course precedent like this may undermine the purpose of the law by provide an angle of defense for the types of actions this law was intended to cover.
Additionally a further downside of Section 252, it does not apply in the case of a 'privilege escalation' style of attack (as long the attack does not 'damage' the system). This is because the law does not apply when a person has been authorized to access for one purpose, but then uses the system for something they did not have authorized access for.

Although Sections 249-252 form the bulk of the computer related laws, Section 248 covers the interpretation, defining what a Computer System is. Briefly, this Section defines a Computer System as one or more of the following:

- "a computer; or
- 2 or more interconnected computers; or
- any communications links between computers or to remote terminals or another device; or
- 2 or more interconnected computers combined with any communications links between computers or to remote terminals or another device"[43]

It also goes on to broadly include all peripheral devices and external storage. Worded this way, allows the laws around computers to remain workable as technology evolves. Most likely the term computer would be clarified through precedents set in case law in much the same way as 'adequate' is expected to under the ETA.

As a 'computer' is not defined, this may also leave these laws open to potential private criminal prosecutions that are not in the 'spirit of the law' (It should be noted that this is unlike as private criminal prosecution cases in New Zealand are quite rare). This is mainly due the pervasiveness of computer devices in much of everyday life.

[42] When governments attack - http://www.pcworld.co.nz/pcworld/pcw.nsf/UNID/866A0C23A4355BA2CC256879000FCA03?OpenDocument&Highlight=2,Juha,Saarinen
[43] Amendment Act 2003, Section 248 ss (a)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Recently in the US, StorageTek made a civil suit against 3rd party people servicing customer owned equipment that they had manufactured[44]. Under New Zealand laws with this wide reaching definition of a 'computer', if StorageTek was able to argue that the 'System Maintenance' part of their tape libraries was a different 'computer' from the rest of the library and that 3rd party people service people (maybe even the customer) had no authorization to use that 'computer', Section 252 of the Act would apply. This would be in New Zealand considered an extreme interpretation of the Act and would raise the interesting idea of when does an owner (and their service agent) have authorization to work with their equipment.

Although the above points do raise some issues with the Crimes Amendment Act 2003, it does cover the typical cases of computer related crimes. However the Act does not address how to apply these laws in the real world. Sasrinen's PC World article does raise some interesting points of how they will work in the real world.
"Does the police force have an IT forensic squad? Or will they rely on outside experts to help them gather evidence?"[45]
Through the author's discussions with a member of the Police's IT forensic squad (The Electronic Crimes Laboratory), it can be confirmed they do exist, however like is often the case with teams of this nature, they are busy team. Investigations of this type require skill and as most IT professions would be aware it also requires time and care. They would also have to deal with issue of "Unless you're technically very skilled, it would be hard to prove your innocence."[46] Most likely, the computer an attack was launched from is another victim.

Although these application issues are real, these issues occurs with new types of laws worldwide and the problems these issues pose should reduce over time as the people that enforce and prosecute the laws gain a better understanding of computer related crimes. Until this happens, it is hoped that the appropriately skilled IT Security people will be involved to ensure that innocence people are not charged with computer crimes.

[44] DMCA hammer comes down on tech service vendor - http://lawgeek.typepad.com/lawgeek/2004/07/dmca_hammer_com.html
[45] When governments attack - http://www.pcworld.co.nz/pcworld/pcw.nsf/UNID/866A0C23A4355BA2CC256879000FCA03?OpenDocument&Highlight=2,Juha,Saarinen
[46] When governments attack - http://www.pcworld.co.nz/pcworld/pcw.nsf/UNID/866A0C23A4355BA2CC256879000FCA03?OpenDocument&Highlight=2,Juha,Saarinen

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Conclusions

Until late 2003 when both of the two Acts outlined in document came into effect, there were no laws that adequately coved the New Zealand IT industry. Up until that point the only legal recourse for IT security was through ill-fitting Acts.

Although some of the details are yet to be worked out through tests of case law, the Electronic Transactions Act 2002, clears up the legal standing of transactions made by electronic methods. This eases the public debate of 'is e-commerce legal' and allows IT professionals to get on with the job on implementing 'e-commerce' systems. With the emphasis of the Act on 'adequate' security, hopefully IT professionals with limited security experience will be encouraged to research Best Practices and work out what adequate is.

The introduction of the Crimes Amendment Act 2003 even with the potential issues within the wording can be seen beneficial to the New Zealand IT industry. The Act gives the law enforcement officials some 'teeth'. Allowing them to investigate and prosecute 'hacking/cracking' and other computer crimes knowing that there are the legal statues to back them up.
The Act does have some serious potential issues in that the wording may allow it to be inappropriately applied. Hopefully if this becomes an issue to the industry, Parliament will be lobbied by people with a suitable IT security background and the Act will be further amendment.

As with many modern laws both the Computer Crimes part of the Crimes Amendment Act 2003 and Electronic Transactions Act 2002 are quite readable for people with no legal background. For those IT professionals that work with security or implementing systems where these New Zealand laws apply it is mostly likely of befit taking the time to read these Acts to gain a better understanding the legal framework.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendices

References

1. Office of the Clerk of the House of Representative. “Legislative Procedure.” The New Zealand Parliament. URL: http://www.clerk.parliament.govt.nz/Publications/Other/Booklet/2+-+Legislative+Procedure.htm (2 Jul 2004)

2. Anderson, J. “The Queen v Borislav Misic [2001] CA454/00.” 11 Apr 2001. URL: http://www.brookers.co.nz/legal/judgments/Default.asp?doc=2000\ca454.htm#Number1 (10 Jul 2004)

3. New Zealand Law Commission. “Part One: A Guide for the legal and business community.” Electronic Commerce. Oct 1998. URL: http://www.lawcom.govt.nz/documents/publications/R50.pdf (03 Jul 2004)

4. New Zealand Law Commission. “Part Two: A basic legal framework.” Electronic Commerce. Nov 1999. URL: http://www.lawcom.govt.nz/documents/publications/R58.pdf (03 Jul 2004)

5. New Zealand Law Commission. “Part Three: Remaining Issues.” Electronic Commerce. Dec 2000. URL: http://www.lawcom.govt.nz/documents/publications/R68.pdf (03 Jul 2004)

6. New Zealand Law Commission. “Computer Misuse.” May 1999. URL: http://www.lawcom.govt.nz/documents/publications/R54.pdf (03 Jul 2004)

7. New Zealand Crimes Amendment Act 2003

8. New Zealand Electronic Transactions Act 2002

9. New Zealand Crimes Interpretations Act 1999

10. Ministry of Economic Development. “Electronic Transactions Act 2002: Plain Language Section by Section Explanation.” Dec 2002 URL: http://www.med.govt.nz/irdev/elcom/transactions/explanation/eta-explanation.pdf (09 Jul 2004)

11. Crimes Act 1961

12. Connell, Brian Parliamentary Debates (HANSARD) 12 June 2003 Wellington: House of Representatives, 12 Jun 2003. 6239

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

13. Alexander, Marc Parliamentary Debates (HANSARD) 17 June 2003 Wellington: House of Representatives, 17 Jun 2003. 6326

14. InternetNZ. “Meeting with Hon Swain - CAB #6, Telecommunications Bill, Digital Copyright Discussion Paper.” 2001 URL: http://www.internetnz.net.nz/issues/issues010919PaulSwain.html (18 Jul 2004)

15. Saarinen, Juha. “When governments attack” 1 Feb 2000 URL: http://www.pcworld.co.nz/pcworld/pcw.nsf/UNID/866A0C23A4355BA2CC256879000FCA03?OpenDocument&Highlight=2,Juha,Saarinen (12 Jul 2004)

16. Schultz, Jason. “DMCA hammer comes down on tech service vendor” 9 Jul 2004 URL: http://lawgeek.typepad.com/lawgeek/2004/07/dmca_hammer_com.html (14 Jul 2004)

17. New Zealand Crimes Amendment Bill (No 6)

18. Boren, Tony. “Legislation to Facilitate Electronic Commerce.” 1 Mar 2000 URL: http://www.itanz.org.nz/docs/Submissions/CrimesAmendmentBillNo61March200.pdf (18 Jul 2004)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abbreviations and Acronyms

"Ecom 1"	Electronic Commerce Part One: A Guide for the legal & business community
"Ecom 2"	Electronic Commerce Part Two: A basic legal framework
"Ecom 3"	Electronic Commerce Part Three: Remaining Issues
"ETA"	New Zealand Electronic Transactions Act 2002
"MED"	Ministry of Economic Development
"NZ"	New Zealand

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Crimes Amendment Act 2003, Sections 248-253

``Crimes involving computers

``248. Interpretation—

``For the purposes of this section and sections 249 and 250,—

```access', in relation to any computer system, means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system

```computer system' —

``(a) means—

``(i) a computer; or

``(ii) 2 or more interconnected computers; or

``(iii) any communication links between computers or to remote terminals or another device; or

``(iv) 2 or more interconnected computers combined with any communication links between computers or to remote terminals or any other device; and

``(b) includes any part of the items described in paragraph (a) and all related input, output, processing, storage, software, or communication facilities, and stored data.

``249. Accessing computer system for dishonest purpose—

``(1) Every one is liable to imprisonment for a term not exceeding 7 years who, directly or indirectly, accesses any computer system and thereby, dishonestly or by deception, and without claim of right,—

``(a) obtains any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or

``(b) causes loss to any other person.

``(2) Every one is liable to imprisonment for a term not exceeding 5 years who, directly or indirectly, accesses any computer system with intent, dishonestly or by deception, and without claim of right,—

``(a) to obtain any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or

``(b) to cause loss to any other person.

``(3) In this section, `deception' has the same meaning as in section 240(2).

``250. Damaging or interfering with computer system—

``(1) Every one is liable to imprisonment for a term not exceeding 10 years who intentionally or recklessly destroys, damages, or alters any computer system if he or she knows or ought to know that danger to life is likely to result.

``(2) Every one is liable to imprisonment for a term not exceeding 7 years who intentionally or recklessly, and without authorisation, knowing



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

that he or she is not authorised, or being reckless as to whether or not he or she is authorised,—

``(a) damages, deletes, modifies, or otherwise interferes with or impairs any data or software in any computer system; or

``(b) causes any data or software in any computer system to be damaged, deleted, modified, or otherwise interfered with or impaired; or

``(c) causes any computer system to—

``(i) fail; or

``(ii) deny service to any authorised users.

``251. Making, selling, or distributing or possessing software for committing crime—

``(1) Every one is liable to imprisonment for a term not exceeding 2 years who invites any other person to acquire from him or her, or offers or exposes for sale or supply to any other person, or agrees to sell or supply or sells or supplies to any other person, or has in his or her possession for the purpose of sale or supply to any other person, any software or other information that would enable another person to access a computer system without authorisation—

``(a) the sole or principal use of which he or she knows to be the commission of a crime; or

``(b) that he or she promotes as being useful for the commission of a crime (whether or not he or she also promotes it as being useful for any other purpose), knowing or being reckless as to whether it will be used for the commission of a crime.

``(2) Every one is liable to imprisonment for a term not exceeding 2 years who—

``(a) has in his or her possession any software or other information that would enable him or her to access a computer system without authorisation; and

``(b) intends to use that software or other information to commit a crime.

Cf 1961 No 43 ss 216D(1), 229, 244

``252. Accessing computer system without authorisation—

``(1) Every one is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system.

``(2) To avoid doubt, subsection (1) does not apply if a person who is authorised to access a computer system accesses that computer system for a purpose other than the one for which that person was given access.

``(3) To avoid doubt, subsection (1) does not apply if access to a computer system is gained by a law enforcement agency—

``(a) under the execution of an interception warrantor search warrant; or



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

``(b) under the authority of any Act or rule of the common law.

``253. Qualified exemption to access without authorisation offence for New Zealand Security Intelligence Service—

``Section 252 does not apply if—

``(a) the person accessing a computer system is—

``(i) the person specified in an interception warrant issued under the New Zealand Security Intelligence Service Act 1969; or

``(ii) a person, or member of a class of persons, requested to give any assistance that is specified in that warrant; and

``(b) the person accessing a computer system is doing so for the purpose of intercepting or seizing any communication, document, or thing of the kind specified in that warrant.

``254. Qualified exemption to access without authorisation offence for Government Communications Security Bureau—

``Section 252 does not apply if the person that accesses a computer system—

``(a) is authorised to access that computer system under the Government Communications Security Bureau Act 2003; and

``(b) accesses that computer system in accordance with that authorisation.

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## *Credits*

A special thanks is due to Ms Sarah Bolland, LLB.

Due the course of writing this essay, Sarah has answered a number of queries relating to clarifying legal terms, correct citations of legal works and suggestions for researching legal documents.

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.