

**Enforcing Without Legislation:
Implementing Information Security in Australian Context**

Sam Berner

August 21, 2001

TABLE OF CONTENTS:

1. [Introduction](#)
 - 1.1. [Stating the Problem: Too Little, Too Late](#)
 - 1.2. [Terminology](#)
2. [Current Legislation](#)
 - 2.1. [Acts and Regulations - Luddites Rejoice!](#)
 - 2.2. [IT Security Policies - Lots of Data With No Backup](#)
 - 2.3. [Trends for the Future](#)
3. [Basics of Information Security](#)
 - 3.1. [Hackers](#)
 - 3.2. [Viruses and related unpleasantness](#)
 - 3.3. [Computer Crime](#)
 - 3.4. [Internet Crime](#)
4. [Recommendations](#)
 - 4.1. [How does this affect the legal firm environment?](#)
 - 4.2. [Best Tools of the Trade](#)
 - 4.3. [Educating the Masses](#)
5. [Appendix](#)
6. [REFERENCES](#)

1. Introduction

1.1. Stating the Problem: Too Little, Too Late

Australia's legislative bodies have been taken by surprise when it came to electronic crime. This in itself is nothing to be surprised about, as Australia has been taken by surprise generally when it comes to all things not related to sheep shearing, dream time and bush. It is, however, an issue of great distress to institutions doing business in and with Australia. This report provides an overview of the legislative situation pertaining to information security in Australia, discusses most common forms of electronic crime and how it affects legal firms doing business, and ends with proposing that some basic tools and massive education of users may provide a better solution than Parliamentary talk.

1.2. Terminology

Before discussing any of the above issues further, I would like to provide the reader with some basic definitions of what constitutes electronic crime, what are computer information systems, and what exactly falls under the auspices of information security.

The Australian Federal Police report, entitled "The Virtual Horizon: Meeting The Law Enforcement Challenges-Developing an Australasian law enforcement strategy for dealing with electronic crime" (AFP, 2000), outlines a number of **electronic crimes**:

- theft of telecommunications services (much like the phone phreakers of old),
- communications for the advancement of criminal conspiracies,
- piracy,
- dissemination of offensive material (which often relates to offences such as cyberstalking),
- electronic money laundering and tax evasion,
- electronic vandalism and terrorism,
- sales and investment fraud,
- illegal interception of telecommunications signals,
- and electronic funds transfer fraud.

The AFP further defines electronic crime as "Offences whereby a computer is used as a tool to commit an offence, or as a target of an offence, or the use of a computer as a storage device in relation to an offence."

Information security is a state of affairs where information, information processing and communication are protected against the confidentiality, integrity and availability of information and information processing. In the context of information networks this also covers reliable identification and authentication of persons and non-alteration of data. It has several dimensions and layers: hardware security; software security; administrative security; physical security; operational security; personnel security; communications security; security of the data resources, etc (Poysti, 2000).

In the legal sense information security covers the obligations to take adequate measures for the purpose of safeguarding the state of affairs corresponding the required level of security, and, notably, the protection of rights related to the informational assets. These assets are composed of raw data organised in structured documents (composed of voice, visual and textual or other symbolic elements), the platform (media) and the rights concerning the use of the actual contents. The protection of this entirety via technical and organisational measures and the legal protection of the technologies fall under the general legal conception of information security. Information security is among the factors that define de facto efficiency of some fundamental rights and freedoms. Right to privacy and to informational self-determination as a personality right can be guaranteed only if the design of the information systems, chains of information logistics and the hardware & software infrastructures and organisation structures take into account the concrete privacy rights.

The US Glossary of Telecommunications Standards defined "information security" as "Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by automated information systems. *Note 1:* The unauthorized disclosure, modification, or destruction may be

accidental or intentional. *Note 2:* Automated information systems security includes consideration of all hardware and software functions, characteristics and features; operational procedures; accountability procedures; and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices, such as computers, transmission lines, and power sources; and personnel and communications controls needed to provide an acceptable level of risk for the automated information system and for the data and information contained in the system. Automated information systems security also includes the totality of security safeguards needed to provide an acceptable protection level for an automated information system and for the data handled by an automated information system.”

Information systems are the means by which organisations and people, utilising information technologies, gather, process, store, use and disseminate information. The definition of information systems includes: computer hardware; interconnected peripheral equipment; software, firmware and other means of expressing computer programs; algorithms and other specifications either embedded within or accessed by such computer programs; manuals and documentation on paper, magnetic, optical and other media; communication facilities, such as terminal/customer premises equipment and multiplexers, on the information system side of the network termination point of public telecommunication transport networks as well as equipment for private telecommunication networks not offered to the public generally; security control parameters; storage, processing, retrieval, transmission and communication data, such as check digits and packet switching codes, and procedures; data and information about parties accessing information systems; and user identification and verification measures (whether knowledge-based, token-based, biometric, behavioural or other). This definition may include elements that are proprietary or non-proprietary, public or private. This definition applies to elements whether or not they interact with the data being transmitted by the system or are necessary for the operation, use and maintenance of the other components of the system.

Prof. J. Patrick of Sydney University calls Information Systems “applied computing” (Patrick, 1998) He believes information systems should be a label that represents in the widest sense the issues apparent in creating a system that uses computers to satisfy individual and organisational needs beyond highly specialised functions. That is, an information system is all the issues involved in creating a system for the management of data in the context of a human organisational need. Hence Information Systems encompasses issues such as strategic planning, system development, system implementation, operational management, end-user needs and education. He differentiates Information Systems and Computer Science by the description that Computer Science is about developing and improving the performance of computers, hence computers are the focus of attention, whereas Information Systems is about making computer systems work for people and hence people are the focus.

2. Current Legislation

2.1. Acts and Regulations - Luddites Rejoice!

The Australian legislator, when it comes to electronically generated or stored information, is closer to the biblical Moses in outlook, than to Mr. Gates. The priorities seem to lie on the side of ensuring the privacy of Mr. Citizen and the protection of his tender offspring from the evils of the cyberspace. The protection of millions of dollars lost through hacking into corporate servers, or infectious viruses spreading corporate confidential information to your competitors are far removed from the quaintly Luddite authorities in Canberra.

A recent example of this mis-placed legislation is the [Privacy Amendment \(Private Sector\) Act¹](#), which comes into force on December 21. In plain English, the act prescribes the use of customer information collected by businesses. It will have a tremendous effect on business information systems, since one of its pre-requisites is that the information kept on the systems is “reasonably secure” (Withers, 2001). Since there is no legislation in Australia that ensures corporate information security can be enforced, businesses will have to cope on their own. Two years ago, it was the Y2K scare. Last year, the government enforced the Goods and Services Tax, throwing information systems in banks, accounting and legal firms into maddening disarray, not to mention the number of small businesses that went under because the cost of compliance was too high. Australian government is working hard at getting every enterprising little businessman out of his

urban comfort and out into the bush to shear sheep. After all, that part of our economy does not need any electronically complex legislation.

Not to mention the fact that the public sector is not governed by the same Amendment Act. The logical conclusion is that whereas the biggest collector of personal information is the state, which can do what it wants with the information in the name of "common good", does not allow others to do the same and withholding the information in its possession from the public domain. Some serious thoughts on the nature of possible amendments to our "Freedom of Information Act" should be in place here.

The way the act came into being, through the NPP Commission, is in itself far from legally proper (Greenleaf, 2000). The Commissioner was not a lawyer, the groups involved in the consultation never reached a consensus, and the whole thing, which was to be a draft of recommendations, not a legislation, passed through the Parliament without debate, and without being approved by any counsel.

The issue of online or computer-related criminal activity in Australia is one fraught with much uncertainty, particularly since authorities such as the Federal Police are unsure as to the actual extent of the problem. Steve Jiggins, director of the AFP's media and public relations, highlighted the issues of attempting to measure the problem. "Electronic crime varies in its manifestations, so it is difficult to discuss in terms of aggregate incidence and impact," he writes. "As a result, definitive information on the present extent and impact of electronic crime in Australia, New Zealand and overseas is not available."

But it is often the victim of these crimes that are resistant to informing authorities of electronic crime. "A significant amount of this crime is simply not reported," explained Jiggins. "This is in part... to avoid any potentially adverse impact on consumer confidence, or perhaps because of a lack of confidence in the capacity of law enforcement to deal with such issues in a timely way." (Jiggins, 2000)

According to the report, only two major Australian studies had been done to establish the extent of the problem--one in 1997 conducted by the Office of Strategic Crime Assessments (OSCA) and the Victoria Police, and one in 1999 by the Victorian Police and Deloitte Touche Tohmatsu.

The study from 1997 concluded that 37 percent of businesses had been subjected to some form of electronic attack or unauthorised computer access. Of those that were attacked, 90 percent experienced some breach from within the organisation and 60 percent were external (OSCA, 1997). The 1999 study offered similar results but also concluded that of those organisations that were attacked, 42 percent didn't even report the breach. Also, of those companies that experienced a breach, one third refused to provide a dollar value on what damage or loss had been incurred.

Another issue which complicates the matter is that cybercrime, or rather computer-related crime, covers so much ground that it can't necessarily be covered under one banner for protection. The breadth of offences that are encompassed by the term "cybercrime" or "e-crime" is a complicating factor in attempting to police it. In fact, no single authority has absolute control of the issue and some state police departments have developed their own strategies regarding particular elements of cybercrime. The Victorian Police Service, for example, has had a Computer Crime Investigation Squad (CCIS) in place since 1993 and its task has been to aid in the discovery and handling of technology-related offences. It liaises with Internet Service Providers (ISPs) and is primarily responsible for developing computer crime investigation and computer evidence handling procedures, as well as Internet investigation practices. Interestingly, a special section of the NSW police, the Child Protection Enforcement Agency, has established the Child Exploitation Internet Unit to help with the crackdown on Net-related offences regarding children. These include offences relating to child pedophilia and child pornography. It tends to take a more proactive approach with this problem by analysing Web sites and newsgroups that could lead to possible offenders. All state police departments have units that handle several types of fraud, including those that are technology related. South Australia's Serious Fraud Investigation Branch handles the state's problems relating to cybercrime offences that have a white-collar aspect, including fraud and false pretences, theft, breach of trust and secret commissions.

The newest invention of the techno-savvy powers in Canberra is the [CyberCrime Bill 2001](#)². Prematurely born, this new addition to the family of legal confusion has already been termed "overbroad knee-jerk reaction to recent well-publicised virus attacks" (Electronic Frontiers of Australia, 2001). It's clauses are in blatant contravention of the above-mentioned Privacy Act, stating among others that the time law enforcement agencies can take possession of computer equipment anywhere from 72 hours to five days - a

process that can cause substantial financial loss and inconvenience to the company concerned. Another clause prescribes the forced release of encryption keys, which raises questions about the security of data (Labihan, 2001). There goes Mr. Citizen's privacy, down the proverbial Australian creek.

The Australian Computer Society, the only Australian formal body that provides recognition of qualifications for the IT industry, has termed the Bill "excessive" (Daerne, 2001). ACS vice-president Philip Argy said an employee adding a graphic to the boss's email that slowed transmission, or a person who disabled a cookie, could also face 10 years in jail, and added that although "the ACS supported the legislation in principle, the breadth of definitions leaves everyday activity vulnerable to prosecution by misguided, if not overzealous, enforcement authorities." The ACS has serious reservations about the broad powers conferred upon statutory agencies. If the Bill becomes an Act, Mr. Citizen's freedom to surf the Internet will also go for a swim.

Apart from the Privacy Act and the CyberCrime Bill, our current regulatory environment is spread over acts and regulations dating from the 1980s. Crimes Act 1914 has an amended section (VIA) dealing with unlawful access and damage of data residing on Commonwealth (i.e. government) information systems. The Copyright Act 1968, in Section 4A provides legislation for copyrights of computer applications. This is about all there is to protect the valuable intangible assets of Australian businesses.

2.2. IT Security Policies – lots of data with no backup

Left with little value and much confusion, the Australian business generally walks the tight rope between trying to protect its own assets, and not breaking some unfathomable legislation that most people don't understand. The general situation is total lack of comprehension among non-technical staff as regards information security systems and management. Left to their own devices, the technical staff draft IT Security Policies that have no formal legal backing. On the other side of the corporate fence, the legal counsel drafts totally different policies, dealing with privacy, copyright and availability, that would be deemed non-executable by a recent university graduate of computing studies.

As an example of what I mean, I now propose to look at two samples of IT (not even IS) Security Policies. One belongs to the University of Technology, Sydney (Colhoun, 1998). The other belongs to a corporate body which we consulted with on their Knowledge Management venture. Due to non-disclosure clauses in our contract with that corporation, I cannot provide its name. We will refer to it as company X (X, 2000). E-Cognus (the KM Consultancy I manage) has not been party to these policies.

The aim of an information security policy is to provide a framework within which to define roles and responsibilities with respect to data security, to formulate and justify any regulations which are felt to be needed, and to make explicit the institution's attitude to any actions which threaten the security of information assets (Rabiette, 2001). The discussion below will limit itself to finding out how the two policies fulfill the roles mentioned above.

Although the UTS policy's aims fall within the general framework, however, its terminology is so broad that it would be very difficult defending it in court. Definitions are seriously lacking: for example, there is no specific definition of what constitutes "unauthorised access", and the responsibility for managing security are given to the "University", making it all quite ephemeral. The Internet is considered a hostile environment, and yet the policy does not clearly state what constitutes "explicitly permitted traffic". The policy purports to encourage privacy for users, while a few pages later, in a glaring inconsistency, allows the "University" to monitor or use "any account, device, or terminal" without notice.

The X's has a major flaw, which is in a way outside the policy. That flaw is that no new employee/contractor starting their work at company X are made aware of this policy. One employee, who is responsible for the Intranet/Extranet servers in company X, has not become aware that there is a policy until she decided it was time to audit the server security (SIRCAM virus having infected a few of the non-patched servers). That was two years into her employment by the company. Another clause prohibits "all" employees from accessing hackers' websites – a problem which the IS Security staff finds very frustrating, since they cannot legally gather intelligence on the "enemy". The third problem with the policy is that it is almost 2 years old, and is not being reviewed in the light of new IT developments. Although the policy talks about using tools to protect the system, it does not have provisions for security testing of these same system.

It is, therefore, a reactive instead of proactive approach to security management. The policy also does not provide for protecting mobile devices such as laptops and WAPs. Company X also did not consider that training the company staff in issues pertaining to information security was important enough to merit a place in the policy.

2.3. Legal Trends for the Future: "So what is the US doing about it?"

The title of this section is not meant to be another pun on Australian lack of initiative. It sadly reflects the current legislative situation in Australia. The government, the IT industry, the legislative bodies and the business are all looking eastward to the Big Brother(s) for guidance and expertise which we sadly lack. This is why it is of benefit to look at what is already happening in places like the UK and USA, since in all probability it will end up happening in Australia as well.

The topics encompassed by law, investigation, and ethics are not only those that practitioners taking the certification examination experience trouble with, but they are also the everyday parts of an information security program that one way or another can cause much embarrassment if not handled appropriately. Although these three subjects are related, to some extent they are different areas of expertise. Each is important in its own realm and can lead to problems if neglected in the administration of a security program. It is very important that the information systems security professional have a clear understanding of the laws and issues that affect their field and the kinds of criminal attacks they may experience against their systems.

In the UK, the [Data Protection Act](#)³ came into power in 1999. It pertains to personal data, i.e. information about living identifiable individuals or 'data subjects'. At the heart of the legislation is a set of eight Principles. Good information security practice is implied in all eight but particularly in Principle 7 which relates to the prevention of unauthorised or unlawful processing, and of accidental loss or damage to data. It is very much the prototype on which the Australian Privacy Act was based.

In 2000, the US Senate passed the [Government Security Information Reform Act](#), on which the Cybercrime Bill is modeled. The Act proposes to reform Government information security by strengthening information security practices throughout the Federal Government. This Act requires each agency to develop and implement an agency-wide information security plan for its assets and operations. It also requires this plan to be reviewed annually by agency program officials and Inspector General audits of information security programs and practices. It suggests implementing much needed and certainly overdue security practices that are as up to date as possible. The security measures on federal systems would also be frequently audited to guarantee that they are running with the most current patches (Cypherwar, 1999).

The [Cyber Security Information Act of 2000](#)⁴ was introduced in the USA to "encourage the secure disclosure and protected exchange of information about cyber security problems, solutions, test practices and test results, and related matters in connection with critical infrastructure protection". The most important part of the Act is that it exempts cyber-security information from the Freedom of Information Act - probably what made it so interesting to the Australian legislator.

Closer to home (and thus to worry) is Japan's attempt to have its Criminal Code amended by the end of this year to include "penal provisions against IT-based crime" (Kantanei, 2001). Other Asian countries are actively hosting seminars and conferences. Asia - especially the south east part - has been the thorn in the side of Western IT industry: software piracy is endemic and counterfeit goods sell under the nose of the authorities. A few of the rather stronger brands of viruses have originated in Asia. Of the 80 plus attempts at my PC ports that the firewall registers per session (4 to 5 hours), more than 80% are from ISPs originating in Asia. It is therefore of great interest to Australia to keep an eye on Information security developments in that region.

3. Basics of Information In-Security

According to Mitchell, the widespread use of computers has resulted in a new challenge for law enforcement - computer crime. A computer crime can be said to occur when a computer is the target of the offense, that is, when the actor's conduct is designed to steal information from, or cause damage to, a computer or computer network. Some computer crime definitions also include cases in which the computer is an integral

tool in committing an offense. For example, a bank teller might write a computer program to skim small amounts of money from a large number of accounts. Although this might constitute a computer crime, such conduct is prohibited by traditional criminal laws, and could be charged accordingly (Mitchell & Charney, 2001).

Security violations occur because many people think that newer means safer. There is always the risk of getting immersed in new technology to the point where we lower the defenses that we developed with the older technology (Chantler, 1998). Most policies have provisions for security audits and logs – however, the fact is that even with quite good software (such as NT Server 4.0 or higher), a good cracker can bypass the logs. A security violation includes one or more of the following acts:

- **Unauthorised access:** unauthorised access to, use of, copying of, or communication with data contained on computing equipment;
- **Unauthorised Release:** discloses or releases data on any matter affecting the Public Service or the business of the Public Service;
- **Damaging computer data:** making unauthorised changes to, damaging, contaminating, destroying, erasing or rendering meaningless data that resides on computer equipment;
- **Computer fraudulent use/misuse:** fraudulently obtaining a financial or other advantage, or causing detriment to another by the use or manipulation of data;
- **Theft:** theft of any hardware device or software containing data or information that is the property, or in the custody of the State.

The extent of action to be taken where a violation has occurred depends on the severity of the violation, the extent of evidentiary material, the mechanisms used to achieve the breach, and the nature of the data contained on the system where the breach occurred. Effective action may involve remedial training, disciplinary action, interim measures (restoring systems, advising other affected agencies, monitoring, advising police of criminal activity), and/or preventative measures against a re-occurrence (system modifications, increased security, monitoring).

To understand what has actually taken place during a computing session, it is often necessary to have a mechanism that captures the detail surrounding access, particularly accesses occurring outside the bounds of anticipated actions. Any activity beyond those designed into the system and specifically permitted by the generally established rules of the site should be considered a violation. Capturing activity permits determination of whether a violation has occurred or whether elements of software and hardware implementation were merely omitted, therefore requiring modification. In this regard, tracking and analyzing violations are equally important (Fisher, . Violation tracking is necessary to satisfy the requirements for the due care of information. Without violation tracking, the ability to determine excesses or unauthorized use becomes extremely difficult, if not impossible. For example, a general user might discover that, because of an administrative error, he or she can access system control functions. Adequate, regular tracking highlights such inappropriate privileges before errors can occur. An all-too-frequently overlooked component of violation processing is analysis. Violation analysis permits an organization to locate and understand specific trouble spots, both in security and usability . A specialized form of violation examination, intrusion analysis (i.e., attempting to provide analysis of intrusion patterns), is gaining increased attention. As expert systems gain in popularity and ability, their use in analyzing patterns and recognizing potential security violations will grow. The need for such automated methods is based on the fact that intrusions continue to increase rapidly in quantity and intensity and are related directly to the increasing number of personal computers connected to various networks. The need for automated methods is not likely to diminish in the near future, at least not until laws surrounding computer intrusion are much more clearly defined and enforced.

Currently, these laws are not widely enforced because damages and injuries are usually not reported and therefore cannot be proven. Overburdened law enforcement officials are hesitant to actively pursue these violations because they have more pressing cases (e.g., murder and assault). Although usually less damaging from a physical injury point of view, information security violations may be significantly damaging in monetary terms. In several well-publicized cases, financial damage has exceeded \$10 million. Not only do violation tracking and analysis assist in proving violations by providing a means for determining user errors

and the occasional misuse of data, they also provide assistance in preventing serious crimes from going unnoticed and therefore unchallenged.

3.1. Hackers

The term “hacker” is a slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject. Among professional programmers, depending on how it is used, the term can be either complimentary or derogatory, although it is developing an increasingly derogatory connotation. The pejorative sense of hacker is becoming more prominent largely because the popular press has co-opted the term to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data. Hackers, themselves, maintain that the proper term for such individuals is cracker [<http://www.webopedia.com/TERM/h/hacker.html>].

Dreyfus (1998) defines a hacker as “anyone who ‘breaks open’ code and manipulates it in a clever or original, but not necessarily illegal, fashion. However a more recent definition would be: anyone who breaks into a computer without authorisation. Breakers are people who ‘hack’ the telephone system illegally.

Hackers use handles - on-line nicknames - to disguise their identities and to present a particular image of themselves. There is a distinct hierarchy in the hacking community, with elite (experienced) hackers at one end, and ‘Script Kiddies’ or ‘Script Weenies’, inexperienced hackers who use automated programs to break into computers, at the other. Top tier hackers usually have a sort of ‘code of honour’. This code tends to make them ‘look-see’ hackers, that is, hackers who ‘look’ to see rather than to sell or to do purposeful damage.

While it is difficult to pinpoint a ‘profile of hacker’ it is possible to detail common themes among types of hackers, in this case among elite hackers. These themes were observed as part of the two years of research for the book ‘Underground,’ including a number of interviews with a number of hackers themselves. These include:

- In general, they are very bright or gifted.
- Their ages at the time of the most frantic and sophisticated hacking were usually between 16 and 24.
- They all admitted that they never quite fit at school or university. This might say more about the education system than the individuals themselves. In almost all cases, they had moved far beyond anything that school or university could teach them about computers in particular fields. Often they described feeling alienated by teachers, whom, it would appear, were ill-equipped to deal with gifted children.
- Most were also introverted, anti-social perhaps even awkward. They usually came from less than picture perfect family backgrounds. Their families were often dysfunctional, in some cases with one parent missing, through divorce or death.
- An anti-establishment view is a key factor for the top hackers. They want to rebel against symbols of authority, such as banks, government agencies and what President Eisenhower called the ‘Military Industrial Complex.’
- They would often describe themselves as being addicted to or obsessed with being on-line, often spending up to 40 straight hours hacking.
- They said they were often driven by the adrenalin rush of being somewhere they were not supposed to be.
- More experienced hackers visit a system numerous times, while less experienced hackers tend to use a system as a one-hit adventure.

- They have tended to experience periods of mental illness or emotional breakdown, particularly immediately after being raided by police. This would seem to be related to being denied access to their gear (computers, modems etc). In some cases, they subsequently moved into drug addiction, perhaps substituting drugs for hacking. This tended to be followed by some sort of mental or emotional breakdown.
- They tend to 'outgrow' hacking.

This is not suggest that all hackers are benign - clearly that is not the case. Some hackers are malicious, most are a nuisance. Leaving a computer system which is not secured attached to any network - particularly the Internet - carries a degree of risk. Clearly, prevention is better than cure. However, at this time, it appears that most hackers, particularly those in the elite category, are not the international saboteurs or professional information warriors presented so frequently in the media. Importantly, based on anecdotal evidence, there appears to be a link between hacking, particularly at the highly skilled end of the spectrum, and mental illness, addiction or obsession, and this link deserves more in-depth study.

Hackers even have a "Code of Ethics", formulated in 1984 by Steven Levy in his book "Hackers: Heroes of the Computer Revolution". The ethics state in summary that:

- Access to computers should be unlimited and total.
- All information should be free.
- Mistrust authority - promote decentralization.
- Hackers should be judged by their hacking not bogus criteria such as degrees, age, race, or position.
- You create art and beauty on a computer.
- Computers can change your life for the better (Levy, 1984).

3.2. Viruses and related unpleasantness

A virus is any program that contains malicious code, and replicates itself by inserting copies of itself into other programs. It infects the host programs by substituting its code for some other code, or overriding instructions, causing the system to perform unwanted tasks. This could be deleting files, destroying the operating system, damaging documents, corrupting or changing important data, or sending out bogus e-mails under your name. A truly malicious virus will not only wipe out the data in a system, but also wipe out any back-up copies. In some cases, the virus is also programmed to infect the back-up program. It will attach itself to the back-up program and execute a delete to the back-up data when there is an attempt to restore any previously deleted data to the system. The only real purpose of a virus is to cause damage, and to be able to spread the damage to as many systems as possible (Harden, 2000).

Almost as damaging as a virus is a virus hoax. A number of virus hoaxes have occurred in recent years that were just as debilitating to organizations as a real virus. What happens in the hoax is that some new non-existent and dangerous virus is announced, typically via e-mail, with some kind of message that says "Please pass this on to others in your organization," or something to that effect. Well-meaning employees, colleagues, and friends, who think they are doing something good, blast the message out to as many people as they can to warn them to protect themselves from this dangerous virus. Soon, the phony virus message is accepted as real, and people begin to react. Perhaps they shut down their systems, or run special anti-virus programs, or stop sending e-mails. Some very large corporations, hit with virus hoaxes that were soon spread by trusted employees, actually took their mail servers and other systems off-line as a precaution against the so-called virus. Even the news media has picked up on some hoaxes and reported them as real viruses.

Trojan Horses (or Trojans) are programs that outwardly appear to be useful and legitimate programs, but contain additional hidden code from a hacker. The additional code may allow the hacker to gain access to the system, exploit various software/system functions, destroy data, release viruses, or perform any function that the hacker intended. Trojan Horses are particularly nefarious since they can impersonate an innocent

program. Employees can download games and screen savers from the Internet that contain these Trojans, yet appear to function properly and show no signs of the hidden code that lurks within. A Trojan Horse program might be embedded within a shareware program that appears to be a wonderful utility program, so copies of it are disseminated from employee to employee or from one organization to another, spreading the hidden code from system to system along the way. Trojan Horses can also be picked up from unfamiliar web sites. Most of us are unaware that when we visit a web site, it visits us in return. Typically, the web site may implant a cookie in our system's cookie file. This is usually a harmless practice that helps the web site understand our browsing preferences. But the "cookie" might also be a Trojan Horse with other, more malicious intentions. It is often best to refrain from visiting questionable web sites (CERT, 1999).

A **worm** is a self-contained program (or set of programs), that is able to spread functional copies of itself to other computer systems (usually via a network). **Host-computer worms** are entirely contained on their host computer. Host-computer worms that delete from one host upon propagation to a new host are called **rabbits** - they 'hop' around a network. Some worms run in multiple parts on many hosts. These worms are called **network worms**. A network worm with one coordinating segment and many client sub-segments is termed an **octopus!** Note: malicious code is called a worm when it requires no specific action on the part of the user to enable infection and propagation. It just spreads. If the code requires the user to open an email or load a screen saver or take some other action, then it is called a virus (Kerby, 2001).

It is interesting to note that of the 60,000 or so known viruses, worms etc., about 55,000 of them are Microsoft-specific. Care is needed here because this statistic does not mean that systems such as Linux, Unix or Mac are immune - there are just less examples found here. We usually think of infection via the network and floppy disks, but CDROMs are notorious for hosting malware.

3.3. *Computer- Assisted Crime*

Any illegal act for which knowledge of computer technology is used to commit the offense (ACFE, 1999). There are many narrower definitions of specific types and varieties of computer crime under numerous statutes and case law: computer fraud, computer-assisted crime and information crime. The newest addition is internet (or cyber) crime. **Computer fraud**, for example, is an act in which the offender knowingly accesses or otherwise uses a computer without authorization or exceeding authorization, with intent to commit a fraudulent act or other criminal act. In a computer crime, the computer itself can be either

- the object - computers and network systems themselves as the object or target of crime (for example, physical theft, damage, destruction of information) OR
- the subject - the computer is the environment within which the crime is committed, (for example, virus attacks), OR
- the tool - computers used as the means to commit a crime, (for example, embezzlement, theft of information, hacking), OR
- a symbol - computers used to lend frauds credibility, (for example, elaborately computerized investment schemes).

An interesting website to read about computer-assisted crime is the Security News Portal [<http://www.securitynewsportal.com/>], which has day-to-day news on the latest stories, including last Thursday's hacking into BrassEagle Inc. website by a hacker who then disseminated inaccurate information about the company's financial dealings, causing a stop of trading at Nasdaq.

The July 2001 report by the US Computer Security Institute Controller states that the cost of computer security breaches now averages more \$ 2 million per affected company per year, This report, which explores the cost of computer crime at 538 large companies and government agencies, reveals that 85% of respondents detected security breaches in the prior 12 months (CSI, 2001)

In Australia, the increasing dependence of business on computer systems has made many more organisations vulnerable to the impact of computer crime. Indeed, more companies are worried about the risk of computer crime than they are about product liability, fraud and theft. Without more effective mechanisms for controlling this abuse we can expect it to increase significantly with the rise in computer use over the next decade. Australian companies remain most vulnerable to computer misuse from their own

employees, contractors, consultants, or anyone else with knowledge of and access to their computer systems. In a survey carried out in 1998 by the Australian Federal Police, 54% of respondents either had suffered from some form of unauthorised use or were unaware whether they had a problem. This is consistent with overseas trends – eg. the US figure for 'Yes' is about 42% . Nearly 90% of those that has a problem were able to trace to people who had legitimate access to their systems. 60% identified the source as external to their organisation (meaning that there was a significant group who had experienced both internal and external attacks). These figs are also on par with similar surveys in UK, US and Europe (Wahlert, 1998).

Wahlert's report mentions the following as the major trends in Australian computer-assisted crime: counterfeiting (identity, currency and plastic payment cards), pornography, gambling (Australia lately passed a law against internet-based gambling), gathering of tactical intelligence, cyber scams and information warfare.

For law enforcement the potential for a rise in external computer attacks, compared to insider abuse, is more worrying. One reason is the anonymous and borderless nature of crime in cyberspace and the associated intelligence, jurisdictional and evidentiary problems that this creates. Another key issue for law enforcement may be the further internationalisation and sophistication of criminal activity utilising powerful computer networks. Additionally, transnational criminal organisations may develop the capability to inflict damage on these systems and disrupt specific components of Australia's national information infrastructure, especially those that have a high level of technology dependence.

Evidence collection is probably one of the most challenging issues facing criminal computer prosecution. All computer crimes cause special problems due to the nature of the files themselves. Computer files are easily erased, moved, or tampered with, and that makes using them as evidence very difficult. Computer forensics is a rapidly expanding field, with all Australian police computer crime units reporting this aspect of their business growing at a dramatic rate. However, it has also proved a steadily growing impediment to the prosecution of even the simplest of criminal cases. Largely inexperienced investigators find the complex technology and operational difficulties of obtaining computer records as evidence a complicated and convoluted subject; and equally inexperienced courts find the presentation of such evidence fraught with potential challenges to its verity. This is already evident in financial investigations: high speed, world wide computer funds transfers are a facet of emerging cyberpayment technologies that add complexity to law enforcement's ability to trace criminal activity and recover illicit proceeds. Additionally, computer hackers use program code to instruct the software they use to erase itself after an illegal transfer of funds has been effected, eliminating any evidence of the transfer. The use of such programming code makes it almost impossible for law enforcement to track money moved electronically. The Australian Securities Commission has identified the main problem for them in investigating allegations of stock manipulation and fraud over the Internet as evidentiary - 'getting useable and meaningful evidence. Investigators admit that they are only catching 'the bottom of the food chain' in relation to computer crime: the well funded, structured, informed and experienced attacker is likely to go undetected and, therefore, operates with impunity. Part of the reason for this is the absence of a 'smoking gun' in computer investigations. The professional computer attacker leaves no traces - 'audit records are removed or altered, access times on files modified, no damage performed against the data itself; no traces, and therefore no evidence of a crime.'

Court challenges concerning the integrity and authenticity of electronic evidence have increased noticeably in the past two years. This may be the result of persons charged being more computer literate or possessing technical skills; counsel for accused persons having gained computer expertise; more legal precedents having been established; and the laws not having kept pace with technological developments. It will be incumbent on law enforcement agencies to devise generally accepted practices, procedures, and principles for the collection and presentation of computer evidence. The failure to develop standards could result in the courts imposing their own rules that may not prove popular among investigators.

Cyberspace is still in the early stages of its development but it is already transforming our world. Over the next decade, the emerging telecommunications, computing and media enabling technologies will affect almost every aspect of our lives. Crime will be no exception. Crime in cyberspace is likely to become more prevalent over the next five years. This is because of a lack of general understanding as to the value of security safeguards; a lack of knowledge as to how to cope with the continual emergence of new security 'holes'; the absence of reliable quantitative data to illustrate the nature and extent of crime in cyberspace; the increasing commercialisation of cyberspace; and differences in national policies, laws and practices

regarding security resulting in difficulties for law enforcement at an international level. It is also possible that cyberspace attacks will result in a blurring of responsibilities between law enforcement, national security and defense interests, necessitating an enhanced level of liaison and cooperation. The increasing level of use of, and reliance on computers and computer networks is clearly creating new challenges for Australian law enforcement agencies. It is a mistake, however, to believe that these problems are insurmountable. Through a process of education and coordination - at both the domestic and international levels - and through regular reviews and updates of our laws and police procedures, law enforcement can keep pace with technological advances. The key is in accepting that these new technologies are drivers of change. Only by the adoption of a strategic approach to change management in law enforcement, and preparing for the future, will we all be able to enjoy the benefits of living in the information age without leaving us unnecessarily vulnerable to high-tech criminals.

4. Recommendations

4.1. How does this affect the legal firm environment?

Legal firms, like any other services bodies, maintain a large collection of customer information. However, in a legal setting, this information must be kept much more secure than in any other (apart from medical) setting, due to the huge liability for breaching client confidentiality and the possibility of losing business if competitors obtained inside information on current cases.

And yet lawyers, who are becoming more and more technologised, are also one of the most technologically unaware groups of professionals. A simple example will suffice to illustrate. At South Brisbane Community legal Service, where E-Cognus was managing an IS project last June, one of the senior solicitors opened an attachment to her email. The result was that the whole Service was infected with the w32.magistr.24876@mm⁵ virus. The virus is particularly lethal in legal settings, as it looks on the computer for legal terminology on the hard drive, then once it finds it, it picks eight lines from any Word document and emails it to everyone on the Outlook address book. It has its own emailing server, so that Outlook doesn't even have to be open. Since the Service had a permanent Internet connection, other lawyers - many of whom used to be associated with the Service - started receiving infected attachments, which they then opened, thus spreading the virus further. I was sent an infected attachment two weeks later, and alerted the so far totally unaware service of their predicament. Unfortunately, by that time, the Dept. of Immigration staff, who received infected attachments from the Service, have also managed to become infected. As result, we had a self-imposed Denial-of-Service for a week, three computers had to be reformatted, and the time lost and inconvenience to everybody was very high.

Adams (2001) details ways in which information security may be violated in a legal firm. Apart from the usual problems with easy to remember passwords (therefore easy to code-break), he also states such incidents as stolen laptops, email risks and being cracked into through using the internet. Yevics (2001) laments the state of investment in IT security among the legal profession in the US, and gives seven points with which a firm should start its Information Security Policy. Among others, she again mentions taking passwords seriously, as well as mentioning backups.

Law firms are significant targets for the theft of information. The threat and the vulnerability level are high in this industry. Information on clients and case strategy stored on computer systems transmitted to attorneys in varying geographically situated offices as well as to clients. Another issue is that of the increasing number of cases involving cyber crimes. As access to client information has opened up dramatically in recent years, the difficulty of keeping that information private has kept pace. Accidental disclosure is easier and more common. Legal communications are easier to intercept and networks are more vulnerable to intrusion and disruptive vandalism. In addition to these technical challenges, the culture in many law firms makes managing information security a complex and lonely undertaking.

4.2. Best Tools of the Trade

For any person responsible for maintaining the information security at a firm, the first task will be to do some data gathering to find out what types of security policies, processes, and procedures currently exist at the company (if any), and to set up one-on-one interviews with each member of your staff, as well as each of

your management team peers (Vigilix, 2001). During these interviews, aside from finding out what security resources currently exist, one should find out what the history of information security has been at the company. Have there been security breaches in the past? If so, what was the prior reconciliation process and the final outcome? Was law enforcement involved? Were any employees terminated? Were lawsuits initiated? Systems that have been compromised before, will most likely be areas carefully watched by your management peers. It will be important to make sure prior security compromises do not get repeated.

Important questions to ask everyone you interview will be:

- What security disasters are waiting to occur?
- What does your company do well as far as security goes?
- Who are the key employees that currently have the best understanding of the current security posture of your company?
- Who are the security advocates inside your organization? (You need the security advocates on your team, and it will be important to keep these folks informed of your findings and future recommendations.)
- Who are the security "naysayers"? Many organizations have factions of security "naysayers" who find every reason in the book not to implement security. (These folks will need special attention if you don't want them to undermine your recommendations.)

The next important step is to understand the immediate security liabilities. Where is the company currently vulnerable? Each vulnerability has to be categorized according to the potential impact it could have on your organization, such as:

- High risk
- Moderate risk
- Low risk

In categorizing risk levels, some of the things to consider are contractual agreements with customers, currently stated privacy notice, and the existence of any life threatening, or financially susceptible transactions.

Typically, the kinds of applications that mandate at least some level of security inspection are:

- Messaging
- Corporate General Ledger
- Human Resource Files
- Customer databases

The network hardware devices that require security inspection are all the hardware platforms that these applications exist on, as well as the corporate routers, gateways, firewalls, VPNs, and authentication systems. If there are no firewalls, VPNs, or authentication systems, there is a need to identify whether there is a need to develop and implement these specialized security systems.

Then an information Security IT agenda should be drafted, and ultimately an overall security project plan. In identifying vulnerabilities, it is wise to have an outside auditing firm perform an objective online security penetration test. An online penetration test will be one of the items you will want to put at the top of your Security IT Agenda.

Any consulting service that does not test for at least 500 vulnerabilities should probably not be considered for an outsourced information security audit. Today, most penetration testing services that truly know what they are doing test for approximately 600-1000 types of online vulnerabilities. Make sure that the penetration

service will include as part of their service, the hand-off of a Vulnerability Assessment Report. The report should assign risk levels to all vulnerabilities reported, and include recommendations on how each one is typically fixed. Have your own staff fix as many of the vulnerabilities as possible, and consider hiring an outside consultant to resolve the vulnerabilities that your team is not able to resolve themselves (Duffy, 2000).

One critical area of security that is probably most ignored by security managers is the review of documented processes and procedures. Auditing processes and procedures can only be performed through human analysis. None of the shortcomings of security checks in processes and procedures will be picked up by an online penetration test. The reason that the review of security processes and procedures is important is because it is sound processes and procedures that will help maintain on-going security moving forward. A penetration test is simply a snap-shot of your security posture at a moment in time.

Because vendors are concerned with getting their software to customers as quickly as possible, they sometimes sacrifice security.

Processes and procedures that typically need review are processes for changing passwords on mission critical systems, ACL changes on the routers, firewall rule-set changes, procedures for configuration of secure remote access accounts, secure remote access user instructions, and general overall change-management procedures. Maintaining security is an on-going process, and just when one thinks the network is locked down and secure, there will be some new area of concern that will require attention.

4.3. Educating the Masses

Policies, processes and procedures are great tools only if they are actually used by the people who are on the front line of attack. No amount of security software, firewalls, intrusion detection packages and event log analysis will prevent a disaster from striking at a firm's information systems if the staff using these resources is not made aware of the impact their actions may have on the whole system.

Examples of issues staff should be made aware of are:

- sharing access on NT servers (by default, the permission is given to "everyone" in a particular group);
- emailing attachments to people, thus creating multiple copies of a file and increasing the risk of its getting into the wrong hands;
- handling old electronic storage media such as floppies, CDs and Zip Diskettes
- securing old data on a PC that is changing users within the firm
- not emptying recycling bins on the PC
- file and print sharing (uses open ports, allowing access into the system)
- using messaging services which allow file transfers
- opening of unscanned email attachments
- lack of updating the anti-virus software, or lack of knowledge how to configure it properly
- being reckless about protecting the privacy of one's passwords
- not encrypting data

Security should be a primary concern for offices of any size. Security should be a primary concern for anyone who owns a computer. The uninformed user is an insecure user - there are any number of items that can decrease security to users who do not know any better. The best defense against an attack is a good offense. If you understand that the person attacking your system is not necessarily a competitor, but can be a disgruntled employee, someone across the ocean who is just looking for an open system in which to plant a worm, then you have made a crucial stride in protecting your network. While it is hard to protect against the unknown, there are preventive steps you can take. The most arrogant error one can make is to assume that somebody cares about what you are doing before they will cause trouble. Just as car thieves do not care who they are stealing the car from, information thieves do not care where the information comes from. If trouble can be caused, it is better to assume that it will be caused on your system. Call it Murphy's hackers addendum, but its better to worry and be safe - than to be caught without the proper protection.

The selection of portable (laptops and WAPs) computing protection strategies must be clearly communicated to portable computer users by means of a thorough user education process. Education should be mandatory and recurring to assure the most current procedures, tools, and information are provided to portable users. In the area of remote access to on-site company resources, such contact should be initiated when remote users register in the remote access authentication system. For the use of shared company portable computers, this should be incorporated with the computer check-out process; portable computer user procedures can be distributed when systems are checked out and agreed to by prospective users. With respect to the use of noncompany computers in a portable mode, the best method of accountability is a general user notice that security guidelines apply to this mode of computing. This notification could be referenced in an employee nondisclosure agreement, in which employees are notified of their responsibility to protect company data, on-site or off-site. In addition to registering all portable users, there should be a process to revalidate users in order to maintain their authorized use of portable computing resources on a regular basis. The registration process and procedures should be part of overall user education on the risks of portable computing, protection mechanisms, and user responsibilities for supporting these procedures (Maier, 2001).

5. Appendix – electronic references to acts and regulations mentioned in the report

- ¹[http://www.pwcrecovery.com/pwcrecovery/site.nsf/54f8a9f77856e17e4a2568b7002793ca/5a940d36a3c867e1ca2569e700008a0a/\\$FILE/Privacy%20Amendment%20\(Public%20Sector\)%20Act%202000.pdf](http://www.pwcrecovery.com/pwcrecovery/site.nsf/54f8a9f77856e17e4a2568b7002793ca/5a940d36a3c867e1ca2569e700008a0a/$FILE/Privacy%20Amendment%20(Public%20Sector)%20Act%202000.pdf)
- ² <http://www.oznetlaw.net.au/pdf/files/p0627376.pdf>
- ³ <http://www.hmso.gov.uk/acts/acts1998/19980029.htm>
- ⁴ <http://www.fas.org/sgp/congress/2000/h062200.html> and <http://www.ombwatch.org/info/2000/HR4246.html>
- ⁵ <http://www.symantec.com/avcenter/venc/data/w32.magistr.24876@mm.html>

6. References

1. Adams, J. (2001). Information Security and the Law Practice. [Online] Available WWW: <http://www.msba.org/departments/loma/articles/techstuff/infosecurity.htm>
2. Association of Certified Fraud Examiners. (1999). *Fundamentals of Computer Fraud*. Austin, TX: ACFE.
3. Australian Federal Police (2000). *The Virtual Horizon: Meeting the law enforcement challenges. Developing an Australasian law enforcement strategy for dealing with electronic crime. Scoping Paper*. Police Commissioners' Conference Electronic Crime Working Party, Canberra.
4. CERT (1999). CERT® Advisory CA-1999-02 Trojan Horses. [Online] Available WWW: <http://www.cert.org/advisories/CA-1999-02.html>
5. Chantler, N. (1998). Electronic Security. Paper presented at the Internet Crime Conference, Melbourne.
6. Colhoun, D. (1998). Information Technology Security Policy, February 1998. [Online] Available WWW: <http://www.caudit.edu.au/caudit/information/public/download/colhoun.html>
7. CSI (2001) Computer Crime and Security Survey. San Francisco, CA.
8. Cypherwar (1999). Government Information Security Act. [Online] Available WWW: <http://cipherwar.com/news/99/s1993.htm>
9. Daerne, K. (2001). Cybercrime Bill 'excessive'. In *The Australian*, July 24.
10. Deloitte Touche Tohmatsu & Victoria Police (1999). *Computer Crime & Security Survey*, Deloitte Touche Tohmatsu & Victoria Police, Melbourne.
11. Dreyfus, S. (1998) Computer Hackers: Juvenile Delinquents or International Saboteurs? Paper presented at the Internet Crime Conference, Melbourne.
12. Duffy, D. (2000) Testing Your Defenses. [Online] Available WWW: <http://www.darwinmag.com/read/120100/defenses.html>
13. Electronic Frontiers of Australia (2001) CyberCrime Bill 2001. [Online] Available WWW: <http://www.efa.org.au/Campaigns/cybercrime.html>
14. Fisher P. (2001). "Operations Security and Controls". In Krause, M. & Tipton, H (eds.): **Handbook of Information Security Management**, CRC Press, NY.
15. Greenleaf, G. (2001) Private Sector Privacy: Problems of Interpretation. [Online]. Available WWW: <http://austlii.edu.au/~graham/CyberLRes/2001/3/>
16. Harden, M. (2000). "Tools of the Trade". In **Information Security: A Guide to Protecting Your Information and Computer Systems from Hackers**. CyberGuardian, McLean (VA)

17. Jiggins, S. (2000). Commissioners' Conference wires up to short circuit electronic crime. In *Platypus*. [Online] Available WWW: <http://www.afp.gov.au/raw/Publications/Platypus/Jun00/cccrime.htm>
18. Kantei [Official Residence of the Prime Minister of Japan] (2001). Policy Initiative: IT Policies. E-Japan Priority Policy Program. Chapter VI: *Ensuring of Security and Reliability over Advanced Information and Telecommunications Networks* [Online] Available WWW: <http://www.kantei.go.jp/foreign/it/network/priority-all/7.html>
19. Kerby, F. (2001). Malicious Software (Malware). SANS Security Essentials Training Manual.
20. Labihan, R. (2001) Australian Cybercrime Bill "overpowers" inquiry. In *Zdnet Australia*. [Online] Available WWW: <http://www.zdnet.com.au/news/breakingnews/story/0,2000020826,20256107,00.htm>
21. Levy, S. (1984) *Hackers: Heroes of the Computer Revolution*. Penguin USA: Garden City, NY.
22. Maier, P. (2001) "Protecting the Portable Computing Environment". In Krause, M. & Tipton, H (eds.): **Handbook of Information Security Management**, CRC Press, NY.
23. Mitchell, S. & Charney, S. (2001). "Federal and State Computer Crime Laws". In Krause, M. & Tipton, H (eds.): **Handbook of Information Security Management**, CRC Press, NY.
24. Office of Strategic Crime Assessments (OSCA) & Victoria Police (1997). *Computer Crime and Security Survey*, OSCA / Victoria Police, Melbourne.
25. Patrick, J. (1998). Personal Statement on The Development of Information Systems at Sydney University [Online] Available WWW: http://www.cs.usyd.edu.au/~jonpat/Information_Systems/IS_propaganda/future_of_IS_at_Sydney.html
26. Poysti, T. (2000) Information Security Commentary. [Online] Available WWW: http://www.urova.fi/home/oiffi/enlist/commentary/information_security.html
27. Rabiette, A. (2001) Developing an Information Security Policy. [Online] Available WWW: http://www.jisc.ac.uk/pub01/security_policy.html
28. Vigilinx (2001) Security Assessment Methodology: A White Paper. [Online] Available WWW: http://www.vigilinx.com/pdf/50722_White_Paper-SAM.pdf
29. Wahlert, G. (1998) *Crime in Cyberspace: Trends in Computer Crime in Australia*. Australian Institute of Criminology, Melbourne
30. Withers, S. (2001) Australia not ready for privacy. In *Zdnet Australia*. [Online] Available WWW: <http://www.zdnet.com.au/biztech/security/story/0,2000010455,20254963,00.htm>
31. Yavics, P. (2001). Security for Computers, Information and Technology. [Online] Available WWW: <http://www.msba.org/departments/loma/articles/techstuff/security.htm>