Global Information Assurance Certification Paper

IT Security: Legal Issues in Australia

By Catherine Edis
3 February 2004

SANS GIAC GSEC Practical Assignment Version 1.4b
Option 1

Abstract

There are a number of legal issues specific to Australia that could potentially impact an organisation's IT security program and practices. Some laws are limited to specific types of organisations (eg, financial institutions or health service providers) and/or types of information (eg, financial or medical records). However, a number of laws have more general application, with the potential to impact most, if not all, organisations that manage their own IT infrastructure.

This paper discusses the Australian laws most likely to impact the IT security program and practices of most organisations. These include:

- a director's duty to exercise care and due diligence,
- privacy laws,
- laws relating to the monitoring of computer and network use, and
- criminal offences for compromising the security of computers or networks.

Staff responsible for IT security in Australian organisations need to be aware of these laws when developing and implementing an IT security program.

Note: This paper is a summary of the author's interpretation of some Australian laws relevant to IT security. It has been developed for the purposes of assessment in the SANS GIAC GSEC course and is not intended as legal advice. Readers are advised not to rely on the information contained in this paper, but rather to consult suitably qualified legal professionals.

Due Diligence

Over the last few years, the global economy has become increasingly reliant on e-Commerce and the Internet. Similarly, the public sector and the military are much more dependent on IT infrastructure than they were a decade or so ago. With this increased reliance, it is now becoming clear that company boards and senior management must focus on IT security as part of responsible risk management and governance (Jones, 2002).

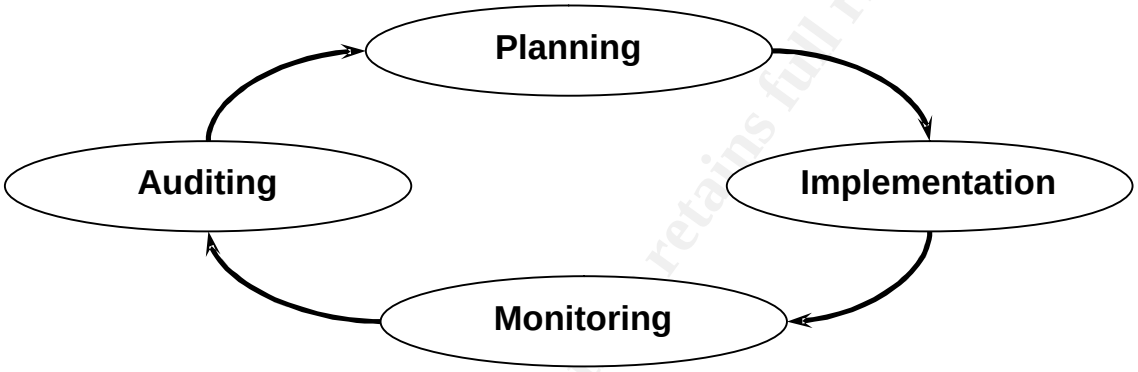
However, having an appropriate IT security program in place is not just "good management". In Australia, directors and other officers of incorporated companies have a legal obligation under the Commonwealth Corporations Act 2001, s180(1) to discharge their duties with a reasonable degree of "care and due diligence". Subsequent case law (Vrisakis, 1993) suggests that "[i]f there is a foreseeable risk of loss to the company resulting from an IT security breach, and the benefit likely to be gained from not adequately addressing that risk is low, then a director who does not adequately address that risk does not act with the requisite care and diligence" (Gadens, 2001).

The principle underlying Australian Law in relation to IT security is that organisations must take reasonable steps to protect the security of their computers and data. Note

that what is considered “reasonable steps” is proportionate to the type of organisation, the nature of the risk, and current IT security challenges and best practices (Hourigan, 2002).

In this context, the question is not so much whether specific technologies or products have been implemented, but rather the extent to which appropriate processes are in place to manage IT security (National Office for the Information Economy, 2002).

For example, Hourigan (2002) suggests that an organisation’s IT security program should include a cycle of activity comprising the following phases:



In order to be considered “reasonable steps”, Hourigan suggests the phases should include the following activities, at a minimum:

Auditing, Risk Assessment and Analysis

This phase should include identification of

- critical/non-critical systems and assets on the network,
- critical vulnerabilities, and
- business operations at risk.

This phase involves the use of structured risk management methodologies. Outcomes from the auditing phase should feed into the subsequent “planning” phase.

Planning

This phase includes development of:

- security policies, standards, etc;
- technical security designs for applications, networks, infrastructure
- incident response/continuity plans

Typically, the particular issues for which policies are needed would be identified as part of the auditing phase. For example, as part of the auditing phase, the

organisation might identify vicarious liability for inappropriate use by employees as a significant risk. This could apply in relation to employee activities that may compromise IT security, as well as more general issues such as copyright infringement.

In the subsequent planning phase, the organisation could develop or modify their "Acceptable Use" policy so that it clearly states the type of activity that is and is not acceptable (and therefore authorised). Ideally, employees and other users should be required to declare in writing that they will abide by the Acceptable Use Policy before commencing employment or before receiving access to IT facilities. This process would help to educate users on their rights and responsibilities and protect the organisation from the vicarious liability risk.

Implementation

This phase includes:

- Product and custom solutions
- Configuration management
- Timely application of patches
- Authentication, access controls etc

Monitoring

This phase comprises activities such as:

- Changes to network configuration
- Compliance with policies
- Detecting and dealing with system misuse

If a director fails in their duty to exercise a reasonable degree of care and due diligence in relation to IT security, then, under the Corporations Act 2001, s1317E he or she may be personally liable for a civil penalty of up to AUD$200,000 and compensation for any loss suffered by the company. As well as the threat of loss to the company, this potential personal exposure should help motivate directors to focus attention on developing, implementing and maintaining an appropriate IT security program.

Privacy

If an organisation's IT security program is lacking, the confidentially of some information is at risk of compromise. Information of particular sensitivity includes personal details (name, residential address, etc), financial records, and health and medical records. In Australia, there are several laws that impose obligations on organisations to maintain the confidentiality of this type of information. If appropriate measures are not taken to protect confidentiality, the organisation is at risk of breaching these laws.

There is no general common law right to privacy in Australia (Oz Netlaw, 2002). The laws of contract, tort and confidential information impose some obligations in limited

circumstances. However, Federal and State legislation imposes obligations on most organisations to protect the privacy of personal information collected from individuals.

All Commonwealth and Australian Capital Territory government departments and agencies must comply with the Commonwealth Privacy Act 1988, and the associated Information Privacy Principles (IPPs). The IPPs define a set of minimum privacy standards. Under the same Act, private sector organisations with an annual turnover of more than AUD$3 million, and all health service providers, must comply with the National Privacy Principles (NPPs). The IPPs and NPPs deal with similar issues: the collection, use, alteration, disclosure, storage and security of personal information.

Under Information Privacy Principle 4, an organisation must ensure that personal information is "protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorized access, use, modification or disclosure, and against other misuse". Similarly, National Privacy Principle 4 states that "an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure". Essentially, both principles require organisations to take reasonable steps to protect the security of the information.

Hourigan (2002) suggests that, when determining what constitutes "reasonable steps" in the context of privacy, organisations should consider:

- the sensitivity of the personal information,
- the harm likely to be suffered by the individual to whom it relates,
- how the organisation stores or holds the information,
- the size of the organisation, and
- that the steps should be proportional to the risks faced by the organisation.

Most state and territory government departments and agencies, except in Western Australia, are subject to similar privacy standards as their Commonwealth counterparts. They are subject to the following state privacy laws or administrative directives. These laws and directives complement the federal privacy legislation, adopting the wording from either the federal Information Privacy Principles or the National Privacy Principles.

New South Wales	Privacy and Personal Information Protection Act 1998 Information Protection Principles
Northern Territory	Information Act 2002
Queensland	Privacy Scheme Information Privacy Principles (Qld)
South Australia	Information Privacy Principles Instruction Information Privacy Principles (SA)

Tasmania	Privacy legislation for the public sector is currently in development Information Privacy Principles (Tas)
Victoria	Information Privacy Act 2000 Information Privacy Principles (Vic)

Public and private organisations that hold health records in Victoria, the Australian Capital Territory, and (from 1 March 2004) New South Wales, are subject to legislation that extends privacy protection to those health records. (More detailed information regarding these laws can be found on the Office of the Federal Privacy Commissioner's web site at: http://www.privacy.gov.au/privacy_rights/laws/index.html)

Privacy and Incident Handling

When handling IT security incidents, an organisation may be asked to, or may wish to, disclose an individual's personal details to a third party. This third party is typically the alleged victim or law enforcement. The Information Privacy Principles and the National Privacy Principles allow organisations to this only in limited circumstances.

Under Information Privacy Principle 11 and National Privacy Principle 2, an organisation may disclose personal information to another party if there is a reasonable belief that a person's life or health is at risk, it is required by law, it is necessary to enforce the criminal law or a law imposing a fine, or it is necessary to protect the public revenue. National Privacy Principle 2 also allows disclosure if the organisation has reason to suspect unlawful activity or improper conduct, and the disclosure is necessary for prevention or investigation of the activity. In some circumstances, organisations are required to document the disclosure.

Other legislation also places limits on the information that can be disclosed when dealing with an IT security incident. The Commonwealth Telecommunications Act 1997 applies to organisations that "supply services for carrying communications to the public", including internet service providers (ISPs). Other organisations that manage their own network infrastructure (eg, most Australian universities), may also be subject to the Act. This will depend on the extent to which the organisation manages its own telecommunications infrastructure, the network design, and the extent to which they provide internet access to the general public. Under the Act, these organisations are obliged to protect the confidentiality of information carried over their network, where it relates to:

- the content or substance of the communication,
- the carriage services supplied, or in tended to be supplied, by the organisation, or
- the affairs or personal particulars of another person.

Use or disclosure of the above categories of information is not allowed, except in some limited circumstances.

Organisations must not allow access to the content of an Internet communication "in transit" except in response to a warrant under the Telecommunications (Interception)

Act 1979. Note that “content” does not include the network/traffic related data required to transmit the communication through the network (Internet Industry Association Fact Sheet).

The other categories of information listed above can be used or disclosed in response to legal warrants, court process, or requests made by law enforcement agencies under the Telecommunications Act.

Note that under section 313 of the Act, an organisation is not liable for damages for anything it did, or did not do, in good faith while assisting law enforcement agencies.

Network and Computer Monitoring in the Workplace

Some organisations may wish to monitor employees’, and other users’, use of IT facilities. This is typically undertaken to reduce the risk of security breaches or other improper use.

Australian federal telecommunications legislation places limits on the monitoring that some organisations can legally undertake on its network. As mentioned above, the Telecommunications Act 1997 and Telecommunications (Interception) Act 1979 apply to “organisations who supply services for carrying communications to the public”, including internet service providers (ISPs). ISPs must not intercept a communication while it is passing over a telecommunications system unless the originator of the communication has consented to the interception (Oz Netlaw, 2001).

Note that the risk of potentially illegal monitoring may be mitigated to some extent by requiring users to provide written acknowledgment and acceptance of policies, which state that the organisation may monitor email and internet use. This may constitute “consent” under the Acts.

The legislation allows interception in some limited exceptions, relating primarily to interception performed for the purposes of maintaining the equipment or network, or for certain law enforcement purposes. The latter requires either a valid warrant or the involvement of the Australian Security Intelligence Organisation’s (ASIO), National Crime Authority, Australian Federal Police, or state police. Different conditions apply depending on the terms of the warrant or nature of the investigation. (Further details are available in the Oz NetLaw Telecommunications Fact Sheet at: http://www.oznetlaw.net/facts.asp?action=content&categoryid=238) Note that information obtained in breach of the Acts cannot be used as evidence in legal proceedings.

The Office of the Federal Privacy Commissioner has released “Guidelines on Workplace E-mail, Web Browsing and Privacy” (see http://www.privacy.gov.au/internet/email/index.html). The guidelines clarify the circumstances in which monitoring use of computers in the workplace is acceptable under Australian privacy law, and are relevant to both public and private sector organisations.

Essentially, the guidelines explain that an organisation is legally responsible for the computer systems and networks it operates. It therefore has the right to make directions regarding their use and to monitor use to ensure it complies with those directions. However, the organisation must take appropriate measures to ensure employees and other users are aware of the directions and the nature and extent of the monitoring.

The Office of the Federal Privacy Commissioner advises that, in order to comply with the guidelines and other Australian privacy laws, organisations should have a policy that explicitly states:

- what is proper and permitted use of the network,
- users' obligations in respect to IT security,
- how the organisation will monitor compliance,
- what information is logged,
- how that information will be used, and
- who can access the logs and content of staff e-mail and browsing activities.

This policy may form part of the IT acceptable use policy or a separate privacy policy dealing with e-mail and Internet use. One potential approach is to include a statement of the principles regarding acceptable use and monitoring in the "IT Acceptable Use Policy". This could be complemented by two sets of guidelines for use of email and the internet, which explain the application of the policy specifically in these contexts. The guidelines can be more "conversational" in tone and explain the application of the policy to common examples of use that are or are not acceptable.

The organisation must also take reasonable steps to ensure all staff and users are aware of the policy. This can include:

- reference to the policy in staff appointment and induction processes,
- requiring staff to declare and sign off on having seen the policy as part of the processes for appointment or receiving access to the network,
- discussion of the policy in relevant internal training courses,
- reference to the policy in on-screen messages at a user's first login (or every login),
- regular reminder emails to all users (eg, every 6 months), and
- reminders in staff newsletters or other internal publications.

The key point to note is that having appropriate IT security policies is necessary, but not sufficient, to comply with Australian privacy laws. The organisation must make users aware of the policies, regularly remind users of their existence, and educate users in their application.

Another form of monitoring that organisations might consider using in the workplace is video surveillance. This is particularly relevant in the context of data centres, where physical access should be tightly controlled. In New South Wales, the Workplace Video Surveillance Act 1998 regulates "covert" video surveillance in the

workplace. Such surveillance must be authorized by a magistrate, and satisfy other conditions. “Overt” video surveillance, as defined in the Act, is not affected by the legislation (Oz Netlaw, 2002). Hence, if an organisation in New South Wales wishes to implement video surveillance of a workplace or data centre to improve security, it must ensure that:

- 14 days prior notice is given to the employee(s) of the intended video surveillance,
- the camera or equipment used is clearly visible, and
- signs notifying the employees of the surveillance are clearly visible.

(Note that under the Act, video surveillance must not occur in a toilet, change room or bathing facility.)

IT Security Incidents - Potential Offences

Actions involving the compromise of the security of a computer may constitute a more general offence, such as fraud. Typically, in order to prove such an offence occurred, the prosecution must establish beyond reasonable doubt that the person intended to commit the offence in question. Establishing that they compromised the security of the computer is not enough – they must have intended to commit the offence in question. Further, in the early stages of incident handling, it is often difficult to determine the intruder’s motivation. This in turn makes it difficult to determine what offence, if any, has occurred.

However, legislation dealing specifically with unauthorised access to computers, regardless of whether a more general offence is involved, has been enacted in all Australian jurisdictions:

Australian Capital Territory:	Crimes Act 1900, ss135J - 135L
New South Wales:	Crimes Act 1900, ss308 – 308I
Queensland:	Criminal Code s408D
South Australia:	Summary Offences Act 1953, s44
Tasmania:	Police Offences Act, ss43A – 43E
Victoria:	Crimes Act 1958, ss247B - 247G (as amended by the Crimes (Property Damages and Computer Offences) Act 2003) Summary Offences Act 1966, s9A
Western Australia:	Criminal Code, s440A

While the precise wording differs amongst jurisdictions, in essence all states and territories have made unauthorized access to a computer an offence, if the computer is subject to some form of access control system.

In addition, in some jurisdictions (including New South Wales and Victoria), the unauthorized modification or impairment of the security of data or an electronic communication is also an offence.

Further, the Commonwealth Criminal Code, ss477.1-478.4 defines additional statutory offences where:

- the intruder intended to commit a serious offence (as defined in the Code), or
- the data, electronic communications or computers involved in the offence were owned, leased, operated, or held on behalf of, the Commonwealth government, or
- a telecommunications service is used in the commission of the act. (Note that this gives the offence potentially very broad application.)

Summary

When developing and implementing an IT security program in an organisation, legal and regulatory issues must be taken into account. This paper has discussed a number of Australian laws, at both federal and state level, that are relevant to most organisations and could impact their IT security programs and practices.

References

Australian Capital Territory. “Fact Sheet #16 – Laws Affecting E-Business.” Information Series – E-Commerce for Small Business. URL: http://www.business.act.gov.au/iiainformationseries-e-businesslaws.pdf (1 Feb 2004).

Australian Communications Authority. “Telecommunications and Law Enforcement Manual.” Jul 1998. Section 3.12. URL: http://www.aca.gov.au/aca_home/licensing/radcomm/about_radcomms_licensing/leac.pdf (1 Feb 2004).

Gadens Lawyers. “IT Security: A director's challenge. E-Commerce Update. May 2001. URL: http://www.gadens.com.au/docushare/dscgi/admin.py/Get/File-642/E-Commerce_E-Update_May_2001.pdf (1 Feb 2004).

Hourigan, Phillip. “Legal Issues Driving e-security for all Enterprises.” 26 Nov 2002. URL: http://www.mlaa.com.au/events/Philip%20Hourigan.pdf (1 Feb 2004).

Internet Industry Association. “Cybercrime Code of Practice.” Public consultation draft version 2.0. Jul 2003. URL: http://www.iia.net.au/cybercrimecode.html (1 Feb 2004).

Internet Industry Association. “Internet Service Providers, Law Enforcement and National Security Fact Sheet.” URL: http://www.iia.net.au/ispsheet.html (1 Feb 2004).

Internet Industry Association. “Privacy Code of Practice.” Consultation draft version 1.0. 14 Aug 2001. URL: http://www.iia.net.au/privacycode.html (1 Feb 2004).

Jones, Helen (Ed). “IT security now forming ‘part of corporate RM’.” The Risk Report. Issue 143, 12 Sep 2002. URL: http://www.cpd.com.au/cpdnews/rr/archive/RR143.htm (1 Feb 2004).

Minter Ellison. “IT security – are you meeting your duty of care?” Technology News. Oct 2003. URL: http://www.minterellison.com/ajpe/resources/file/eb001008a9bb97d/TechNewsOct03.pdf (1 Feb 2004).

Minter Ellison. “Legal liability for on-line security.” Technology News. Sep 2002. URL: http://www.minterellison.com/ajpe/resources/file/eb005c494b680fe/Technology030902.pdf (1 Feb 2004).

National Office for the Information Economy. “Information Security Awareness for Managers: What Do They Really Need To Know?” 19 Mar 2002. URL: http://www.cript.gov.au/www/CriptHome.nsf/0/FED08C213D917939CA256BDD00033D5C?OpenDocument (1 Feb 2004).

National Office for the Information Economy. “Understanding the e-commerce environment.” Doing Business Online with Government. Nov 2002. URL: http://www.noie.gov.au/publications/NOIE/biz-online/chapter_3.pdf (1 Feb 2004).

Office of the Federal Privacy Commissioner. “Guidelines on Workplace E-mail, Web Browsing and Privacy.” 30 Mar 2000. URL: http://www.privacy.gov.au/internet/email/index.html (1 Feb 2004).

Office of the Federal Privacy Commissioner. URL: http://www.privacy.gov.au/privacy_rights/laws/index.html (1 Feb 2004).

Oz NetLaw. “Cyberspace Crime Fact Sheet.” 28 Mar 2001. URL: http://www.oznetlaw.net/facts.asp?action=content&categoryid=219 (1 Feb 2004).

Oz NetLaw. “Privacy Fact Sheet.” 1 Jan 2002. URL: http://www.oznetlaw.net/facts.asp?action=content&categoryid=235 (1 Feb 2004).

Oz NetLaw. “Telecommunications Fact Sheet (short version).” 14 Aug 2001. URL: http://www.oznetlaw.net/facts.asp?action=content&categoryid=238 (1 Feb 2004).

Oz NetLaw. “Workplace Net Control Fact Sheet.” 26 Feb 2002. URL: http://www.oznetlaw.net/facts.asp?action=content&categoryid=240 (1 Feb 2004).

Legislation and Case Law

Corporations Act 2001 (Cth), s180(1). URL: http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001172/s180.html (1 Feb 2004).

Corporations Act 2001 (Cth), s1317E. URL: http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001172/s1317e.html (1 Feb 2004).

Crimes Act 1900 (ACT), ss135J - 135L. URL: http://www.austlii.edu.au/au/legis/act/consol_act/ca190082/#s135j (1 Feb 2004).

Crimes Act 1900 (NSW), ss308 – 308I URL: http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/#s308 (1 Feb 2004).

Crimes Act 1958 (Vic), ss247B - 247G, as amended by the Crimes (Property Damage and Computer Offences) Act 2003 (Vic). URL: http://www.austlii.edu.au/au/legis/vic/consol_act/cdacoa2003416/ (1 Feb 2004).

Criminal Code (WA), s440A. URL: http://www.austlii.edu.au/au/legis/wa/consol_act/cc94/s440a.html (1 Feb 2004).

Criminal Code Act 1899 (Qld), s408D. URL: http://www.austlii.edu.au/au/legis/qld/consol_act/cc189994/s408d.html (1 Feb 2004).

Criminal Code Act 1995 (Cth), ss477.1-478.4. URL: http://www.austlii.edu.au/au/legis/cth/consol_act/cca1995115/sch1.html (1 Feb 2004).

Information Act 2002 (NT). URL: http://notes.nt.gov.au/dcm/legislat/Acts.nsf/84c76a0f7bf3fb726925649e001c03bb/676b979c0909b85269256c15007f2153?OpenDocument (3 Feb 2004).

Information Privacy Act 2000 (Vic). URL: http://www.dhs.vic.gov.au/privacy/html/info_privacy_act/index.htm (3 Feb 2004).

Information Privacy Principles (Cth). URL: http://www.privacy.gov.au/publications/ipps.html (1 Feb 2004).

Information Privacy Principles (Tas). URL: http://www.go.tas.gov.au/standards/privacy/privacy.htm (3 Feb 2004).

Information Privacy Principles Instruction (SA). URL: http://www.archives.sa.gov.au/services/public/privacy_index.html (3 Feb 2004).

National Privacy Principles. URL: http://www.privacy.gov.au/publications/npps01.html (1 Feb 2004).

Police Offences Act 1935 (Tas), ss43A – 43E. URL: http://www.austlii.edu.au/au/legis/tas/consol_act/poa1935140/#s43a (1 Feb 2004).

Privacy Act 1988 (Cth). URL: http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/ (1 Feb 2004).

Privacy and Personal Information Protection Act 1998 (NSW). URL: http://www.lawlink.nsw.gov.au/pc.nsf/pages/generalinfo (3 Feb 2004).

Privacy Scheme (Qld) . URL: http://www.justice.qld.gov.au/dept/privacy.htm (3 Feb 2004).

Summary Offences Act 1953 (SA), s44. URL: http://www.austlii.edu.au/au/legis/sa/consol_act/soa1953189/s44.html (1 Feb 2004).

Summary Offences Act 1966 (Vic), s9A. URL: http://www.austlii.edu.au/au/legis/vic/consol_act/soa1966189/s9a.html (1 Feb 2004).

Telecommunications (Interception) Act 1979 (Cth). URL: http://www.austlii.edu.au/au/legis/cth/consol_act/ta1979350/ (1 Feb 2004).

Telecommunications Act 1997 (Cth). URL: http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/ (1 Feb 2004).

Workplace Video Surveillance Act 1998 (NSW). URL: http://www.austlii.edu.au/au/legis/nsw/consol_act/wvsa1998295/ (1 Feb 2004).

Vrisakis v ASC (1993) 11 ACSR 162 at 212, Ipp J.