COMPUTERS & LAW

Journal for the Australian and New Zealand Societies for Computers and the Law

Editors: Lesley Sutton and Nicole Wellington
Number: 46

ISSN 08117225
December 2001

Under lock and keyboard – Prevention of unauthorised use of corporate computer systems

Leif Gamertsfelder, Andrew Handelsmann, & Praveena Sivanesarajah, Deacons

Leif Gamertsfelder is the leader of the E-security Group at Deacons in Sydney. Leif advises medium to large institutions in relation to a wide range of IT, privacy and e-security issues. Leif is also a columnist for the Australian Personal Computer. Andrew Handelsmann works in the Digital Industries and E-security Group at Deacons in Sydney. Andrew advises clients in the fields of information technology, e-commerce, privacy, intellectual property and trade practices. Praveena Sivanesarajah is a Lawyer in the Digital Industries Group at Deacons in Sydney. Praveena has been involved in advising a wide range of clients on IT, trade practices, intellectual property and privacy issues.

1. Introduction

For some time now, employers have perceived the threat of unauthorised use of their computer systems as an external menace.[1] This is due in part to the high media attention given to stories about hackers gaining illegal access to the well-guarded computer networks of large companies and government departments. The truth is, however, that the vast majority of unlawful access and computer trespass offences against companies occur under the very noses of management, committed by employees from within the company's own ranks.

The American Computer Security Institute recently surveyed a large number of corporations, medical institutes and government agencies about serious security breaches of their computer systems such as the theft of proprietary information, financial fraud, denial-of-service attacks and the sabotage of data or networks.[2] It found that 71 percent of those surveyed reported these kinds of attacks as having occurred from inside the company while only 25 percent reported system penetration from outsiders.

Employees, who often occupy positions of trust, have the greatest access to information within the organisation and so have the greatest potential to exploit information sources or sabotage computer systems for personal gain.[3] These acts involve the unauthorised viewing or use of data and information and the unauthorised entry or alteration of data to produce false transactions and tamper with information systems.

Fraud may be characterised as any practice that involves deceit or other dishonest means by which a benefit is obtained. Before the advent of complex computer networks such as the internet, fraud generally involved

Continues page 3

In this issue:

Continued from page 1

deception through the use of a tangible object such as a forged legal instrument. In the new online environment, however, fraud may be committed through the unauthorised use of digital technology without the need for any such object.[4] The vastly increased scope of access and the instantaneous effect of transactions in the digital age have endowed computer frauds with a new potency[5] and have provided a plethora of new opportunities for crackers.[6] Examples of computer fraud include 'bogus transactions' (the use of false or forged electronic information and communications in commercial transactions), and 'data diddling' (the deliberate entry of inaccurate or misleading data into a computer system for financial gain).[7]

The trends in computer crime enforcement all seem to suggest moves towards harsher penalties, more expansive provisions and heightened enforcement. In Australia, there has been much legislative activity in this area at both federal and state level. As will be discussed in more detail later, it is essential that employers acknowledge the risks of unauthorised access and computer fraud by employees and put in place monitoring systems and preventative measures that address these risks.

2. Australian legal context

In the area of computer crimes, there are Commonwealth, State and Territory offences which exist and operate side by side. The State and Territory offences apply to wrongful conduct within each jurisdiction and the Commonwealth offences generally target unlawful access to Commonwealth computers and data. These laws make it an offence for a person to do or attempt to do[8] the following:

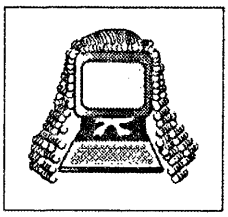
(a) gain unlawful access to a computer system;
(b) damage data and impeding access to computers;
(c) steal computer data; and
(d) commit fraud.

These pieces of legislation and by implication, the relevant case law will be triggered when an employee is involved in any computer fraud or unauthorised access to computer systems.

2.1 Commonwealth

Crimes Act 1914 (Cth)* and *Criminal Code Act 1995 (Cth)

Until May 2001, fraud was generally dealt with under section 29 of the *Crimes Act 1914*. The section has now been repealed[9] under Schedule 2 of the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000* and modified fraud provisions have been incorporated into the *Criminal Code Act 1995*.[10]



COMPUTERS AND LAW

Editors

Lesley Sutton
C/- Freehills
Level 32, 19 – 29
MLC Centre, Martin Place
Sydney NSW 2000
Australia
(DX 361 Sydney)
www.freehills.com.au
Tel: +61 2 9225 5169
Fax: +61 2 9322 4000
Email: Lesley_Sutton@freehills.com.au

Nicole Wellington
C/- Freehills
Level 32, 19 – 29
MLC Centre, Martin Place
Sydney NSW 2000
Australia
(DX 361 Sydney)
www.freehills.com.au
Tel: +61 2 9225 5229
Fax: +61 2 9322 4000
Email: Nicole_Wellington@freehills.com.au

Australian Subscription: $32.00* per 4 issues

Overseas Subscription: $44.00 per 4 issues

Advertisements: $300.00* for half page advertisement within the journal (see page 51).

Further information on rates will be provided by the Editors on request.

Articles, news items, books for review and other items of interest may be sent to the Editors.

**Please see back cover for GST details.*

Part VIA of the *Crimes Act 1914*, which dealt with unauthorised access and data infringement offences relating to computers,[11] was largely repealed by the *Cybercrime Act 2001 (Cth)* ("**Cybercrime Act**"). The *Cybercrime Act* received Royal Assent on 1 October 2001 but has not yet commenced operation.[12] Under this new Act, new computer offences will be inserted as Part 10.7 of the *Criminal Code Act 1995* (Cth) ("**Criminal Code**").[13]

Under the amended fraud provisions of the *Criminal Code*, it is an offence to dishonestly or by deception appropriate property or obtain financial advantage from another person if the property belongs to a Commonwealth entity or the other person is a Commonwealth entity.[14] Property is defined in the Code to include "intangible property". It remains to be seen whether computer data will fall within this definition.[15] The Act defines "deception" as including "conduct by a person that causes a computer, a machine or an electronic device to make a response that the person is not authorised to cause it to do" and there are detailed provisions relating to fraudulent money transfers[16] and the forgery or falsification of documents.[17]

The specific Commonwealth computer crime offences created by the *Cybercrime Act* in Part 10.7 of the *Criminal Code* are primarily focussed on targeting unlawful access to Commonwealth computers and data.[18] The scope of the Commonwealth legislation is limited by the legislative powers granted to the Parliament in the Australian Constitution.[19] Therefore, the offences must have a 'Commonwealth connecting factor', such as conduct in relation to computers owned, leased or operated by a Commonwealth entity, conduct in relation to data held by or on behalf of the Commonwealth, and conduct via telecommunications services. The *Cybercrime Act* introduces seven new offences, which are directed at conduct that impairs the security, integrity and reliability of computer data and electronic communications. The new Part 10.7 prohibits unauthorised access, modification or impairment of electronic data or electronic communications.[20] "Data" is defined in the Act as including all information and programs held in a computer.[21]

These provisions would apply in a number of situations that might affect employers including:

(a) a public sector employee using Commonwealth computers or data outside the scope of their authority; or
(b) a private sector employee tampering with Commonwealth computers or data within the course of their employment (ie misusing employers' computer network in some way).

As the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000* commenced only recently on 24 May 2001, and the *Cybercrime Act* is yet to commence, there have not been any prosecutions relating to the new provisions on computer fraud. There are however a number of cases where individuals have been prosecuted for a breach of unauthorised computer access under the *Crimes Act 1914*. *Gilmour v DPP*[22] is instructive as it demonstrates the type of situation which may arise under the amended *Criminal Code*.

Gilmour v DPP

In *Gilmour v DPP*[23], the defendant was a public servant employed in the Relief Section (RS) of the ATO. The RS's function is to consider applications by taxpayers for relief from payment of income tax. Gilmour himself did not have any authority to determine whether relief should be granted in a particular instance, rather his duty was to record data relating to the determination of applications for relief (this included entering certain codes into the system). Under this duty, the defendant had general authority to access the system by entering his user ID and password and he was permitted by his employer to enter relief code '43' only in situations where relief had been granted.

On 19 occasions, the defendant entered relief code '43' into the computer system when he knew that relief had not been granted. He was prosecuted under section 76C of the *Crimes Act 1914* for unauthorised entry of data into a Commonwealth computer.

Gilmour argued that his general authority to access the ATO's computers (through his user ID and password) granted him authority to make the entry of relief code '43' in each case. He further argued that his access was not unauthorised or unlawful because the computer system had the capacity to be programmed to prohibit unlawful entry of data but was not so programmed in the case of relief code '43'.

It was held by the Supreme Court of New South Wales Court of Criminal Appeal that an entry of data is made "without authority" when the officer is not authorised to make the particular entry, notwithstanding that the officer has general authority to gain access to the computer and make other entries.[24] The Court rejected the defendant's arguments and held that the fact that the computer accepted the entries did not mean that the entries were authorised.

2.2 State Legislation

***Crimes Act 1900 (NSW)* ("Crimes Act 1900")**

Section 124 of the *Crimes Act 1900* deals with "fraudulent appropriation" of property and provides that a person who fraudulently appropriates or retains the property of another for his/her own use is guilty of an offence. Presumably, this applies to computer-related property such as data.[25]

Each State and Territory (with the exception of the Northern Territory) has its own criminal provisions relating to computer and computer data offences.[26] Taking the NSW legislation as an example, Part 6 of the *Crimes Act 1900* provides for computer offences involving unlawful access and damage to data in a computer. The *Crimes Act 1900* provides that a person who intentionally and without authority or lawful excuse destroys, erases or alters data stored, or inserts data into a computer, or interferes with, or interrupts or obstructs the lawful use of a computer is liable to

imprisonment or a fine, or both.[27] The NSW Act also states that a person who uses a computer with intent to defraud is guilty of the crime of computer-related fraud.[28]

Computer crimes involving the misuse of data for financial gain may also fall under the general fraud provisions of State and Territory criminal legislation.[29] For example, in NSW, section 178BA of the *Crimes Act 1900* provides that it is an offence to, by any deception, dishonestly obtain money or financial advantage. The term "deception" is defined to include an act done with the intention of causing a computer system to make a response which that person is not authorised to cause the computer system to make.[30]

***Crimes Amendment (Computer Offences) Act* 2001 (NSW)**

On 30 May 2001, the New South Wales Parliament passed an Act to amend Part 6 of the *Crimes Act 1900* to include crimes in relation to impairment of electronic communication. The new Act, the *Crimes Amendment (Computer Offences) Act 2001*[31], relates to crimes concerning unauthorised impairment or modification of computers and electronic communications.

The provisions are more comprehensive than the existing provisions of the NSW Act and are intended to ensure that the *Crimes Act 1900* is up to date with the most recent technological developments. Punishment for the proposed offences is by way of a fine as well as imprisonment in accordance with sections 15 and 16 of the *Crimes (Sentencing Procedure) Act 1999 (NSW)*. The provisions apply to all instances of computer fraud by employees and in particular those that involve online fraud.

Each individual State and Territory is following suit with similar amendments to their respective criminal statutes.

2.3 Case Law

Once again, it is prudent to examine how legislation governing computer crime has been applied in practice. There is a dearth of NSW cases dealing with employees gaining unauthorised access to computers and data, but the following Victorian case is instructive in that it turned on similar provisions under the *Crimes Act 1958 (Vic).* (**"Crimes Act 1958"**)

***DPP v Murdoch*[32]**

In this case, the defendant was employed in the information systems department of a bank. On a number of occasions, the defendant typed entries into a terminal connected to the bank's main computer so that he was able to make withdrawals from automatic teller machines notwithstanding that his account was in debit. The defendant also made an entry to link his automatic teller machine debit card to a different account of his which was in credit.

He was charged with a large number of offences including charges of obtaining property by deception contrary to section 81(1) of the *Crimes Act 1958* and charges of computer trespass contrary to section 9A of the *Summary Offences Act 1966 (Vic)*. At first instance, the magistrate found the respondent not guilty of the computer trespass charges and the Director of Public Prosecutions appealed.

Section 9A of the *Summary Offences Act 1966* provides that "a person must not gain access to, or enter, a computer system or part of a computer system without lawful authority to do so". None of the expressions "gain access to", "enter", or "computer system" are defined in the Act. The magistrate held that section 9A was intended to prevent entry to computer systems by "outside persons or hackers". There was an appeal on the question of whether the magistrate erred in ruling that this section "did not apply to persons who are authorised users of a computer system and used a computer system or part of a computer system without lawful authority."

Hayne J held on appeal that the section does not distinguish between persons who have no permission to enter a computer system (eg hackers) and persons who have authority of some kind to enter the computer system. Rather, the section invites attention to whether the particular entry or gaining of access to the computer system was with or without lawful authority.

> "If [an employee] has a general and unlimited permission to enter the system then no offence is proved. If however there are limits upon the permission given to him to enter that system, it will be necessary to ask was the entry within the scope of the permission? If it was, then no offence will be committed; if it was not, then he has entered the system without lawful authority to do so"[33].

Hayne J allowed the appeal with regard to section 9A on the basis that the trial magistrate had erred in concluding that the section distinguishes between entrants who have some permission to enter a computer system and those who have none (eg hackers).

The approach adopted by Hayne J in this case accords with the intent of the legislature in enacting the legislation. The then Attorney General said during his second reading speech of what was to become section 9A that:

> "The offence will consist of gaining access to or entering a computer system without lawful authority to do so. It will apply not only to hackers but also to authorised users, such as employees, who deliberately enter a part of a computer system to which they do not have authorization."

3. Major Legal Risks

3.1 Civil Liability – Employee related risks

Negligence

If, due to a vulnerability in the information system of a company, another party suffers loss or damage as the result of employee fraud, this may give rise to an action in negligence.

The issue of whether there exists a

positive duty on a party to act so as to prevent criminals causing harm or economic loss to others is yet to be tested in Australian courts. The High Court did however, recently consider in an analogous scenario, whether a party has a duty to take reasonable steps to prevent criminals causing injury to others in *Triangle Shopping Centre Pty Ltd v Anzil*[34]. In their judgment, the High Court restated the principle developed by Brennan CJ in *Sutherland Shire Council v Heyman*[35], that the ability of a plaintiff to recover in these types of cases will be dependant on the plaintiff being able to show that there was sufficient nexus (eg reliance or assumption of responsibility) between the plaintiff and the defendant to give rise to a duty on the defendant to take reasonable steps to prevent third parties causing loss to the plaintiff.[36] Following from this, if a plaintiff in a breach of computer security could show that the defendant company did not in fact take reasonable steps to provide system security against both internal and external attacks, and that the act of the third person (eg fraudulent employee) could not have taken place but for the defendant's own fault or breach of duty, then the negligence action may be successful.

It is interesting to contrast this general proposition with a peculiar case where the plaintiff went to great lengths in an attempt to recover loss caused by its own negligence, namely loss suffered due to computer fraud perpetrated by its own employee in its own system. In the unreported case of *Mercedes Benz (NSW) v ANZ and National Mutual Royal Savings Bank Ltd*[37], the Supreme Court of New South Wales considered whether a duty to prevent fraud arises if there is a foreseeable possibility of loss. The case concerned the pay mistress of Mercedes Benz who fraudulently misappropriated almost $1.5m of her employers' funds through misuse of the company's computerised payroll system. Mercedes Benz sought to recover its loss by alleging negligence on the part of the first defendant (ANZ), which paid various cheques fraudulently procured by the pay mistress to be drawn upon it, and also from the second defendant (NMRB) which provided banking facilities for the administration of the payroll scheme, collected the cheques fraudulently procured by the pay mistress and paid away the proceeds at her direction. The court dismissed the plaintiff's claim, holding that employers who are lax in their vigilance against fraud and have in place only very rudimentary systems for scrutiny of employees are liable for the losses that flow from fraudulent acts committed by those employees. The judges relied for their decision on authority dating back to the 18th century in the judgment of Holt CJ in *Hern v Nichols (1701) 1 Salk 289*: "seeing somebody must be a loser by this deceit, it is more reason that he that employs and puts a trust and confidence in the deceiver should be a loser than a stranger".[38] While the plaintiff was unsuccessful in this case, the situation may be different where the flawed processes were not operated by the plaintiff but by a party providing services to the plaintiff under an outsourcing agreement.

Vicarious Liability

Vicarious liability for the actions of employees can be imposed on an employer in common law[39] and by statute.[40] The standard test for vicarious liability is that the action of the employee must have been committed in the course and scope of their employment.

It is important to note that "within the scope of employment" is a broad term for which there is as yet no absolute legal definition. However, case law has established the following principles:

- where an employer authorises an act but it is performed in an improper or unauthorised manner, the employer will still be held liable;[41]
- it does not matter that an employee is unauthorised to perform an act[42]; and
- the mere fact that an act is illegal does not bring it outside the scope of employment[43].

Even though unauthorised access or computer fraud by an employee is an act that ostensibly lies outside of the employee's scope of employment, this does not automatically exclude the employer from vicarious liability.[44] Also, it is not necessarily an answer to a claim against an employer that the wrong done by the employee was for the employee's own benefit. The law was authoritatively stated in the well known case of *Lloyd v Grace, Smith and Co* [45], where a solicitor was held liable for the fraud of his clerk, even though the fraud was entirely for the clerk's own benefit.[46] *Lloyd v Grace, Smith and Co* was referred to by Dixon J in the leading High Court case, *Deatons Pty Ltd v Flew*[47]. That case concerned an assault by the appellant's barmaid who threw a beer glass at a customer. In discussing the applicable principles, Dixon J suggested that a servant's intentional wrongful acts may incur liability for their master in circumstances where:

> "they are acts to which the ostensible performance of his master's work gives occasion or which are committed under cover of the authority the servant is held out as possessing or of the position in which he is placed as a representative of his master."

By this authority, it is fairly well settled that if an employee commits fraud or uses a computer system in an unauthorised manner and thereby causes damage to a third party, the employer may be held liable for their actions.

Unfair Dismissal/Contracts of Employment

If an employment contract is terminated on the basis that the employee gained unauthorised access to a company's computer systems and the employee subsequently argues that they believed they had authority to do so (or authority is unclear), this may provide grounds for a claim of breach of the employment contract or an unfair dismissal action against the employer. Employees might seek compensation for lost wages and in some cases, psychological trauma, distress, anxiety and injured feelings[48] and this can prove very costly for employers.

There have been a number of cases dealing with the issue of unauthorised access to computer systems that have been brought in front of the Australian Industrial Relations Commission and

various State and Territory Commissions. Most of these actions were brought under section 170 CE(1) of the *Workplace Relations Act 1996 (Cth)* for relief in respect of the termination of employment on the grounds that it was harsh, unjust or unreasonable[49] and the equivalent provisions under the various State and Territory workplace relations Acts.[50]

For a claim of this nature to succeed, the plaintiff employee has to show there was no valid reason for the termination related to their capacity or conduct or to the operational requirements of the employers' undertaking, establishment or service.[51] In *Helen Utting and Commonwealth of Australia - Department of Social Security*[52], the applicant was employed as a receptionist at a regional Department of Social Security office in Dee Why (NSW) where her duties included accessing the computer records of some clients for particular and limited purposes. Her employment was terminated when it was discovered that she had unlawfully accessed the computer records of seven clients of the Department (known colloquially as "browsing"). In the hearing, the applicant argued that due to procedural shortcomings within the office, she had insufficient knowledge of Departmental protocols and was unaware of their strict instructions and guidelines on browsing. She further argued that she had not been provided with updated written instructions or changes to policies or procedures and had not committed unlawful access as she was ignorant as to the true extent of her computer access rights. Although the applicant was unsuccessful in this instance, the case clearly demonstrates the risks that employers face in this context.

The touchstone in unfair dismissal cases of this type is whether, in the circumstances, the termination was "sound, defensible and well founded".[53] If an employee can show that the reason for termination was not well established in that they were inadvertently breaching their authority of access to the computer systems due to lack of knowledge about procedures, then the action against their employer may be successful. In *Australian Municipal, Administrative, Clerical & Services Union v Ansett Australia Ltd [2000]*[54] the court considered whether an employee's use of her employer's email system to distribute an ASU bulletin on the current state of enterprise bargaining constituted unauthorised use of the company's computer system. The court looked at whether the email might have been a legitimate business communication in accordance with Ansett's IT Policy which states that Ansett employees are only authorised to use its IT and Communications facilities and resources for "performing lawful business activities". The court held that management did not have a "good enough grasp of who needed to authorise" such a communication to make a reasonable determination on the employee's conduct.

These cases indicate why it is so important for employers to have policies and procedures in place that describe unambiguously the rights of access for each employee. This issue will be discussed in greater detail in the Risk Prevention section of this paper.

Privacy

The *Privacy Amendment (Private Sector) Act 2000* ("**Privacy Amendment Act**") will commence on 21 December 2001. Under this new Act, an organisation[55] must take reasonable steps to protect the personal information it holds from misuse and loss, from unauthorised access, modification or disclosure.[56] Protecting the security of personal information will involve taking reasonable steps to maintain: physical security, computer and network security, the security of communications and the appropriate training of staff. Information should either be destroyed or de-identified when it is no longer needed for the purpose of collection, any permissible secondary purposes or for the purpose of meeting a legal requirement to retain the information. A security policy that deals with privacy issues is essential for an organisation that wants to avoid breaching the National Privacy Principles as it establishes strict systems to ensure that personal information held or processed by the organisation is not subject to unauthorised access or use. For example, in an online context, a policy would dictate that personal data would never be stored in the clear on a transaction server.

Companies should also be aware of the enormous reputation risks associated with a breach of security relating to personal information. For example, in 1995 Skeeve Stevens was convicted for hacking into AUSNet's computer network using the user account and password details of AUSNet's technical director.[57] He then altered the company's home page by displaying a message that subscriber credit card details had been captured and distributed on the internet, and subsequently published some credit card details of identified individuals. Stevens was sentenced to three years imprisonment, with eighteen months non-parole. Although the intrusion caused minor direct financial loss, the reputation of AUSNet was severely damaged and the incident is alleged to have resulted in widespread loss of consumer and business confidence costing the company more than $2 million in clients and contracts in the months following the incident.

3.2 Civil Liability – General risks

An employer whose systems are breached because they did not have adequate protections in place may open themselves up to other potential areas of liability including under contract law, the *Corporations Act 2001(Cth)* ("**Corporations Act**") and possibly the ASX Listing Rules.

Contract/Trade Practices Act

Entities that have contractual relationships with a company who suffers a breach of computer security may sue for breach of contract or under an indemnity clause if they incur loss or damage as a result. This is more likely to happen if a party has an express obligation in relation to electronic security and the breach of security could have been prevented if reasonable steps had been taken to secure the relevant systems. Any case involving an allegation of breach of contract will largely turn on

interpretation and incorporation of terms issues and to what extent a party is able to derive assistance from legislation such as the *Trade Practices Act 1974 (Cth)* and mirror State Fair Trading Acts.

Directors' Liability

If a security breach is attributable to a failure by a company to take reasonable steps to implement robust e-security architecture, shareholders may ask questions. They may want to know what steps (if any) the directors took to prevent the breach of network security. After all, directors have a duty to exercise fiduciary care[58] and due diligence[59] in the protection of corporate assets and minimisation of loss. Accordingly, in order to comply with their obligations under the *Corporations Act*, directors need to once again ensure that appropriate measures are taken to protect the company's information systems and the data on those systems.

A breach of the *Corporations Act* can result in a variety of actions against the director personally:

(a) criminal proceedings;[60]
(b) proceedings for a civil penalty order by the Australian Securities and Investments Commission;[61]
(c) claims for compensation by the company or its creditors under the *Corporations Act* or the Common Law;[62] and
(d) claims by shareholders resulting from losses derived from a drop in the share price as a result of the security breach[63].

ASX Listing Rules

Downward pressure on a company's share price may be caused by the effect of ASX Listing Rule 3.1 requiring continuous disclosure. A breach of computer security cannot be concealed from the world if information about the breach itself falls within the scope of this rule. Listing Rule 3.1 imposes on listed companies a duty of disclosure where the information is material to share prices. Entities that are required to disclose information under the Listing Rules must not contravene the law by intentionally, recklessly or negligently failing to notify the ASX of information:

- that is not generally available; and
- that a reasonable person would expect, if it were generally available, to have a material effect on the price or value of the securities of the entity.

Penalties for non-disclosure are severe, including removal from the official listing on the ASX.

3.3 Criminal Liability

In some situations, employers can become directly or vicariously liable for their employees' criminal conduct.

Direct liability means the liability that attaches to a company or organisation when the employer directs or authorises the performance of acts of the employee. According to Lord Reid in *Tesco Supermarkets Limited v Nattrass*, this occurs when a person is "not acting as a servant, representative, agent or delegate" of the company, but as "an embodiment of the company".[64] For a company, this normally relates to the actions of directors and upper management when those people are acting "as the company". However, as directors can delegate their functions, direct liability can extend to employees acting with delegated authority. Where it can be shown that by a direct act or omission the employer stood by and allowed the employee to commit the crime, the employer may be directly liable for the crime.

An employer cannot be held vicariously liable for a crime committed by an employee where that offence requires proof of *mens rea*.[65] An employer can, however, be held vicariously liable for an offence committed by an employee if the offence does not require proof of *mens rea*,[66] or where a statute creates vicarious liability (either expressly or impliedly). In these cases, the conduct or mental state of an employee is attributed to his or her employer, so long as the employee is acting within the scope of his or her employment.

Indeed, there appears to be an increasing willingness on the part of courts to attribute criminal liability to a corporation for the acts of its employees. An example of this is the recent Privy Council decision of *Meridian Global Funds Management Asia Ltd v Securities Commission*[67]. In this case an investment manager fraudulently invested in another company without making the necessary disclosures he knew he was obliged to do. Lord Hoffman refused to limit corporate responsibility to only the upper management, who represent the "directing mind and will" of the company, and found that the investment manager had acted on behalf of the company in committing the crime. He stated that in each case, the court had to "fashion a special rule of attribution for the particular substantive rule".[68] The rule here was one requiring disclosure of substantial investments to the company and to the stock exchange. In this case, as the investment manager was authorised by the company to make the investments, the court held that his acts and knowledge could be attributed to the company. It is likely that this type of fraudulent activity will only be made easier by the implementation of new technologies in the workplace and that the attribution of criminal liability to an organisation in this way may extend to acts involving misuse by employees of these new technologies.

It is also worth noting that section 85ZK of the *Crimes Act 1914* makes it illegal to use equipment connected to a telecommunications network in the commission of an offence against a law of the Commonwealth or of a Sate or Territory. While this section does not of itself create liability, it adds to the penalties that an employer faces if liable for an employee committing Commonwealth and State offences via the internet.

4. Risk Prevention and the Responsibilities of Management

4.1 Prevention is the key

Much of the computer fraud committed by employees can be averted if employers implement effective processes for monitoring and controlling access to, and use of, information resources and networks. As Dorothy Denning points out, "even if an offensive operation is not prevented, monitoring might detect it while it is in progress, allowing the

possibility of aborting it before any serious damage is done and enabling a timely response."[69]

However, it is important to note that not all unauthorised access by employees is intentional. Poorly drafted contracts of employment, computer use procedures and access protocols may result in employees being confused about what types of access and use are in fact permitted. It is the duty of management to ensure that employees are fully aware of the scope of their access rights and that breaches of any kind are expediently brought to their attention.

A good risk management strategy will reduce risk of fraud and assist in prosecuting fraud. This will determine what a department needs to do to reduce opportunities for fraud. Electronic security risk management policies, which include appropriate technical measures, do not necessarily have to be very expensive. The key is to remove opportunity.

An effective risk management strategy involves a two-stage process:

1. *Identifying and eliminating security weaknesses:*

(a) monitoring information systems for vulnerabilities;
(b) developing systems that are free of vulnerabilities;
(c) implementing acceptable use policies; and
(d) continuing user training and awareness programmes, and

2. *Implementing safeguards to prevent or detect attacks:*

(a) access controls (access control monitors, authorisation policies etc);
(b) filters (firewalls, web filters etc); and
(c) intrusion and misuse detection (audit logs, automated detection, workplace monitoring, computer misuse detection, virus protection etc).

4.2 Monitoring Policies

It is vital that employers are at all times aware of how their information systems and databases are being accessed and by whom. This involves monitoring all information systems performing their tasks and collecting information about network traffic, CPU, disk usage and access attempts using log files or more sophisticated techniques such as intrusion detection systems[70]. Detection mechanisms should be used to detect both attempts to violate security and successful security violations, when or after they have occurred in a system. Regular electronic audits[71] are necessary (eg checking network logs) as are exhaustive due diligence processes that identify and fix existing security flaws.

Many employers are concerned that the private sector *Privacy Amendment Act* will prevent them from monitoring employee use of the employer's information systems. As long as the employer takes certain precautions and clearly sets out its monitoring practices in a well drafted, effective privacy policy, they will generally be able to continue monitoring the electronic practices of their staff in some circumstances.

The key element in determining whether monitoring practices will breach the new *Privacy Amendment Act* is the purpose for which the information is collected. It is highly arguable that backup information and logs are designed to monitor an employee's activities, hence these secondary uses probably will not breach the National Privacy Principles. However, all organisations need to get specific advice on whether they need to obtain employee consent before undertaking specific monitoring activities.

4.3 Security Measures

Given the fast moving pace of the IT industry, determining appropriate technical safeguards against cracking and computer fraud for a given company will necessarily involve consideration of prevailing industry practice. For some organisations, this may mean issuing a request for tender for computer security services to ensure that the security systems are sufficiently robust. For others, it may mean hiring a consultant to audit the rule sets in a firewall on a periodic basis.

At the very least though, a non-exhaustive list of reasonable steps for Australian companies should include:

- The compilation of a documented network architecture that has been reviewed by a number of skilled staff (or external experts). This document should include not just traffic flow control, but consideration of authentication and access control,[72] and the use of other measures specifically designed to defend confidentiality, integrity and availability.[73]
- Purchase of equipment that complies with the appropriate criteria set out for security standards.
- Purchasing of equipment on the Defence Signals Directorate Evaluated Products List[74] may also be a prudent course of action in some circumstances.
- An appropriate maintenance cycle for measures such as patches and configuration auditing. Implementation of each and every security upgrade for a system as it becomes available is essential.[75] A proactive approach can render any accusations of negligence moot and prevent civil law suits from customers or employees.
- Documented and reasonable technical administrative practices. This would include consideration of standards like AS4444 Information Security Management and the use of industry recognised checklists, such as the AusCERT UNIX Security Checklist and the AusCERT NT Security Checklist.
- Documented and reasonable human administrative practicessuch as acceptable usage agreements, staff education programs, physical security measures and effective enforcement processes.

Irrespective of the final solution though, all companies should conduct and document a risk analysis process which considers all the risks, the solutions available, and make reasonable decisions in light of that process.[76] In most cases, an organisation may need to obtain an

independent audit to identify its critical and non-critical information assets, determine what its risk profile is, and suggest solutions.

Independent audits will allow an organisation to determine what is reasonably required for it to minimise legal risk. While internal staff must assist in this task, they should never audit their own work. Where possible, prevailing industry practice suggests that an audit should be conducted every six months or whenever a major system change occurs.

However, this does not mean that exorbitant amounts of money need to be allocated to security processes. Some commentators believe that a quantitative approach is required when considering the level of resources allocated to security.[77] For example, if the expected loss associated with a network intrusion of a networked partner is $10,000,000,[78] but the probability of such an incident occurring is only 0.1%, then the annual loss expectancy is only $10,000. According to this theory,[79] a company may be acting reasonably if it spent only $10,000 per year to protect its information systems being used as a launch pad for attacks against those of its partner. This is due to the fact that while the gravity of harm is high, the risk of such harm occurring is quite low. In such cases, it is arguable that a court would consider the expenditure (and therefore the security measures that it will allow to be implemented) to be reasonable.

Notwithstanding the actual amounts that such analysis indicates is appropriate in any given case, it is interesting to note that some commentators believe that the standard practice in most organisations is to have at least one security professional for every one thousand employees and that approximately 3 to 5% of a firm's total information systems' budget should be spent on security.[80] In light of the fact that the courts will consider prevailing industry practice and norms that are important in determining what is reasonable in any given case, these figures serve as valuable reference points.

While expenditure may be one measure of reasonableness in this context, it is not what an organisation spends, but what tools it uses and how it uses those tools.

4.4 Computer Usage Policies

It is essential for employers to implement well-drafted contracts of employment and comprehensive induction programs that deal exhaustively with the issue of authorised access to the company's computer systems.

An employer may wish to establish an explicit computer systems use policy that contains a section titled "Conditions of Authorisation" or may want to include such a provision within the contract of employment. Such a provision should specify the explicit conditions under which employees are authorised to use the computer systems.

An employer may want to provide, in the most explicit language, that the employee's authorisation to use the computer system (including any email, web browsing or other form of internet access) is contingent on his or her continued compliance with all the conditions. Any use of the system to send any information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the company's business interests, should be explicitly prohibited.

The policy can be implemented via a written agreement, although it is probably easier for employers to establish a computer-systems based procedure, whereby the employee is required to assent to the terms and conditions of use as a prerequisite for signing onto the computer system. At the very least, there should be a notification at the logon point that clearly states that use of the system is subject to the terms and conditions of use that may vary from time to time.

The employer may also want to include a provision that allows the policies to be updated from time to time, and to have the updates become effective, as to any employee, when that employee continues to use the computer system after the updates are published. An email to all employees directing them to view the new policies on the company intranet can be an effective method of notification, so long as the employer can demonstrate that every employee had due and adequate notice of the new policies.

The policy should contain a disclaimer, stating that the list of explicit conditions of use is not meant to displace or supersede any implicit conditions that are otherwise recognised by law. The employee might argue, in later litigation, that the employer's express identification of specific conditions was meant to imply an exhaustive listing. Such arguments, which are usually based on the infinite ambiguity of language and the rules of construction, can often be avoided by careful drafting.

An employee who intentionally accesses a computer without authorisation and thereby obtains information from a protected computer violates the criminal law. An employer may want to provide that violation of a condition also constitutes grounds for dismissal, although such a result may well be implied even without an explicit statement. If an employer provides, as suggested, that such a violation automatically revokes the employee's authorisation, then any further use by the employee of the computer system after the automatic revocation is likely to constitute a violation of at least one section of the various Commonwealth and State criminal statutes.

4.5 Insurance

In response to increasing occurrences of economic loss stemming from computer-based crimes, insurance companies are beginning to develop policies targeted specifically at those kinds of contingencies. Lloyd's of London, one of the world's largest insurance firms, recently began to offer insurance against business losses due to mischief by crackers and hackers.[81] Insurance programs of this nature protect against the loss of revenue and information assets caused by computer security breaches. Claims would, in most cases, cover the cost to repair and replace data and/or software to the same standard as

before the attack.[82] As an added benefit to policyholders, coverage often includes consultation from security consultants on how to prevent computer security breaches.[83] Clearly, if a company relies heavily on technology or uses the internet for business, it should be in the market for technology insurance.

Companies should review all current policies (including director and officer policies) in order to determine whether those policies cover risks related to computer security. Many companies will find that they will not be covered as most general insurance policies fail to either include technology-related incidents in their descriptions of coverage, or exclude such areas entirely.[84]

Companies should exercise care in choosing the right policy for their particular needs.[85] To do this, management may want to consult a technology lawyer who can evaluate the company's exposure and point out areas that require significant protection. Not all policies will cover a company for the intentional acts of its employees. It is important for a company to read the policy carefully. Often, buried deep within the terms and conditions of the policy, there will be limitations or exclusions of coverage that might be very important to the business. If the policy is ambiguous, a company may find itself in court just trying to determine the extent of the coverage. Depending on the type of business, it might be worth seeking out specific insurance against credit card and data theft, site shutdowns, system damage from viruses etc[86]. Currently, there is a paucity of insurance products on the market that specifically cover computer security risks, but demand is strong and it should not be long before many more products are available.

5. Evidence

Parties to litigation are more frequently seeking to introduce into evidence information that has been created, used or stored on or by computers. As a result, the courts' treatment of electronic evidence has significant implications for businesses in their management, record-keeping and security practices.

5.1 Admissibility

Under Commonwealth and NSW legislation there are no specific admissibility provisions which apply to computer generated or stored information. The *Evidence Act 1995 (Cth)* and the *Evidence Act 1995 (NSW)* ("**the Acts**") exclude hearsay evidence as inadmissible.[87] Both Acts create a business record exception, which allows business records to be admitted into evidence as an exception to the hearsay rule.[88] The Acts create a rebuttable presumption of the proper operation of devices and processes that produce business records.[89]

Some States have created a specific exception for computer-generated evidence.[90] These provisions allow for the admission of computer output, subject to the court being satisfied as to certain matters regarding the reliability of the computer. These provisions impose a significant burden of investigating in every case the reliability of all computer evidence. The presumption created under the Acts simplifies the process whilst allowing the fact-finder to decide upon the weight to be given to computer evidence. In contrast to the computer-specific provisions, the Acts properly treat the issue of computer evidence as a matter of reliability rather than categorising it as a matter of admissibility.

As not all computer-generated or stored data will be encompassed by the business records exception[91] under the Acts, the hearsay rule may exclude electronic evidence as evidence of the fact it records. The case law has established two types of electronic evidence that are not considered to be within the ambit of the hearsay rule[92]:

(1) Where the computer is being used as a calculator or scientific tool.[93]

In *Rook v Maynard*[94], an employee of the Department of Social Security (DSS) accessed data relating to the personal affairs of various people in a computer owned by DSS without any authority to do so. A computer trace program had been activated in respect of the defendant's logon identification number. The prosecution sought to tender the hard copy printouts of the data recorded by the trace program. The printouts purported to show the times and dates upon which the defendant had accessed the relevant files and to identify parts of the material accessed.

At first instance, the Magistrate held that the trace printouts were inadmissible due to a concern about the inaccuracy of the printout produced, as the trace printout did not show all of the information that would have been viewed by the defendant. On appeal, it was held that the incompleteness of the trace printouts does not preclude their admissibility into evidence. It was held that the incompleteness of the trace printouts goes to the sufficiency rather than the admissibility of the prosecution evidence.

It was held that the computer printouts were admissible into evidence and did not infringe the hearsay rule. The reasoning followed the principle expounded in *R v Wood*[95] that where a computer is used as a calculator and its programming and use are both covered by oral evidence, the printout produced is not hearsay evidence.

(2) Where the computer automatically recorded data that is not supplied by any human source.

In *Rook v Maynard*[96], Wright J held that unlike a print-out of a bank statement which, except for the final print-out, relies upon the accuracy of each operator who has caused transactions to be recorded and which is therefore plainly almost entirely hearsay in content, the operation of a computer trace program is totally devoid of any such human hearsay element and is therefore admissible.

5.2 Reliability

Courts have expressed significant difficulty with accepting the reliability of electronic documents. The common, and perhaps somewhat misguided view, appears to be that documents in electronic form are less secure than paper documents.[97] Courts have applied this view to justify

higher standards of reliability required of electronic evidence than is required of paper documents.[98] As Laryea points out, "while the security concerns about electronic data are legitimate, it must be borne in mind that paper documents are equally insecure."[99] "Paper documents can rather easily be forged, misassembled, misdirected, changed and lost".[100]

It is interesting to note that in order to make a determination as to the reliability of the electronic evidence in *Rook v Maynard*[101], both the Magistrate and Judge on Appeal made trips to the DSS to view the Department's information systems and the manner in which the relevant trace program operated.

6. Increasing obligations for organisations

6.1 The NSW Police: Future directions 2001-2005

Senior officials have indicated that organisations will play an increasing role in this area in the future. Recently, the NSW Police Service proposed a legislative process whereby the police service sets standards, provides advice and monitors performance. Under this scheme, organisations use their own resources to prevent, detect, investigate and prepare evidence. Briefs are then submitted to police or the DPP for further investigation. The proposal is driven by the cost of fraud resistant systems, forensic accounting and skilled employee drainage. Irrespective of whether such proposals actually get implemented, organisations would do well to ensure digital evidence gathering protocols are in place.

6.2 What can management do to ensure its computer evidence will be admitted?

The necessity to rely upon electronic evidence will inevitably increase as advances in technology move us further away from a paper-based society. Evidential rules were traditionally created for, and accordingly, are more suited to, paper records and documents. Faced with this position and the likelihood of increasing numbers of e-security breaches, businesses must adopt appropriate measures to ensure that computer evidence will be admissible.

In addition to hearsay and reliability issues posing an obstacle to the admission of computer evidence, such evidence may not be admitted if there are concerns about its integrity. The process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable (known as forensic computing) is important in this regard.[102] Chain of custody issues relevant to paper evidence will also be relevant to computer evidence. Electronic evidence must be preserved wherever possible and where changes are inevitable, an explanation of the nature and reason for the change must be available to the court.[103]

Any company involved in an action where a breach of e-security has been alleged, should have in place policies and procedures to ensure its computer evidence will be admitted in court. Issues that these policies and procedures should cover, include:

- physical steps to quarantine evidence;
- recovery of evidence;
- reproduction of evidence;
- processing and analysis of evidence; and
- generation of a report regarding the evidence by an expert for use in court.

This process should proceed in a manner that guarantees that:

1. there is a minimum handling of the original evidence;
2. any changes in the evidence are accounted for;
3. the rules of evidence have been complied with; and
4. experts do not exceed their knowledge.

If these steps are taken in accordance with acceptable industry practice, a company will have a much better chance of proving its case or disproving the other side's case in any trial.

7. Conclusion

The new open network architecture of information systems has given rise to greater vulnerabilities in the security and integrity of these systems. These vulnerabilities expose organisations to great risks, particularly in relation to unauthorised use and access by the organisation's own personnel.

While it may be the employees that face criminal prosecution for these breaches, employers may incur civil liability if the breaches result in loss or damage to third parties. In addition, if there are imprecise access controls in place, employers may find themselves subject to a claim of unfair dismissal by the very employee who allegedly committed the breach if the employee is terminated in a manner which contravenes the law. There can be significant costs to an organisation when their network security is compromised, both in financial terms and in terms of the organisation's reputation and image and business recovery costs.

In light of these concerns, it is clear that the protection of data within these systems is an important consideration for management and that these issues should be addressed with strategies appropriate to the security needs of the particular organisation. This necessarily involves the implementation of security policies that include both procedural and technological safeguards. An effective security policy will put in place measures that are targeted at prevention, ongoing monitoring and recovery strategies in the case of breach.

---

1 Over 90 percent of global chief executives and chief information officers believe a breach of their computer systems would be perpetrated through the internet or other external means according to a survey of 1,283 companies by the accounting firm KPMG. See *KPMG: Biggest Threat to Data From Insiders*, Reuters, 30 March, 2001 at http://news.zdnet.co.uk/story/0,,s2085405,00.html

2 *Study: Cybercrime Continues to Boom* at http://www.e-commercetimes.com/perl/story/?id=2795

3 See supra n1 "most security breaches are committed by individuals who possess intimate knowledge of the systems they are attacking".

4 See *Fact Sheet: Cyberspace Crime* at http://www.oznetlaw.net/facts.asp

5 In one case, employee Timothy Lloyd was convicted of planting a 'bomb' on Omega Engineering's computer system after he found out he was about to be fired. The 'bomb' systematically erased all of the

company's contracts, as well as proprietary software used by the company's manufacturing tools causing an estimated US$12 million damage.

6 The term 'crackers' is used to refer to people who intentionally seek access to computer systems or networks with dishonest or fraudulent intentions (eg to alter data for financial gain) as opposed to "hackers" who have more noble intentions.

7 See Dorothy E. Denning, *Information Warfare and Security*, ACM Press, New York, 1999.

8 Each jurisdiction's criminal legislation contains provisions which establish that attempts to commit certain offences are themselves offences: *Criminal Code Act 1995 (Cth)*, section 11.1; *Crimes Act 1900 (ACT)*, section 347; *Crimes Act 1900 (NSW)*, section 344A; *Criminal Code (NT)*, sections 277-279; *Criminal Code (Qld)*, sections 535-538; *Criminal Law Consolidation Act 1935 (SA)*, sections 270a-270ab; *Criminal Code (Tas)*, section 299; *Crimes Act 1958 (Vic)*, sections 321M, 321O-P, *Criminal Code (WA)*, sections 552, 554-555A.

9 Section 149 of Schedule 2 of the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000 (Cth).*

10 Sections 131-5 and sections 143-145.

11 Under the old section 76B(1), a person was guilty of an offence if he/she intentionally and without authority obtained access to or damaged data stored in a Commonwealth computer or data stored in a non-Commonwealth computer on behalf of the Commonwealth.

12 The *Cybercrime Act* is to commence on a day to be fixed by Proclamation or, if a date is not so fixed, on the first day after the end of the period of 6 months beginning on the day of Royal Assent. As yet no date has been fixed for commencement of these provisions.

13 See section 154 of Schedule 2 of the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000 (Cth).*

14 *Criminal Code Act 1995 (Cth),* sections 131.1, 134.1 and 135.1.

15 See also the definition of "document" in section 143 of the Code which includes "any article or material (for example, a disk or a tape) from which information is capable of being reproduced with or without the aid of any other article or device." The definition of "information" under section 143.1 is also pertinent: "information means information, whether in the form of data, text, sounds, images or in any other form." .

16 Section 134.1 of the *Criminal Code Act 1995 (Cth).*

17 Id., sections 143 and 145. Note that in section 145, the definition of forgery includes "to dishonestly cause a computer, a machine or an electronic device to respond to the document as if the document were genuine".

18 Under section 477.2(1)(d)(iii) of the new Commonwealth *Criminal Code Act 1995 (Cth)*, unauthorised modification of data to cause impairment that involves a telecommunications service (eg the internet) constitutes an offence under Federal jurisdiction concurrent to any State or Territory offence. This is subject of course to the operation of s 109 of the Constitution and related case law: see for example: *R v Credit Tribunal; Ex parte General Motors Acceptance Corp, Australia* (1977) 137 CLR 545 and *Bond v R* (2000) 201 CLR 213.

19 Section 51 of the *Constitution*

20 See section 4 of the *Cybercrime Act (Cth) 2001*

21 Division 476.1(1) of the Commonwealth *Criminal Code Act 1995 (Cth)*

22 No. 60488 of 1995.

23 Ibid.

24 Reference was made to Hayne J's judgment in *DPP v Murdoch* [1993] 1 VR 406 which is discussed below.

25 See the definition of "property" in the definitions section of the *Crimes Act 1900*: "property includes every description of real and personal property; money, valuable securities, debts, and legacies, and all deeds and instruments relating to, or evidencing the title or right to any property, or giving a right to recover or receive any money or goods, and includes not only property originally in the possession or under the control of any person, but also any property into or for which the same may have been converted or exchanged, and everything acquired by such conversion or exchange, whether immediately or otherwise.".

26 *Summary Offences Act 1966 (Vic)*, section 9A; *Summary Offences Act 1953 (SA)*, section 44; *Crimes Act 1900 (ACT)*, section 135J; *Criminal Code Act 1913 (WA)*, section 440A; *Criminal Code 1995 (Qld)*, section 408D(i); *Criminal Code 1924 (Tas)*, section 257D.

27 Section 310 of the *Crimes Act 1900 (NSW).*

28 Id., section 390; see also Part 4 Div 1.

29 See *Crimes Act 1900 (NSW)*, Part 4; *Criminal Code Act 1913 (WA)*, section 409; *Crimes Act 1958 (Vic)*, sections 80A – 83A; *Criminal Code 1995 (Qld)*, section 408C; *Crimes Act 1900 (ACT)*, section 104.

30 *Crimes Act 1900 (NSW)*, section 178BA(2)(b)(1).

31 No.20 of 2001.

32 [1993] 1 VR 406.

33 Id., at 410.

34 [2000] HCA 61.

35 (1985) 157 CLR 424.

36 In *Smith v Leurs* (1945) 70 CLR 256; (1945) 51 ALR 392; (1945) 19 ALJR 230, Dixon J pointed out that a 'special relationship' of this kind might arise in reference to things involving a special danger and the control or of actions or conduct of the third person. See *Modbury Triangle Shopping Centre Pty Ltd v Anzil* [2000] HCA 61, para 140.

37 No. 50549 of 1990.

38 Id., at 358.

39 *Broom v Morgan* [1953] 1 QB 597.

40 See the *Employees Liability Act 1991 (NSW).*

41 See *Century Insurance Co Limited v Northern Ireland Road Transport Board* [1942] 1 All ER 491; and *Tiger Nominees Pty Limited v State Pollution Control Commission* (1992) 25 NSWLR 715, at 721 per Gleeson CJ.

42 *Tiger Nominees Pty Limited v State Pollution Control Commission* (1992) 25 NSWLR 715.

43 *Bugge v Brown* (1919) 26 CLR 110, at 117 per Isaacs J.

44 See unreported decision in *Warne and Others v Genex Corporation Pty Ltd and Others* — BC9603040 — 4 July 1996.

45 *[1912] AC 716*

46 Lord Shaw of Dunfermline said at 739: "the loss occasioned by the fault of a third person in such circumstances ought to fall upon the one of the two parties who clothed that third person as agent with the authority by which he was enabled to commit the fraud."

47 *(1949) 79 CLR 370 at 381*

48 See, for example, *Simon Richard Lane v The Commonwealth Bank of Australia [2000] NSWIRC 274 (15 December 2000).*

49 See for example *R.A. Bauer and Australian Taxation Office [U No 40217 of 1997]; Helen Utting and Commonwealth of Australia - Department of Social Security (U No. 20099 of 1997); Dean Uink and Department of Social Security (U No. 60032 of 1997).*

50 See Part 6 of the *Industrial Relations Act 1996 (NSW).*

51 Id., section 170CG(3).

52 U No. 20099 of 1997.

53 See judgment of Northrop J in *Selvachandran v Peteron Plastics Pty Ltd (1995-96) 62 IR 371*

54 FCA 441 (7 April 2000)

55 Defined in the Actto include individuals, bodies corporate, partnerships, unincorporated associations and trusts.

56 National Privacy Principle 4 – "Data Protection".

57 See *R v Stevens [1999] NSWCCA 69 (15 April 1999).*

58 See *Hospital Products Ltd v United States Surgical Corp (1984) 156 CLR 41 at 96.*

59 Section 180 of the *Corporations Act 2001*: "A director or other officer of a corporation must exercise their powers and discharge their duties with the degree of care and diligence that a reasonable person would exercise"

60 See section 64 of the *Corporations Act 2001.*

61 Id., section 180.

62 The right to bring civil proceedings is preserved by section 185 of the *Corporations Act 2001.* Under general law, a breach could give rise to a claim for monetary compensation for any loss caused by the breach. The basis of a claim under general law could, in the case of any director, be the duty of care and diligence arising from common law negligence or equitable obligation. In the case of an executive director it could be a breach of the employment contract. For any director it could be a liability to pay compensation on the basis of a tort for breach of statutory duty: *Dominion Insurance Co of Australia Ltd v Finn (12 December 1987, SC(NSW),* Hodgson J, No 1308/1984, unreported).

63 Ibid.

64 [1972] AC 153, at 170 per Lord Reid.

65 See *Pearks, Gunston & Tee Limited v Ward* [1902] 2 KB 1,.at 11 per Channell J, and *Mousell Bros Limited v London and North-Western Railway Company* [1917] 2 KB 836, at 843 per Viscount Reading CJ.

66 See *Mousell Bros Limited v London and North-Western Railway Company* [1917] 2 KB 836, at 845 per Atkin J.

67 [1995] 2 AC 500.

68 Id., at 507.

69 Dorothy E. Denning, *Information Warfare and Security*, ACM Press, New York, 1999.

70 See Tomas Olovsson, *A Structured Approach to Computer Security*, Department of Computer Engineering Chalmers University of Technology, Gothenburg SWEDEN, Technical Report No 122, 1992 at <http://www.ce.chalmers.se/staff/ulfl/pubs/tr122to.pdf>

71 An audit trail, for example, is a log containing security-related events and transactions. It contains information about when, how and by whom a transaction was ordered, thus it is a valuable tool for protecting both objects and the integrity of entities.

72 Within a system, objects can be protected by an access control mechanism which mediates all accesses to objects and controls the way in which entities can use them. The basic components of an access control mechanism are entities, objects and access rights. The access rights describe entity privileges and state under what conditions entities can access an object and how these entities are allowed to access the object.

73 For a story that brings home the importance of these types of measures, see Roderick Campbell, "Consultant Motivated by Greed, Court Told", Canberra Times, 24/04/2001, which describes how a Canberra consultant defrauded the Commonwealth (DOFA) of $8.735 million by exploiting the fact that staff at DOFA had shared individual log-on codes and passwords.

74 For a current version of this list visit http://www.dsd.gov.au/infosec/

75 Security experts claim that 80% of all security breaches could be prevented if software patches and updates are applied when they are first available. See Will Garside, *FBI Warns Failure to Implement Patches Causes Most Security Breaches*, Computer Weekly.com, 29 March 2001.

76 Interested readers may wish to consult the following publications: AS/NZS 4360:1999 Risk management; HB 231:2000 Information security risk management guidelines; and HB 240:2000 Guidelines for managing risk in outsourcing utilizing the AS/NZS 4360 process.

77 See Schneier, B., *Secrets & Lies: Digital Security in a Networked World*, (2000) John Wiley & Sons Inc, New York, 301-302.

78 This is based on the cost of hiring consultants to identify what occurred, the recovery of lost data and so forth.

79 While the quantitative approach or other approaches incorporating an element of quantitative analysis have their supporters, some commentators have openly criticised them: see Power, R., *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace*, Que Corporation, Indianapolis, 2000, at 283-284. See Schneier, B., *Secrets & Lies: Digital Security in a Networked World*, (2000) John Wiley & Sons Inc, New York, 301-302.

80 Power, R., *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace*, Que Corporation, Indianapolis, 2000, at p283-284.

81 Lori Enos, *Lloyd's of London to offer Hacker Insurance*, E-Commerce Times, July 10, 2000. See also Keith Regan, *Hacker Insurance? Buy a Boatload*, E-Commerce Times, July 14, 2000.

82 Ibid.

83 Paul A. Greenberg, *Hacker Attacks Will Bring Profits to Insurance and Security Firms*, E-Commerce Times, February 11, 2000

84 Lori Enos, *Report: Cybercrime Outpacing Security Spending*, E-Commerce Times, October 6, 2000

85 See Mark Grossman, *The Importance of Technology Insurance and How to Buy It*, http://www.gigalaw.com/articles/grossman-2000-07-p1.html

86 See *Does Your Company Need Hacker Insurance?*, at: http://www.gigalaw.com/articles/2001/wood-2001-06-p4.html

87 See section 59 of each Act.

88 See section 69 of each Act.

89 See section 147 of the Acts.

90 See for example, section 55B (8) of the *Evidence Act 1958 (Vic)*; section 59a of the *Evidence Act 1929 (SA)*; and section 95(7) of the *Evidence Act 1977 (Qld)*.

91 And may not satisfy the requirements of the computer-specific exception in the relevant States.

92 It is unclear whether this evidence is considered to be not within the ambit of the hearsay rule – see *Rook v Maynard (1993) 126 ALR 150* or an exception to the hearsay rule see eg. *Mehesz v Redman (1981) 26 SASR 244.*

93 See Laryea, T. *The Evidential Status of Electronic Data (1999) NLR 3* at http://web.nlr.com.au/nlr/HTML/archive/laryea/laryeatxt.htm

94 *(1993) 126 ALR 150.*

95 *(1982) 76 Cr App R 23.*

96 Supra, note 95.

97 Supra, note 96 at 11.

98 Id., at 13.

99 Supra, note 94.

100 Supra, note 94 also see Wright B and Winn J K, *The Law of Electronic Commerce*, (3rd edn, 1998) Aspen Law & Business, New York.

101 Supra, note 95.

102 McKemmish, R. *What is Forensic Computing?* Trend and Issues in Crime and Criminal Justice. June 1999. Australian Institute of Criminology: Canberra.

103 Ibid.