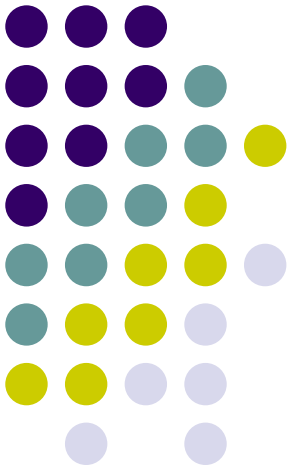
Cyber Crime & Information Security

A Legislative Regime

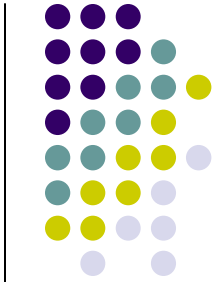
Dr. Adrian McCullagh

Information Security Institute

Queensland University of Technology



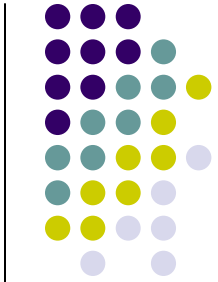
Agenda



- Introduction
- Telecommunications
- Cyber crimes Act
- Federal Criminal Code
- Queensland Criminal Code
- Privacy Issues
- Conclusion

Introduction

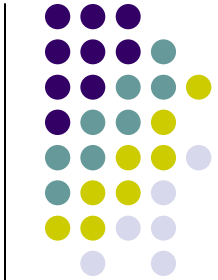
Promoting a Culture of Cyber Security



- The Australian Federal Government in recent years have undertaken a number of steps in promoting a culture of cyber security.
- These steps have included:
  - The establishment of a Trusted Information Sharing Network that comprises various parties and industry associations directly involved with Critical Infrastructure;
  - The enactment in 2001 of the Cyber Crimes Act which substantially improved the legal basis covering cyber crimes;
  - The extension of the Privacy Act in 2001 to cover more private organisations that hold personal information;
  - The enactment of the Federal Criminal Code especially division 12 which covers “corporate Culture of Non-compliance” with Federal, State or Territory Laws.
  - The recently published “Security Breach Disclosure Guidelines” by the Privacy Commissioner.

Introduction

Promoting a Culture of Cyber Security



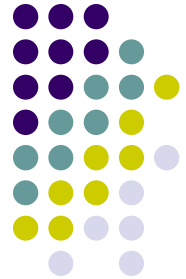
- There are two principal difficulties in developing a national approach in Australia for promoting Cyber Security:
  - Federated Environment : the Federal Government must operate within the scope of the Australian Constitution which at time can be restrictive in developing a national approach;
  - In many industry sectored covering Critical Infrastructure the relevant infrastructure is owned by private organisations. For example,
    - the Banking system,
    - Telecommunications infrastructure,
    - most transport is either privately owned or operated by Government Owned Corporations,
    - in some states the electricity network is privately owned whilst in other states it is owned by Government Owned Corporations.

Introduction

Promoting a Culture of Cyber Security

- Fortunately the Commonwealth does have legislative power to regulate:
  - Telecommunications;
  - Banking.
- Unfortunately, the Commonwealth does not have direct power to regulate the Power Industry, but there has been some movement in this arena through the enactment and adoption by the State of the National Electricity Law.

Telecommunications Act 1997



- **Section 313 Obligations of carriers and carriage service providers**

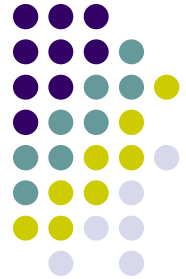
  (1) A **carrier or carriage service provider** must, in connection with:

  (a) the operation by the carrier or provider of **telecommunications networks** or **facilities**; or

  (b) the supply by the carrier or provider of **carriage services**;

  do the carrier's best or the provider's best **to prevent telecommunications networks and facilities from being used in**, …, the **commission of offences** against the laws of the Commonwealth or of the States and Territories.

Telecommunications Act 1997

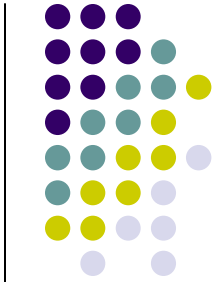


- **Applies to Carriers and Carriage Service Providers**
- **Carriage Service providers include ISP and content management providers.**

Telecommunications Act 1997

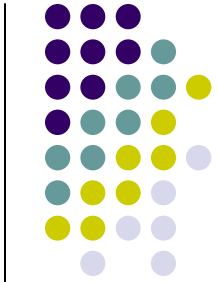
- **“do its best” : What do these words mean?**
  - **Kendall v. Telstra**
    - **Probably means do what is reasonable in the circumstances.**
  - **Could it apply to say a denial of service attack which would be a crime under the Cybercrimes Act?**
  - **Do carriers have an obligation to protect clients from such attacks?**
  - **Do Consumers have a obligation to take reasonable actions to better protect their own systems against illegal activity.**

CyberCrime Act



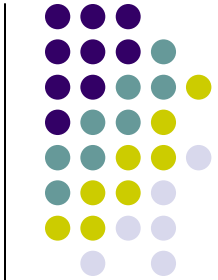
- 15th December 2001
- **Unauthorised access**, **modification** or **impairment** of **data** or **electronic communications** :
  - now a Federal Offence

CyberCrime Act



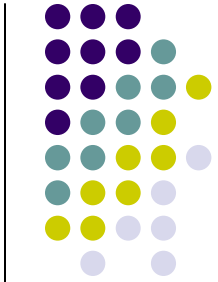
- Accomplice provisions - “conduct substantially contributing to” the occurrence of the offence
- An offence will occur if there is unauthorised access through Telecommunications Service or unauthorised access to a Commonwealth computer.
- A commonwealth computer is any computer that is owned or controlled by the Commonwealth or hold commonwealth data.

Cybercrime Act



- Telecommunications services means a service for carrying communications by means of guided or unguided electromagnetic energy or both.
- Impairment of communications is meant to cover a denial of service attack.
- Issue: does it cover a distributed denial of service (DDOS) attack.
- DDOS occurs when a botnet is secretly placed upon an unsuspecting computing and then remotely activated to form part of a distributed attack upon a target computer.

Regulatory Obligations Corporate Culture Offences



- Company criminally liable for offences committed by employees, where the company has a "corporate culture of non-compliance" to Commonwealth Laws
- Strict liability for "tolerating" non-compliance

- Positive duty to create and maintain a culture of compliance with commonwealth laws. - Corporate Compliance Program
- Similar to Internal Audits and External Audits for Financial records

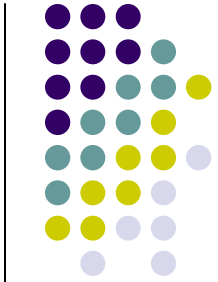
Queensland Criminal Code

- Section 408D
  - (1) A person who uses a restricted computer without the consent of the computer's controller commits an offence.
  - Maximum penalty--2 years imprisonment.
  - (2) If the person causes or intends to cause detriment or damage, or gains or intends to gain a benefit, the person commits a crime and is liable to imprisonment for 5 years.

Queensland Criminal Code

- Section 408D
  - (3) If the person causes a detriment or damage or obtains a benefit for any person to the value of more than $5 000, or intends to commit an indictable offence, the person commits a crime and is liable to imprisonment for 10 years.

Queensland Criminal Code



- Section 408D
  - "damage" includes--
  - (a) damage to any computer hardware or software; and
  - (b) for information--any alteration, addition, removal or loss of, or other damage to, information.

Queensland Criminal Code

- Section 408D
- "**restricted computer**" means a computer for which--

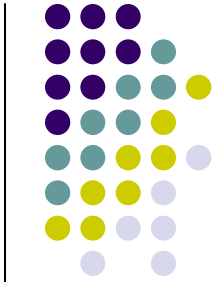
(a) a device, code or a particular sequence of electronic impulses is necessary in order to gain access to or to use the computer; and

(b) the controller--

(i) withholds or takes steps to withhold access to the device, or knowledge of the code or of the sequence or of the way of producing the code or the sequence, from other persons; or

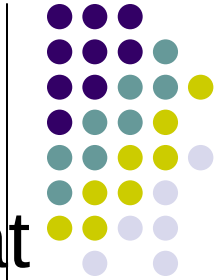
(ii) restricts access or takes steps to restrict access to the device or knowledge of the code or of the sequence, or to the way of producing the sequence, to a person or a class of person authorised by the controller. .

Information Assets



- "Information is valuable, but knowledge is neither real nor personal property. A man with a richly stored mind is not for that reason a man of property. Authorities which relate to property in compositions,… belong to the law of copyright and have no bearing upon the question whether knowledge or information, as such is property".
  - Per Latham CJ. : FCT v. United Aircraft Corp.

Information Assets

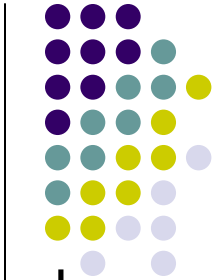


- “ Either all knowledge is property, so that the teaching of, for example, mathematics involves the transfer of property, or only some knowledge is property. If only some knowledge is property then it must be possible to state a criterion which will distinguish between that knowledge which is property and that knowledge which is not property.” Latham CJ
  - FCT v. United Aircraft Corp.

Information Assets

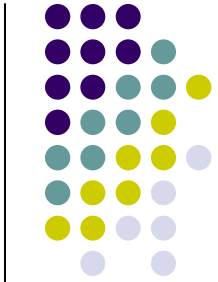
- So is it possible to identify the elements that support the position that some information can be property.
- Latham CJ. Rejected the element of secrecy.
    - **Points about this case**
- 1943 case
- The case is a pre-Information revolution/computer case
- The dependence on information had not developed

Information Assets



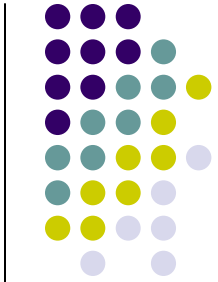
- Pont Data Case:
  - The Federal Court recognised the value of information and specifically noted that commerce was now absolutely dependent upon information and the integrity of that information.
  - NOTE THE EMPHASIS ON THE INTEGRITY OF THE INFORMATION
  - See also Hepples v. FTC
  - Smith Klein and French v. Federal Department of Community Services and Health
  - Different position in other jurisdictions such as:
    - Hong Kong : Koo case
    - USA : Carpenter v. US

Management Responsibility



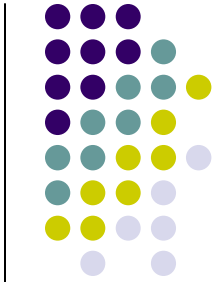
- At Common law Management has a fiduciary responsibility to act in the best interests in the Company.
- Traditionally this has primarily concerned protecting the corporation's property.
- BUT THINGS HAVE CHANGED
- Property is no longer the issue; the issue now concerns ASSETS of the corporation
- This is a much wider term "ASSETS". And will include information.

Security Breach Guidelines



- Guidelines only apply where personal information is the subject of the breach;
- No civil liability applies;
- Substantially follows the Canadian approach which is partially based upon the Californian enactment of 2003.
- Based on Shame Factor
- In California notices to Secretary of Commerce for California are made public via a web site.

Conclusion



- Law is still developing in this arena;
- Privacy could be a substantial issue in raising awareness for security culture;
- Data Breach disclosure could be the answer but too early to tell.