MGTS1201

For Final Exam (Lecture 5-12)

LECTURE 5 (Chapter 6 and 7)

Case Study: Big Brother Watching You Work (Pg 182-183)

ETHICAL ISSUES

A. Ethics: Principles of right and wrong that individuals use to make choices that guide their behaviour (define socially acceptable behaviour)
B. Different from law
C. Laws: Rules that mandate or prohibit certain societal behaviour
D. Laws carry sanctions of a governing authority, ethics usually do not
E. Most organisations develop and formalise a body of management views/expectations called 'policy'
F. Policies serve as organisational laws - the view of management

ETHICAL STANDARDS

Utilitarian Approach An ethical action is the one that provides the most good or does the least harm.	**Rights Approach** An ethical action is the one that best protects and respects the moral rights of the affected parties.
Fairness Approach An ethical action treats all humans equally, or if unequally, then fairly, based on some defensible standard.	**Common Good Approach** An ethical action is the one that best serves the community as a whole and is important to the welfare of everyone, not just some members.

ETHICS IN THE CORPORATE ENVIRONMENT

A. Code of Ethics: a collection of principles that are intended to guide decision making by members of an organisation
B. Fundamental tenets of ethics:
   - Responsibility: accepting the consequences of your decision and actions
   - Accountability: determining who is responsible for actions that were taken
   - Liability: a legal concept that gives individuals the right to recover the damages done to them by other individuals, organisations or systems

IT LAW - INCLUDING PRIVACY LEGISLATION

A. Telecommunications Act 1997
   - Prohibits breaches of privacy in telecoms traffic
   - Exemptions made for police-obligations on ISPs
B. Cybercrime Act 2001
   - Unauthorised access, modification or impairment with intent to commit a serious offence
   - Possession or control of data with intent to commit a computer offence
   - Producing, supplying or obtaining data with intent to commit a computer offence
C. Spam Act 2003
   - Three steps:
     - Consent
     - Identity
     - Unsubscription
D. Privacy Act 1988
   - 10 Principles:
     - Collection
     - Data Quality
     - Openness

- Use and disclosure
- Transborder Data Flows
- Private Sector Coverage
- Data Security
- Sensitive Information
- Access and Correction
- Targets Public Sector

E. Copyright Act 1968
   - Protects the expression of ideas in all forms: artistic media, as well as computer programs
F. Surveillance devices bill 2004: Regulates the use of surveillance devices (data, optical, listening and tracking devices) by law enforcement agencies

(Red means more important)

INTRODUCTION TO INFORMATION SECURITY

A. Security: the degree of protection against criminal activity, danger, damage, and/or loss
B. Information security: Protecting an organisation's information resources from unauthorised access, use, disclosure, disruption, modification or destruction
C. Threat (to an information resource): any danger to which a system may be exposed
D. Exposure (of an information resource): the harm, loss or damage that can result if a threat comprises that resource
E. Vulnerability (of an information resource): the possibility that the system will be harmed by a threat

THREATS TO IS

- Threat types:
  a) Outside
  b) Inside
     - Very frequent
  c) Intentional
     - Theft (inc. identity)
     - Extortion
     - Social Engineering
     - Int property
     - Software
     - Cyberterrorism
  d) Unintentional
     - Human Errors

DELIBERATE THREATS

- Software attacks
  e) Remote attack needing user action
     - Virus: introduced via email, disk transfer etc. - designed for malicious purposes - attaches to a host computer/file and runs every time that file is run/executed
     - Worm: very similar to virus software with one major difference - worms are designed to spread (e.g. by reading email address books)
     - Phishing attack: masquerade as official-looking emails
     - Spear-Phishing attack: Phishing attack on specific target
  f) Remote attack needing no user action
     - Denial-of-service (DoS) attack: bombarding a server and denying its use to legitimate users
     - Distributed DoS attack: using multiple hacked computers (zombies) to perform 'massed' DoS attack from the internet
  g) Attack by Programmer Developing a system
     - Trojan horse: disguised as an innocent program - may well do some good but also contains malicious logic