IT Applications: VCE Information Technology Units 3 & 4

Chapter 7: 'Storage, Communication and Disposal of data and information'

Test Your Knowledge answers

Organisational goals

1 Explain the difference between an organisational goal and a mission statement.

2 How does an information system support an organisational goal?

3 Apart from making a profit, think of an organisational goal for each of the following types of organisations:

- **(a) a veterinary clinic**
- **(b) a large shopping centre**
- **(c) an airline**
- **(d) a brewery**
- **(e) a public library.**

1 The mission statement explains what the company is trying to achieve, whereas an organisational goal explains how the organisation will achieve its mission.

2 Information systems are designed to assist the company in achieving organisational goals. An information system itself has its own goal, known as the system goal. The system goal explains how the system will help achieve the organisational goal.

3 There are several possibilities for this, but a possible goal for each one may include:

a) A veterinary clinic: To provide the best care for sick animals and heal them as quickly as they can.
b) A large shopping centre: Having the lowest prices and widest range of shops in the country.
c) An airline: Increase the number of flights departing within a minute of their scheduled time.
d) A brewery: To provide the best tasting, widest range of beer available.
e) A public library: Increase the number of new books available to patrons.

Legal requirements

1 Explain why an organisation must comply with legal requirements.

2 Briefly summarise the role and scope of the four key laws affecting privacy of information.

3 Why have these laws been introduced?

4 If you believe that the privacy of your information has been breached by the Taxation Office, to whom can you complain?

5 What are the penalties for breaches of the Information *Privacy Act 2000*?

6 What is the *Copyright Amendment (Digital Agenda) Act 2000* designed to protect?

7 What is a code of practice?

8 For each breach of privacy below, suggest under which privacy law it would be covered:

- **(a) You find that your employer has published your tax file number on the Internet.**
- **(b) Medical records are found at the tip.**
- **(c) A bank refuses to give you a loan because the manager claims your credit record is poor, when it should actually be very good.**
- **(d) A consultant working for the Victorian government passes on your VCE results to a friend without your permission.**
- **(e) A website you visit asks for personal information from you, but does not display its privacy policy.**
- **(f) A friend makes a copy of a music CD for you.**

1 Laws passed by the state and federal government place certain responsibilities with organisations. If organisations fail to comply with a law they can be taken to court. Organisations can be fined and directors imprisoned if found guilty of certain crimes.

2 Privacy Act 1988: This law safeguards personal information held by federal government departments, use of tax file numbers and people's credit details.

Privacy Amendment (Private Sector) Act 2000: Extends the provisions of the Privacy Act to include the storage and handling of personal information by non-government organisations.

Information Privacy Act 2000: Outlines the privacy obligations of Victorian state government agencies and contractors working for the government. The Act covers the same broad areas as the federal Privacy Act 1988, although it is customised to suit the Victorian Public Sector.

Health Records Act 2001: The Victorian Government passed the Health Records Act 2001 with the intention of protecting patient's medical information. It was introduced separately to the Information Privacy Act described above because it covers both public and private medical sectors.

3 These laws have been introduced in order to control how personal information is acquired (collected), handled and stored by both government and non-government organisations. They have become necessary because of the public concern over just what information was being collected about people and how it was being used.

4 You can complain to the Federal Privacy Commissioner if you believe that the Australian Tax Office has breached your privacy.

5 A Compliance Notice may be issued to organisations that do not observe the provisions of t he Privacy IPA. Maximum penalties for non-compliance currently range from $300,000 for organisations and $60,000 for non-corporate offences.

6 The Copyright Amendment (Digital Agenda) Act 2000 is designed to protect intellectual property which is in an electronic form. Examples include software and other electronic works.

7 When the government creates a new law, they will also release a set of guidelines which suggest ways in which people can comply with those laws. The guidelines are called Codes of Practice.

Whilst an organisation does not have to follow a government issued Code of Practice, it needs to create its own and ensure that it follows the laws on which it is based.

8 Breaches would be covered under the following Acts:

a) Privacy Act 1988
b) Health Records Act 2001 (assuming they came from a local hospital)
c) Privacy Act 1988
d) Information Privacy Act 2000
e) Privacy Amendment (Private Sector) Act 2000
f) Copyright Amendment (Digital Agenda) Act 2000 (obviously a breach of copyright rather than privacy)

Ethics

1 Explain how ethical requirements differ from legal requirements.
2 What are some responsibilities that employers and employees have to one another?
3 What is the purpose of a code of conduct?
4 How is employee monitoring justified?
5 In your view, is employee monitoring ethical or unethical? Explain your answer.
6 Why is a company computer use policy important?
7 What type of ethical restrictions can be applied to the Internet?

1 Ethics relates to behaving in ways which are based on our morals and accepted standards. Whilst acting unethically might be morally questionable, it is not against the law.

2 An employer is expected to pay employees for their labour and provide a safe work environment. In return, an employee is required to work in the interests of the organisation for the duration of time they are being paid.

3 A code of conduct explains the behavior expected of an employee.

4 Employee monitoring is justified to ensure that a high standard of service is being provided to customers and that the employees are doing company work during company time.

5 It depends on your point of view as to whether or not employee monitoring is unethical. Question 15, above, has some reasons in favour of monitoring. People who oppose employee monitoring say that it often invades the privacy of employees because it can be very intrusive if every aspect of the working day is being tracked.

6 A company computer use document is similar to a code of conduct in that it outlines what behaviour is considered acceptable with regard to computer use within the organisation.

7 The key ethical restriction which can be applied to the Internet is Netiquette (net etiquette).

Threats to information

1 What are some possible consequences if data security is violated?
2 List some common threats to data that is stored, communicated or disposed of by organisations.
3 Explain the term 'unauthorised access'.

4 Describe how a computer virus might work.

5 How do hackers and crackers differ?

6 What are some methods by which files can be tampered with?

7 How does theft of hardware differ from theft of information?

8 What are common forms of user error?

9 Explain why file extensions and descriptive filenames are important.

10 How can equipment failure lead to loss of data?

1 Some possible consequences resulting from the violation of data security include breaches of privacy, loss of intellectual property and loss of income due to unavailability of information or services.

2 Common threats to data which is stored, communicated or disposed of by organisations include: intentional damage through the creation and spreading of computer viruses, hacking or cracking, tampering with files, information theft and vandalism or theft of hardware. Accidental damage can be caused by user error, failure to follow file-management procedures and equipment failure or damage.

3 Unauthorised access involves the use of a computer or a network without permission.

4 A computer virus may infect boot sectors of a computer or affect individual files. It can cause loss of data by deleting or altering files or running the hardware until it fails. Email viruses typically send messages to addresses in the address book in order to clog email servers. The action of a virus is called its payload.

5 Hackers gain unauthorised access to electronic information systems and may view data, but will not tamper with it. Crackers on the other hand, break into systems with the intention or stealing or damaging the data in some way.

6 Files can be altered by crackers who break into a system. Files can also be changed by personnel who have access rights to the system, but might be selling the information to someone else. Files can also be intercepted whilst being transmitted.

7 Information theft involves the stealing of data. This can be done from a remote location. Theft of hardware involves the physical removal of hardware from an organisation. The hardware may also contain data of course.

8 Common forms of user error can include copying an older version of a file over a newer version, formatting a disk containing important data or corrupting files by not correctly shutting-down hardware.

9 File extensions and descriptive file names are important because it reduces the possibility of losing data due to user error. It also makes it easier to locate certain files and identify different versions of documents.

10 The failure of hardware which may store or manipulate data, like the hard disk, CPU or RAM, may lead to the loss of data because these devices are critical to the operation of the computer. Likewise, if software fails to save or manipulate data correctly, corruption or loss of data can occur.

Consequences of violating security and privacy measures

1 How do consequences differ from penalties?
2 What are some consequences of the loss of intellectual property?

1. A consequence is some kind of flow on effect resulting from an action. For example, loss of revenue for a musician might be a consequence of their CDs being pirated. On the other hand, a penalty is a punishment like a fine or imprisonment.

2. When intellectual property is stolen the main impact is financial. As noted in the previous answer, the property owner misses out on revenue and the government may lose tax revenue.