Security

National 4 and 5

Administrative Practices

SECURITY in a business is all about **taking steps** to try and **MINIMISE RISKS** to the people, property and information in the workplace.

People, property and information in a business can be put at **RISK of becoming injured, damaged or** destroyed by any of the following security risks:

- FIRE
- FLOOD
- THEFT
- ACCIDENTAL DAMAGE
- MALICIOUS DAMAGE (damage done on purpose to cause problems)

The amount of security that will be used by a business to protect itself from the above risks will depend on a number of factors such as:

- THE AREA THE BUSINESS WORKS IN (eg high crime area)
- THE VALUE OF EQUIPMENT OR INFORMATION (eg computers are very valuable)
- THE TYPE OF WORK THE BUSINESS DOES (eg banks need lots of security)

Protecting People, Property and Information

Businesses can use both **physical** and **electronic** systems to protect the **people** within the organisation, **information** that they may hold and the **property** that they own.

Questions

1. **Describe** what security is concerned with. [2]

2. **Outline** at least 4 risks to security that can occur in businesses. [4]

3. **Explain** why security is important to businesses. [2]

4. **Suggest** at least 2 factors which will influence the amount of security in a business. [2]

Physical Security Systems

Reception:

- This is a staffed area where visitors must report – this helps prevent **unauthorised** people from entering the business.

- Visitors must sign the **VISITORS BOOK** which will record when authorised visitors arrive and leave. This allows the receptionist to see who is in the business at any point in time.

This can help prevent the security problem of visitors being locked in a business by accident because nobody knew that they were still there.

Physical Security Systems

Security ID:

- **WORKERS ID BADGES** and **VISITOR BADGES** can help make sure that any unauthorised people are quickly spotted and dealt with before any problems arise.

Security Guards:

- Patrols by **SECURITY GUARDS** (and dogs) can be used to keep businesses secure (especially when they are closed).

Physical Security Systems

CCTV:

Can **DETER** (put off) people from causing problems and will record any problems as evidence for the police. Used in areas that are **very important** (eg bank vault) or not supervised (eg car park).

Alarms:

Alarms can **prevent** security issues because they may deter break ins or if they do happen detect them and signal the problem. They can also be connected to Police stations to automatically bring them to an incident.

Physical Security Systems

Cable Ties:

These are metals cables that can be used to secure equipment to walls or desks so that they cannot be easily stolen.

Security Marking:

This involves marking equipment (by **ENGRAVING**, **ULTRA VIOLET MARKER**, etc) with the details of the business so that if it is stolen it can be easily identified and returned by the police.

Physical Security Systems

Locks:

Physically locking areas will prevent unauthorised access.

- Key Locks/Swipe Card Locks

(only permitted members of staff will have keys or swipe cards)

- Security Number Locks
- Retinal or Finger print scanners
- Voice Recognition Locks

Electronic Security Systems

Activation Cards/Keys:

These pieces of security equipment **prevent unauthorised access** as they must be inserted into the computer by authorised personnel to make it work.

Back Up Procedures:

Back up procedures involve **copying computer information** to allow it to be **restored** if it gets lost due to a computer problem. Good back up procedures involve taking back-ups **regularly** and securely storing them in another location so that the original and copy cannot be easily destroyed together.

Electronic Security Systems

Virus Scanning Software:

Virus scanning software can be used to minimise the possibility of damage from a **COMPUTER VIRUS** (this is a program designed to damage or steal computer information).

Access Rights:

Access rights allow **different users** to do different things with an electronic file.

Access right are usually set up on the basis of USER IDs (and/or PASSWORDS). ***E.g. – Staff (ST) and Pupils (01)***

Encryption:

Encryption involves **converting** the information in an electronic file into a **code** that can't be read by anyone who does not have the software or access rights

Electronic Security Systems

Passwords:

A password is a code that is required to access a computer or file and so it prevents unauthorised access to electronic files.

Passwords are often used with USER IDs (***e.g. – 04surnam01***) to add even more security.

- *PASSWORDS SHOULD BE REMEMBERED – NOT WRITTEN DOWN*
- *PASSWORDS MUST BE KEPT SECRET*
- *PASSWORDS SHOULD NOT BE EASY TO GUESS*
- *PASSWORDS SHOULD BE CHANGED FROM TIME TO TIME*
- *PASSWORDS SHOULD BE A MIX OF LETTERS. NUMBERS AND SYMBOLS*

Laws

Protection of electronic information is not only important to prevent damage and loss, but in order to make sure that **LAWS** about the storage and use of electronic information are followed.

- Data Protection Act 1984 & 1998
- The Computer Misuse Act 1990
- The Copyrights, Designs and Patents Act 1998
- The Freedom of Information (Scotland) Act 2002

Data Protection Act 1984 & 1998

- Users of electronic info must register with the Government's Data Protection Registrar to say what they hold and what it is used for.

DATA USERS **MUST** FOLLOW THE **DATA PROTECTION PRINCIPLES**:

- info should be collected and processed fairly and lawfully
- info should be held only for the lawful specified purposes in the register
- info should be used only for the lawful specified purposes in the register
- info should be disclosed only to those people described in the register
- info should be adequate, relevant and not excessive
- info should be accurate and kept up to date
- info should not be passed outside the EU
- info should be held for no longer than necessary
- info should be protected by proper security

Data Protection Act 1984 & 1998

Individuals can access the data held about them and have it corrected or erased if it is wrong.

Unless the information is used for:

- preventing or detecting crime (ie police information)
- catching or prosecuting criminals (ie police or legal info)
- assessing or collecting tax or duties
- some health and social work details
- national security (eg some military information)

Data Protection Act 1984 & 1998

Individuals can contact the Registrar about data users who don't follow the guidelines. This is so that the Registrar can serve notices to correct or punish the data users actions:

- Enforcement notice (action must be taken to follow principles)
- Deregistration notice (cancels the data user's register entry)
- Transfer prohibition notice (stops transfer of data overseas)

DATA USERS CAN BE **FINED** IN COURT IF THEY **DO NOT** FOLLOW NOTICES

Computer Misuse Act 1990

- This law regulates, prevents and punishes the use of IT hardware or software for **HACKING.**

- This is the **deliberate** (and often secret) **theft** of information or malicious damage to information and hardware. This means that businesses must take steps to make sure that their **equipment is not used** for this kind of activity by workers.

The Copyrights, Designs and Patents Act 1998

This law makes it **illegal** to **copy** or **use someone** else's materials (eg software, music, books) without their permission or payment to them. In the case of IT this law is mainly concerned with preventing illegal piracy of software and so businesses must make sure that they only **use legally obtained** and licensed programs.

Freedom of Information Act (Scotland) 2002

- This law creates a GENERAL RIGHT OF ACCESS to information held by GOVERNMENT businesses ONLY – for example, local authority spending on teacher's wages.

- To access this kind of information, a person would outline the information that they would like in a FREEDOM OF INFORMATION REQUEST (**FOI Request**) and send it to the relevant Government business.

- Any person can request information under the act and there is no special format for a FOI Request. Applicants do not have to give a reason for their FOI Request.

- On receipt of a FOI Request, a Government business has to inform the applicant whether or not it holds the information they want. The Government business usually has 20 days to do this.

Freedom of Information Act (Scotland) 2002

- If the Government business does hold the required information, it will then have to communicate it to the applicant unless the FOI request is rejected for any of the following reasons:

- IT IS AGAINST THE PUBLIC INTEREST (**eg disclosing it would harm investigations**)
- IT IS TOO COSTLY (if a request will **cost more than £600 to process** it can be refused)
- IT IS **VEXATIOUS** (eg it lacks serious value, is very unreasonable, or distresses workers)

As well as the above general right of access, the Act places a duty on Government businesses to adopt and maintain pro-active PUBLICATION SCHEMES for the routine release of important information (such as annual reports and accounts). These publication schemes must be approved by the Scottish Information Commissioner.