۷۸۶
۹۲
مدینہ
بقیع

Study Notes

MANAGING PEOPLE & SYSTEM

CAT Paper

T5

by

**Mohammad Faizan Farooq
Qadri Attari**

faizanacca@yahoo.com
http://www.ffqacca.co.cc

SECTION E

SYLLABUS

Health and safety in the workplace

(a) Outline the main provisions of relevant legislation on health and safety
(b) Identify possible sources of danger to health and safety of individuals within the workplace
(c) Suggest appropriate preventative and protective measures
(d) Discuss the role of training in raising awareness of safety issues
(e) Describe safe working conditions
(f) Outline the role and responsibility of management in promoting health and safety

Security in the workplace

(a) Describe possible sources of security breaches within the workplace
    (i) identify means of physical intrusion
    (ii) describe threats related to hardware and equipment security
    (iii) explain hazards from internal and external software security breaches
(b) Outline measures for preventing security breaches
    (i) describe methods of preventing physical intrusion
    (ii) explain measures of protecting hardware and equipment
    (iii) identify strategies for reducing the risk of software security breaches

CHAPTER 17

Health and safety at work act 1974
Fire precautions act 1971
Fire safety and safety of sport act 1987
Offices, shops and railway premises act 1963

WHY HEALTH AND SAFETY? …

There are many reasons why health and safety at work should be important to all organisations.

- Employees – as human beings – should be protected from needless pain and suffering.
- Employees and employers often both have legal obligations to take reasonable measures to promote health and safe working.
- Accidents, illness and other causes of employee absence and/or impaired performance cost the employer money.
- A business's corporate image may suffer if its health and safety record is poor.
- A business's employer brand, i.e. its reputation as an employer may suffer if its health and safety record is not good. This may make it difficult to attract and keep qualified staff.

RESPONSIBILITIES OF EMPLOYEE

Role of Individuals – should be aware of safe working practices.

Individuals have a responsibility for their own safety and for that of their fellow workers. They should carry out instructions associated with maintaining health and safety e.g. the wearing of protective clothing, or the use of safety guards when operating machinery. Individuals should ensure that they are up to date with the location of fire exits and fire extinguishers, safety equipment and of the named first aider in the area.

In very general terms, everyone in the organisation is responsible for health and safety. As an individual, in order to contribute to a healthy, safe and secure environment there are a number of things that you may need to do:

- Be alert to potential hazards as you go about your work
- Take responsibility for your own behaviour in the workplace, in order to protect yourself and others.
- Co-operate with your employers' health and safety measures: read instructions, follow procedures, perform fire drills, etc.
- Keep yourself informed about health and safety issues relevant to your workplace.
- Undertake regular training as necessary.
- Warn people who may be at immediate risk as a result of hazardous conditions or behaviours.
- Take steps to minimise hazards, for example by clearing your own work area of obstructions.
- Take steps to mobilise appropriate response procedures for example by sounding alarms or calling a first aid officer in the event of an accident.
- Inform appropriate people of identified hazards and the need for corrective action which might be beyond the scope of your own authority.

RESPONSIBILITIES OF EMPLOYER

Your organisation may have dedicated departments, managers or staff in charge of health and safety. These may include specialists such as, a first aid officer or a medical officer, an employee counsellor and/or health promotion officer, a fire prevention officer, security guards or a building manager with responsibly for a many different aspects of the work environment. The role of all of these people is to make and implement relevant polices and procedures, to listen to employee concerns and to respond to problems and emergencies.

In addition, a number of employee health and safety representatives may be appointed by the trade unions or staff associations in your workplace, by agreement with your employer. Their role is to listen to employees' concerns and to consult with the employer on their behalf.

Legislation can also impose general duties upon employers to make sure that all systems and work practices are safe, that the work environment is safe and healthy – i.e. well lit, warm, ventilated and hygienic and that all plant and equipment is kept up to the necessary standard. Organisations may be required to provide protective clothing, safety guards on machinery and appropriate training to enable employees to use machinery and equipment in a safe manner.

ACTIVITIES WHICH MAY RAISE HAZARDS

There are many activities which are undertaken in the workplace which can give rise to hazards and risks and where accidents can easily happen. Whilst many of the ones that you are likely to come across will be in the office environment, there are a variety of other situations that you may need to be aware of, e.g. those that might occur in a manufacturing environment.

The broad range of activities which might give rise to hazards and risks include, but are not limited to, the following:

- General maintenance of building and fabric – involving use of ladders or roof work where there is potential for people to fall from high buildings or constructions.
- Using certain types of equipment e.g. VDUs where there is potential for eyestrain or repetitive strain injury associated with the continued use of a keyboard or a mouse.
- Using badly designed workspaces and office accommodation, where posture may be affected or there is potential for falls or tripping over electrical or computer connections; or where light is inappropriate.
- Using electricity, hand tools or extension leads where there is potential for electric shock or physical harm if using the equipment incorrectly.
- Carrying and/or lifting equipment which might lead to muscle strain or damage to the spine if not carried out correctly.
- Receiving raw materials – involving lifting or carrying, again having the potential to cause muscle damage or damage to the spine.
- Stacking or storing material – there may be falling materials.
- Moving material – using forklift trucks or lifting equipment.
- Operating machinery, where it is important that appropriate guards and shields are correctly deployed and where it is important to operate the machine within specified operational limits in terms of speed, or running time.
- Not wearing protective clothing and equipment for example ear defenders, safety glasses, protective footwear or using appropriate barrier creams when using certain substances.
- Dealing with emergencies, this is especially important as it is when dealing with emergency situations that standard procedures and ways of working are often inadvertently ignored or forgotten.

HOW TO REDUCE HAZARDS

All new employees should attend any health and safety training offered as part of their induction program and employees should be encouraged to update their knowledge and the information provided on a regular basis. This can be done by attending further training or by reading notice boards or any safety bulletins which may be issued.

They should be fully aware of any procedures associated with evacuation in the event of accidents or fire and this will include familiarization with the location of fire escapes, fire extinguishers and any other safety equipment.

They should make themselves aware of the nominated first aid in their area.

They should be aware of any specific hazards associated with the nature of their work i.e. exposure to substances hazardous to health, unsafe operating practices, potential dangers when using machinery and lifting equipment and the possible hazards of using computers.

They should wear protective clothing if necessary e.g. gloves, eye shields or ear defenders and ensure that they adopt safe seating positions and avoid repetitive strain injuries by having adequate and regular breaks from work stations during the working day. These measures should be provided and promoted by the organisation as necessary but all employees have a responsibility to ensure that they are made available and appropriately used.

COSTS THAT MIGHT BE INCURRED BY AN ORGANISATION AS A CONSEQUENCE OF ACCIDENTS OR ILLNESS:

Costs to the employer may include the following
(i) Productive time lost by the absent employee, and by other employees who stop work at the time of, or following, the accident.

(ii) A proportion of the cost of employing first aid and medical staff.

(iii) The cost of disruption to operations at work.

(iv) The cost of any damage to equipment, including subsequent modifications to make it safer.

(v) The cost of any compensation payments or fines resulting from legal action following an accident or illness.

(vi) The costs of increased insurance premiums.

(vii) Possible reduced output from the employee on return to work.

(viii) Possible reduced output, increased absenteeism or increased labour turnover as a result of low morale among workers in an environment which has been shown to be unsafe or unhealthy.

(ix) The cost of recruiting and training a replacement for the absent employee.

FACTORS WHICH CAN CONTRIBUTE TO A SAFE AND HEALTHY WORKING ENVIRONMENT.

Some of the key requirements of a safe and healthy working environment are as follows:

Cleanliness

Floors and steps to be cleaned regularly. Clean furniture and fittings. No accumulation of rubbish.

Avoid overcrowding

Make sure that each person has an adequate amount of space in which to work comfortably.

Ventilation

There must be an adequate supply of fresh or purified air in circulation.

Temperature

A reasonable temperature must be maintained.

Lighting and windows

There must be adequate natural or artificial light. Windows must be kept clean inside and outside.

Toilets

There must be enough suitable toilets for all employees. They must be properly ventilated and lit, kept clean and properly maintained.

Washing facilities

There should be access to clean hot and cold water, soap and towels, or equivalent.

Drinking water

Adequate drinking water must be provided together with cups or a fountain.

Seating

Where work must be done sitting down, seats must be suitable in design, construction and size.

Lifts

Lifts must be safe and maintained regularly.

Machinery and equipment

All equipment must be maintained. Dangerous parts of machinery should have appropriate guards. Appropriate training should be given in the use of all machinery.

No heavy lifting

People should not be required to lift, carry or move a load likely to cause injury. Appropriate training should be provided for all those required to undertake any lifting.

Fire precautions

Appropriate fire fighting equipment should be provided. Valid fire certificates should be in evidence. Escape routes clearly marked etc.

First aid

A first aid box/room, a trained first aider, and first aid training should all be made available.

ROLES

Role of Senior management is responsible for developing and implementing policies and can ensure that appropriate procedures are in place for carrying out risk assessments and safety audits. Management can also ensure that a coordinated approach to health and safety issues is maintained across the organisation. They also have a duty to monitor and evaluate health and safety and for taking any necessary corrective action.

Role of Supervisors – can have most influence as they are in immediate control of a situation and are usually in a position to take immediate action. They need to be vigilant and safety conscious at all times. They are also directly responsible for ensuring that individuals are conscious of health and safety hazards and do not take unnecessary risks. Supervisors are likely to be responsible for maintaining and updating any safety manuals and notices in conjunction with HR departments. They should ensure that all employees under their supervision are aware of things like fire exits and location of fire extinguishers, safety equipment and of the named first aider in the area.

ROLE OF TRAINING

Training has a key role to play in the area of health and safety and can be seen as an important preventative measure. Health and safety training should be an important aspect of an induction programme for all new members of staff. They should be advised of their own responsibilities and those of their colleagues and the organisation. Attention should be drawn to particular hazards or safety issues associated with the specific industry in which they are working, within their workplace or within the specific context of their own particular work environment. Training should also take place following a transfer to a new job or department or following any relocation or change in working methods. Refresher training should take place at regular intervals. Special courses should be arranged whenever new equipment or changes to working methods or processes are introduced. Formal training can be reinforced in many ways including the use of notice boards, electronic bulletin boards and staff handbooks.

HEALTH AND SAFETY POLICY

There will be several elements to a health and safety policy, whatever the specific needs and hazards of a particular workplace. Some of the key components are as follows

Risk assessment

This is part of continuing risk management and includes:

(a) Identifying risks,
(b) Controlling risks,
(c) Sharing information,
(d) Providing training as appropriate.

Having appropriate systems and procedures

This will include having safety procedures, procedures for the reporting of incidents, the removal of hazards and appropriate checking procedures. Emergency and evacuation procedures may also be included.

Minimising hazards associated with equipment

This will include the provision of any protective clothing, ergonomic design of work areas, soundproofing, safety equipment and appropriate maintenance of machinery and equipment.

The provision of information

This includes any warning signs, instructions about location and use of fire extinguishers, updating safety manuals and ensuring that everyone is aware of their location.

Training provision

This includes training in safety procedures and the use of equipment. It includes induction training, training when moving to a different department and regular updates on any new policies or information.

Responsibilities

This includes employee duties and the appointment of health and safety officers and representatives.

On-going monitoring

On-going monitoring to ensure policies and procedures are being adhered to. Making changes to systems and procedures as appropriate.

There a number of steps an organisation/Manager can take to ensure that its health and safety policy is effective, including:

- Making sure that the policy is known and understood by everyone in the organisation.
- Involving people in the development of the policy.
- Regularly reviewing the policy.
- Clear identification of roles and responsibilities. Everyone in the organisation has a role to play in ensuring their own health and safety as well as that of their colleagues. It is important that employers and employees are aware of their own specific responsibilities.
- On-going risk management rather than a one-off risk assessment. This includes the following: introducing controls to reduce risk, sharing of risk and hazard information, revising safety policies as appropriate, identifying any particular categories of employee who are especially at risk and identifying any training needs.
- On-going health and safety training. The amount and types of training required should be assessed according to individual needs. All employees should receive induction training when joining the organisation or when transferring to a different department or location. In addition there may be training requirements associated with the use of specific equipment or machinery. Training may also be required on a regular basis to update people regarding any changes to the law or for technical updates
- Information sharing, awareness and consultation are important in ensuring a health and safety policy is effective. Employees must be clearly advised of any risks and how they can be minimised.

TYPICAL STEPS THAT A HEALTH AND SAFETY MANAGER MIGHT TAKE IN ORDER TO ENSURE ON-GOING RISK MANAGEMENT

The typical steps that a health and safety manager might take in order to ensure on-going risk management are as follows:

(i) Carry out a risk assessment, generally in writing, of all work hazards on a continuous basis.

(ii) Introduce controls to avoid/reduce risks and plan contingency measures to minimise impact.

(iii) Assess the risks to anyone else affected by their work activities (such as suppliers, customers or visitors).

(iv) Share hazard and risk information with other employers, including those on adjoining premises, other site occupiers and
all subcontractors coming on to the premises.

(v) Revise safety policies in the light of the above – or initiate safety policies if none were in place previously.

(vi) Identify employees who are especially at risk (such as pregnant women or night shift workers).

(vii) Provide up-to-date and appropriate training in safety matters.

(viii) Provide information to employees (including part-time and temporary workers) about health and safety.

(ix) Employ/appoint competent health and safety advisors in all key areas.

CHAPTER 18

AIM OF SECURITY

Security aims to prevent others from illegally accessing, stealing and damaging the property of an organisation and/or the people who work in it.
Security aims to prevent others from taking away or doing damage to things that belong to your organisation and/or the people who work within it.

BASIC PRINCIPLES OF EFFECTIVE SECURITY

The basic principles of security are

- delay,
- checking and
- alarm.

Delay means providing appropriate lines of defence before vulnerable areas and items can be reached. This could include some or all of the following: making sure that outer doors to the main building are securely locked and bolted, ensuring that there is a secure, staffed reception area for visitors, ensuring that all offices are locked and where appropriate, guarded, by making sure that filing cabinets are lockable and are kept locked when not in use and finally by providing safes.

The second principle of ***security*** is checking – this means having appropriate procedures for authorised access to vulnerable areas or items. This could include some or all of the following: making sure that authorised staff can be clearly identified either by a uniform or an identity badge, (preferably showing a photograph), by ensuring that all visitors are checked in, escorted while they are on the premises and checked out on departure, by always ensuring that any unauthorised visitors on the premises are challenged, by the use of personal pass words or swipe cards to gain authorised access to different parts of the organisation and finally by seeking appropriate authorisation before access to files can be allowed.

The third principle of effective security is ***alarm***. This means making sure that there are adequate procedures for alerting those responsible for responding to security breaches. This could include some or all of the following: ensuring that buildings are fitted with electronic security alarms and by carefully controlling access to entry codes, by training all individuals in the organisation to be alert to potential security breaches and to be aware of the procedures for reporting them and through ensuring that computer systems have the ability to warn of any unauthorised attempts to access files. Internal security is also important and organisations should ensure that they have effective recruitment, selection and screening systems for all staff and security staff in particular.

Areas Need Security in Business Premises / Risky Areas in Office

- Public and open areas, such as entrances, hallways, parking areas, toilets, stairways and lifts – particularly if these are unattended or inadequately attended for the volume of traffic.
- Points of entry and exit, e.g. doors, windows, gates and lifts. These are points where intruders may attempt to gain access. Attention should be paid to open, unsecured or broken windows or doors – especially in unattended areas.
- Unattended areas, e.g. store rooms or back stairs, where there are not always people about.
- Ill-lit areas like car parks and stairwells.
- Reception areas, if an unauthorised person can talk, trick or slip their way past reception they may be much harder to identify as a stranger (and subsequently to locate within the premises) later.
- Areas where at-risk items and data are concentrated e.g. store rooms, computer rooms, offices etc., especially if they are located near points of entry or exit and busy public areas.
- Points of transit or storage outside the organisation's premises. Valuable items taken out of the office (for banking, delivery, work at home) may be particularly vulnerable.
- Risks to computerised systems relating to the environment in and around the location of hardware – this could lead to disruption of service.
- Risk of fraudulent manipulation of data.
- Manipulating input data.
- Incorrect processing of data.
- Unauthorised access to personal or confidential data.
- Risks to data output.
- Risks to data at point of storage.

OTHER SECURITY RISKS

Items that are

- valuable,
- portable and
- easily saleable

are particular security risks in an organisation

For example

- small equipment such as computers, printers, video and television equipment; vehicles or office furniture.
- Documentation such as ownership documents e.g. share certificates or title deeds and cash and cheques are also vulnerable.
- Other vulnerable items include security devices like pass cards and keys or information stored in portable form e.g. paper files, floppy discs and CD Roms.

The types of people who might be at particular risk in an organisation are:

- front line security staff e.g. security guards and reception staff, staff with custody of important assets e.g. counter staff in banks.
- Key personnel may also be at risk of intimidation for the purposes of obtaining cash, assets or security codes.

SECURITY PROCEDURES

The following are examples of security procedures.

- Procedures for identifying regular staff. This includes instructions about the wearing of identity badges at all times, regardless of how well people might be known. Clear instructions about showing the pass whenever buildings and premises are entered. It also includes being clear about the requirement to sign in and out of buildings and premises.
- Procedures for vetting non staff members. If someone is coming to visit you on business then you may be required to go down to a reception area and accompany him or her back to the place where you work. If you have not met them before you may need to ask them to produce some further means of identification, for example a letter inviting them to attend a meeting or an event.
- Procedures for non-business visitors. If you are meeting a friend or relative for lunch, your visitor may not be allowed on the premises or beyond the reception area. It is important that your visitor does not unwittingly break, or try to break, the rules.

- Procedures for protecting the building. A particular door may have to be kept locked at all times or at specified times. It may be a nominated person's responsibility to ensure that this is adhered to. It may be part of an individual's responsibility to ensure that all windows in his or her working area are closed and locked at the end of the day or at the end of a shift.
- Procedures for protecting the organisation's assets. Individuals usually have responsibility to lock away items in a desk drawer, e.g. calculators etc.
- Procedures for protecting documents and information. Locking away files and ledgers, or not leaving a computer terminal such that it can be used by someone without the password, are typical of measures of this sort. Other aspects of work may be sensitive and some individuals may have a confidentiality clause in their contract of employment.
- Procedures for protecting procedures. Computer passwords should not be revealed to others. Safe and lock combinations should not be made generally available, they should be restricted to nominated individuals. There should also be procedures to control keys – such as a list of authorised key holders and instructions about where keys should be kept and who should hold master keys if they are used. The organisation's security should not be discussed with anyone outside of the organisation.
- Procedures for explaining what to do in the event of a breach of security. The names and numbers should be available of people to contact and also of the information that they will need to be told: location of the intruders, for example, time of entry, how many there are, items missing or damaged, and so on.
- Fall back procedures. If service is disrupted by non-availability of computerised services there should be fall back procedures in place to enable (limited) business services to continue. Also tested stand by and recovery procedures should be available to enable normal business to be quickly resumed.

EMERGENCY PROCEDURES

Emergency procedures are particularly important to ensure that people are aware of the scope and limits of their responsibility.

Health emergencies may include any form of workplace injury (e.g. fractures, burns, eye injuries etc), electric shock, fainting or collapse, allergic reactions to toxic substances or manifestations of illness such as heart attacks or epileptic fits.

Procedures need to be in place so that these can be dealt with as quickly and effectively as possible. Employers also need to plan for emergency situations such as fire and bomb alerts, chemical spillage etc. The plan should be written down and communicated to all employees and others who may be affected by it. Specific employees with allocated duties within the plan should be given appropriate, regular training in the correct procedures to follow. The purpose of emergency procedures is to ensure that everyone is clear about what to do and where to go in the event of an emergency.

The following areas should be included in an organisation's emergency procedures:

- How to raise the alarm – this includes ensuring that employees are aware of the location of fire alarms and that the alarms are regularly tested so that employees are able to recognise the sound.
- What to do – i.e. how to call the emergency services and how to respond to a fire or evacuation alarm. This is achieved by carrying out fire and evacuation drills throughout the year.
- Where to go to reach safety – this includes ensuring that employees are aware of fire and emergency exits, that they are clearly marked and lead as quickly as possible to a designated safe area and are kept clear at all times. This may also include evacuation procedures.
- Names of nominated first aiders in each department or area – with full contact details.
- Essential actions such as emergency factory shutdown – locations of adequate protective equipment (such as sprinklers and fire extinguishers) should be in hand and regularly maintained.

ACCIDENT REPORTING

Accident reporting procedures are important to ensure that the circumstances and facts are recorded accurately as soon as possible after an accident. It may be necessary to refer to accident reports at a later date if complications emerge some time later.

An accident reporting procedure would require the person reporting the accident to do the following:

- Report the accident to someone in authority as soon as possible. This can be done informally, but in addition it is usual practice to complete an accident report form.
- Record the details of the accident in an accident book.
- Get signed statements from any witnesses to the accident, including names and addresses.

RISKS TO DATA

The main risks to data are as follows:

- Human error – individuals can lose, damage or incorrectly input or store data.

- Technical problems – data can be lost or corrupted when equipment fails.

- Catastrophic events such as natural disasters or accidents such as fire or burst pipes can break or destroy data storage and transmission facilities

- Malicious damage by individuals inside or outside the organisation who deliberately attempt to damage or tamper with data.

- Industrial espionage or sabotage by individuals who deliberately attempt to steal or damage data and information from the organisation with a view to commercial gain.

- Dishonesty by those who may wish to access information for personal gain.

- When data is transmitted over a network or a telecommunications line, especially the internet, there may be additional specific security dangers which arise because the data is carried by third party carriers and is outside the direct control of the organisation.

- additional dangers include the following: corruptions from viruses, the possibility of inadvertently overwriting someone else's data, unauthorised individuals being able to access parts of the network, risks from hackers, the downloading of inaccurate or imperfect information or information being intercepted leading to loss of service.

- In addition to the above, all organisations have a responsibility to ensure that data is adequately protected against any breaches of confidentiality.

HOW TO REDUCE OR AVOIDED RISK TO DATA.

There are a number of ways in which the risks to data identified above can be minimised.

Risks of human error can be reduced by checks and controls, systematic procedures, ongoing employee training and also appropriate supervision. Rigorous recruitment and selection procedures go some way to ensuring that staff employed are honest and trustworthy and will not engage in malicious acts or any form of espionage.

Risk of malicious damage can also be minimised by controlling access, both physically (using locks and security checks) and electronically (using passwords, encryption of data, anti-virus software etc).

Risks of disaster are difficult to foresee, but contingency plans may be made, including off-site back-up storage of files, emergency power generators and adequate insurance for any loss or damage to data and associated systems.

Organisations should take care to ensure that paper files or computer disks are not left where they are generally accessible.

Safes, strongboxes and filing cabinets should be locked when not in use.

Passwords should be used where advised and should not be shared.

Confidential information should not be copied or transmitted without specific authorisation and appropriate security measures. It is important to ensure that appropriate communication channels are selected to protect data where necessary.

Back-up systems are important to minimise the risks associated with data held electronically.

E-mail, intranets and the Internet mean that computer systems are increasingly connected over telecommunications lines and these are rarely completely secure. Use of passwords and user profiles make an important contribution to minimising risk. A password is a unique code a person uses to enter the system. For a password system to be effective, passwords should be changed regularly, difficult to guess, confidential and hidden.

A user profile in a networked system only allows certain people access to certain files. Records can be kept of access to files, so that a trail can be left of unauthorised attempts at entry. Despite passwords and user profiles, expert hackers may still be able to enter the system. Keeping track of any attempts made can alert managers to repeated attempts to break into the system or of any emerging patterns.

Use of anti-virus software which can detect and eradicate viruses is an important way to minimise risks to electronic data. Latest upgrades should be used to ensure that any new viruses could be dealt with.

Organisations must also guard against the introduction of unauthorised software to their systems as many viruses are spread on pirated versions of popular software. Any disks received from outside should be checked to ensure that they are virus free.

Systems should also make use of firewalls to ensure the safety and security of their data.