Component 3B

Threats to digital systems and how to control them

Organisations have increasingly been reliant on digital systems to hold data and process information/perform business operations. Cybersecurity is vital for the protection of organisations and individuals from internal and external threats.

Reasons why systems are attacked

- Data and information theft for own benefit or to sell for cash.
- For challenge or fun, sense of thrills and achievement.
- Industrial espionage. Theft of intellectual property; plans, designs, inventions of other organisations
- Disruption of system and operation of organisations.
- Personal attack; ransomware by encrypting local file, from ex-employees with a grudge for instance.
- Financial gains. Theft motivated by financial gains from victims for example.

External threat to systems and data

Attacks on systems can come from system users or from external organisations.

- **Unauthorised access/hacking**. Where users attempt to access the system illegally without permission/authorisation. Also, illegal access by external hackers, paid to do so.

- **Social engineering** where criminals, claiming to be from legitimate organisations, contact users via e-mail or phone seeking personal ID and financial information.

- **Phishing.** This is another form of social engineering, where spoof e-mail are sent to users on the hope the sender can obtain personal ID information.

- **Pharming.** This is a combination of phishing and farming. User are directed to fake website where they innocently enter personal information.

- **Man-in-the-middle attack.** Where communications between user and server are intercepted and personal details are stolen and benefited from.

Internal threats and data security

How can organisations deal with internal threats to their digital system?

Internal threats: Internal threats are also common.

- Accessing untrustworthy website may have viruses and phishing threats.
- Downloads. Illegal/unapproved software may contain virus and infect system.
- Employees selling/leaking information for financial gain, revenge or political reasons.
- Employees trying to access data and information they shouldn't.
- Using portable devices such as laptops, USB drives may be infected with viruses and can infect the entire system.

Impact of security breach

Security breach can impact an organisation in many ways.
- Immediate impact: loss of data, downtime, loss of sale, loss of productivity.
- Long term impact: financial loss, public image, possible legal action.

Access restriction

To prevent unauthorised access to its systems, an organisation must implement both physical and encrypted password measures.

Physical security measures. Means to prevent unauthorised entry to secure premises. For instance, using locks, electronic keys or hiring guards.

Password. This can be traditional password. Most organisation include creation and use of password in their acceptable policy. Other forms of passwords such as gesture passwords are also used.

Setting levels of access to systems. Levels of access to systems vary according to staff functions and responsibilities within organisations. For example, certain important/private details can only be accessed by managers/directors.

Biometric. The following are examples of biometric access control:

Fingerprints, hand geometry, eye retina/iris pattern, facial recognition, voice recognition and handwriting analysis.

Two-factors identification (TFA). Sometimes more information other than password and pin are required. Example, asking users to provide two forms of identification.

Data level protection

Firewalls. Firewalls form the first line of defence. They can be software or hardware based. Firewalls are set of rules/codes that filter and reject suspicious packets entering the system through the network.

Antivirus software. Checks the system for malicious software and removes them before they cause damage. They infect the system through e-mails, network or removable devices.

Device hardening. There are different techniques for hardening a device.

- Installing a firewall for first line of defence.
- Installing an anti-virus software
- Using encryption
- Closing unused network
- Restricting user access

Backing up and recovering. Regular backing up is essential. Usually done nightly or weekly. Backing up is saving copies of daily stored data on an external medium to be used to recover the system from loss of data.

Encryption. It is common to encrypt data when it is stored and when it is transmitted between system. Unencrypted data is vulnerable to hacking.

When transmission is encrypted, a green pad lock is shown the https; an assurance that the website being connected to is secure.

Improving security

It is the responsibility of the organisation to take the necessary measures to protect their IT systems and protect the personal and sensitive data.

Ethical hacking. This an arranged hacking by an organisation to test the security if its system looking for weaknesses and improve the security. Ethical hackers are described as white hat or grey hat hackers. This type of testing is called penetration testing.

Penetration testing. This is a systematic process called 'Pen' test used by ethical hackers to ascertain the security of the IT system. The ethic hackers conduct their testing outside the busy hours to minimise business disruption. Penetration testing can be automated.

Security policies

Organisations create security policy to ensure that all employees are aware of the security procedure they need to adhere and the plans to follow in case of security breaches or disasters. Also included designated responsibilities; who is responsible for what.

Content the security policy:

- System security
- Data security
- Compliance with regulations and legislations
- Environmental; disposal of waste products.
- Disaster plans recovery
- Data recovery
- Updating and replacing hardware and software (infrastructure).
- Responsible use of policies.

Password policy. Password creation and protection.

How to create a good password and how to protect it. Regularly change the password and immediately replace the default password.