SUBJECT: BTEC Tech Award Digital IT

UNIT: Component 3: Cyber Security

SANDHILL VIEW
EST. 1953
ACHIEVE · ASPIRE · ENJOY

Why systems are attacked:
- Fun/challenge
- Industrial espionage or financial gain
- Personal attack
- Disruption
- Data/information theft.

External threats to digital systems and data security:
- Unauthorised access/hacking
- Malware
- Denial of service attacks or phishing
- Pharming
- Social engineering
- Shoulder surfing
- 'man-in-the-middle' attacks.

Internal threats to digital systems and data security:
- Unintentional disclosure of data
- Intentional stealing or leaking of information
- Users overriding security controls
- Use of portable storage devices
- Downloads from internet
- Visiting untrustworthy websites.

Impact of security breach:
- Data loss
- Damage to public image
- Financial loss
- Reduction in productivity
- Downtime
- Legal action

Prevention and management of threats to data

User access restriction:
- Physical security measures (locks)
- Passwords
- Using correct settings and levels of permitted access
- Biometrics
- Two-factor authentication (who you are, what you know, what you have).

Data level protection:
- Firewall (hardware and software)
- Software/interface design (obscuring data entry, autocomplete, 'stay logged in')
- Anti-virus software
- Device hardening
- Procedures for backing up and recovering data
- Encryption of stored data (individual files, drive)
- Encryption of transmitted data.

Finding weaknesses and improving system security:
- Ethical hacking (white hat, grey hat)
- Penetration testing
- Analyse system data/behaviours to identify potential risks.

Policy

Defining responsibilities:
- who is responsible for what
- how to report concerns
- reporting to staff/employees.

Defining security parameters:
- password policy
- acceptable software/installation/usage policy
- parameters for device hardening.

Disaster recovery policy:
- who is responsible for what
- dos and don'ts for staff
- defining the backup process
- timeline for data recovery
- location alternative provision

Actions to take after an attack:
- investigate
- Respond
- manage
- Recover
- analyse