**Directed Study**

How are **cyber security technology components** typically deployed in **networks and systems** to provide security functionality (including hardware & software) for a **small to medium business?**

**Physical ways a business can protect it’s network & systems:**

* **Fences, gates, walls & doors**
* **Locks, barbed wire, visible security methods & signs**
* **Security guards**
* **Security cameras - CCTV**
* **Disaster-protection devices such as smoke alarms or fire extinguishers**

**Procedural**

* **UserID & password procedures**
  + Use a strong email e.g. minimum 14 characters with a combination of upper, lower case & special characters.
  + Use a separate login and password for every important system account.
  + Another good technique is to use 3 random words in a password.
  + Password manager – easy to use and create long complex passwords and they’re better than humans at spotting fake websites, but you can’t use them for everything e.g. Some banks. They’re also attractive targets because if hackers crack the main password, they then have access to all the users' passwords.
  + Two-factor authentication – helps to stop hackers from getting into their accounts, even if they have their password.
* **Employee awareness & training**
* Teaches employees to understand vulnerabilities and threats to business operations so they are aware of their responsibilities and accountabilities when using a computer on a business or public network.
* Management - commitment to practising and promoting information security.

**Technical**

* **Access control policies:**
* Controls who is permitted access to business systems based on their position and responsibilities within the company.
* Strict policy must be in place to remove all access in the event of an employee ceasing to work for the business.
* Monitor and control of important employee actions to safeguard against tampering.
* **Backup data** using an external hard drive which are inexpensive & easy to use or via the cloud.
* **Secure configurations:**
* Change default passwords.
* Avoid generic userID’s e.g. ’admin’
* Apply correct rights and privileges for user and files.
* Configure security options on all OS and applications.
* **Network security:** 
  + Firewalls e.g. Deep packet inspection Firewall to look deeper into network packets & block, reroute or log potential breaches.
  + Intrusion prevention systems (IPS) constantly watches your network, identifying possible incidents and logging information about them, stopping the incidents, and reporting them to security administrators.
  + Restrict connections to ensure they can’t access harmful or malicious websites.
* **Encryption**
* Any files containing sensitive data
* Important Memory sticks, drives.
* **Anti-malware**
* Formal policies prohibiting the use of unauthorized software.
* Application whitelisting – allowing only authorized software to operate on the company’s servers and endpoints.
* Blacklisting – prevent the installation & execution of undesirable websites/applications.
* Install, regularly update & repair good business malware detection software e.g. McAfee Total Protection.
* Scan email attachments and downloads for malware.
* Have a pre-prepared plan in place for recover in the event of sever malware attacks (backup and recovery).
* Ensure all staff are educated and aware of hoaxes e.g. spam emails and how to handle them i.e. Report, don’t open and delete.
* **Patch management –** fixes vulnerabilities on software that are susceptible to cyber-attacks to help the business manage its security risk ensuring software and applications are kept up-to-date and running smoothly.
* **Monitoring Controls (SIEM Security Information and Event Management)**
* Cyber risk management - Detecting and preventing early cyber threats and data breaches before they cause damage and disruption.
* Recording all system activities such as user ID’s dates, times and details of key events e.g. log on, log off.
* Recording Uses of privileges, applications, files, websites, transactions executed.
* Intrusion prevention systems (IPS) constantly watches your network, identifying possible incidents and logging information about them, stopping the incidents, and reporting them to security administrators.