Methods for combating a range of ICT crime

- Can be physical theft of computers and hardware
- Or to gain access to another computer system and commit a crime,
- Or breaking one of the Acts involving ICT (Data Protection Act, Computer Misuse Act)
- Computers from film are hard to achieve.
- Industrial Espionage

Physical methods

- If computers are in office buildings, the company can employ security guards, a password protected door for a computer room.
- Security cameras to monitor corridors and rooms.
- Position of the screen and keyboard to prevent password seen by the public.
- Chaining computers to a desk for receptions.
- Biometric scanners for doors or even computers.

Logical methods

- Username and Password protected network for users to log on with their unique username and password.
- User ID can be allocated to groups with restrictions.
- User ID can restrict the user to only logging onto certain machines or at certain times of the day,
- To log what the user is doing.
- To apply controls to passwords:
- Use a minimum number of characters
- Use a combination of numbers and letters
- Do not use words from the dictionary
- Change password regularly
- Restricting login attempts
- Making the password impersonal
  - Keeping anti-spyware, anti-spam and anti-virus software up-to-date
  - Auditing, firewalls and encryption.
  - Auditing is a method of looking over logs. Logs can be created for events that occur on the network,

Encryption

- Encryption aims to prevent anyone who has the data being able to understand it without the appropriate key.
- The process is to take plain text and applying an algorithm to it to turn it into encrypted text.
- Only one with the key can encrypt the text back to plain text.