NETWORK SECURITY

DATA SECURITY

THREE MAIN TYPES OF SECURITY

- Physical
- Perimeter
- Network

PHYSICAL SECURITY

- Physical security is the protection of all the people, hardware, networks and data that can cause a data breach. It relates to the physical environment in which the computer is stored.
- An organisation that has the best cyber security in place would still be vulnerable if it does not have any physical security to the building and IT infrastructure. If an organisation's physical office is not 'defended' properly, the lack of physical security can be largely responsible for a data breach.
- If an unauthorised person gains access to the building, they can then have access to the computers and have access to the data that the organisation holds.
- Laptops and mobiles are entrusted with the most sensitive of information about the organisation. These devices, whether they are company property or personally owned, often contain company documents and are used to log on to the company network.
- Often, these mobile devices are also used during conferences and travel, thus running the risk of physical theft.

PHYSICAL SECURITY (CONTINUED)

Physical security can be enforced in several ways:

- ❑ Set up surveillance
- ❑ Lock server room, all access doors and windows
- ❑ Lock away vulnerable portable devices
- ❑ Alarm systems
- ❑ Security guards
- ❑ Disable USB connections for backing storage devices on computers
- ❑ Encrypt data on laptops and portable backing storage devices

PERIMETER SECURITY

- The perimeter of a network is the boundary that separates the data that flows in and out of the network.
- It contains all the architecture and elements to secure the perimeter of the internal network from other outside networks, like the internet.
- In the past, it was straightforward to secure the perimeter of the network. A firewall was used to dictate what traffic was allowed into and out of the network.
- However, more recently, this has become increasingly difficult to do. This is due to the vast number of different devices requiring different access to the network at different times, some permanently, some temporarily.

PERIMETER SECURITY (CONTINUED)

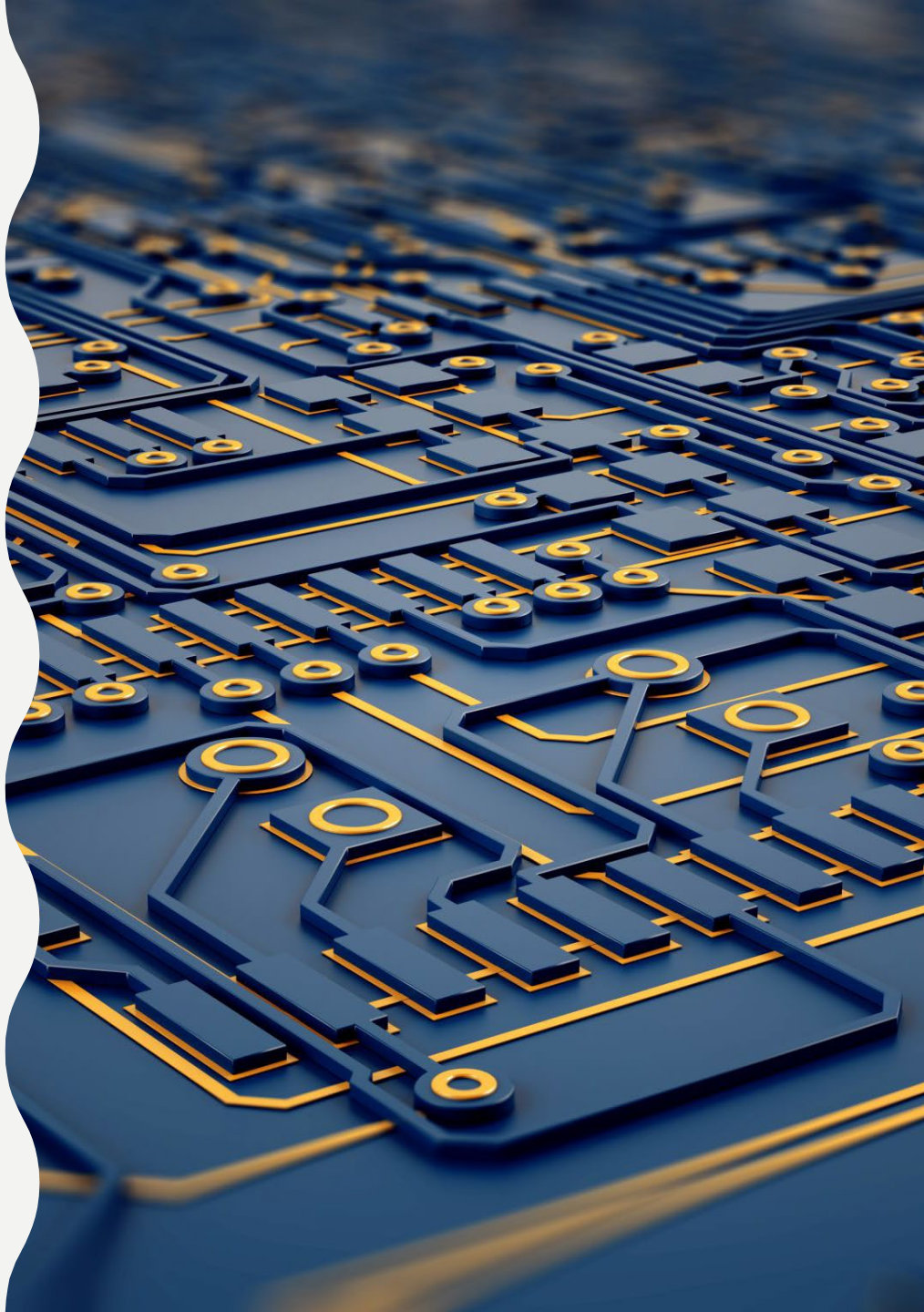
- Mobile devices (Bring your own device, laptops, tablets, smart phones)
- Software, such as JavaScript that needs access to run on local machines.
- Wireless Access Points throughout the organisation (Internet of Things)

There are several layers of protection to the network in the perimeter. Different technologies working together to create a barrier between the internal network and the outside world.

- ❑ Border Routers
- ❑ Firewalls
- ❑ Intrusion Detection Systems
- ❑ Intrusion Prevention Systems
- ❑ Virtual Private Networks
- ❑ Demilitarised Zone

INTERNAL NETWORK

- If the perimeter is breached, then the internal network can become exposed.
- However, data breaches and cyber-attacks do not always come from outside the organisation.
- Many breaches and attacks come from the inside.
- All the defences securing the perimeter are useless if the organisation already has a weakness on the inside.



INTERNAL NETWORK (CONTINUED)

It is very important that in the event of perimeter breach, or if the attacker is already inside the organisation, the internal network has security protocols and techniques in place.

These include:

- Anti-virus
- Malware protection
- Up to date software
- Strong password policies
- User permissions
- Website monitoring
- Encryption on stored data
- Internal Intrusion Detection Systems
- Internal Intrusion Prevention System

TASK

NOW DO TASKS 16 AND 17