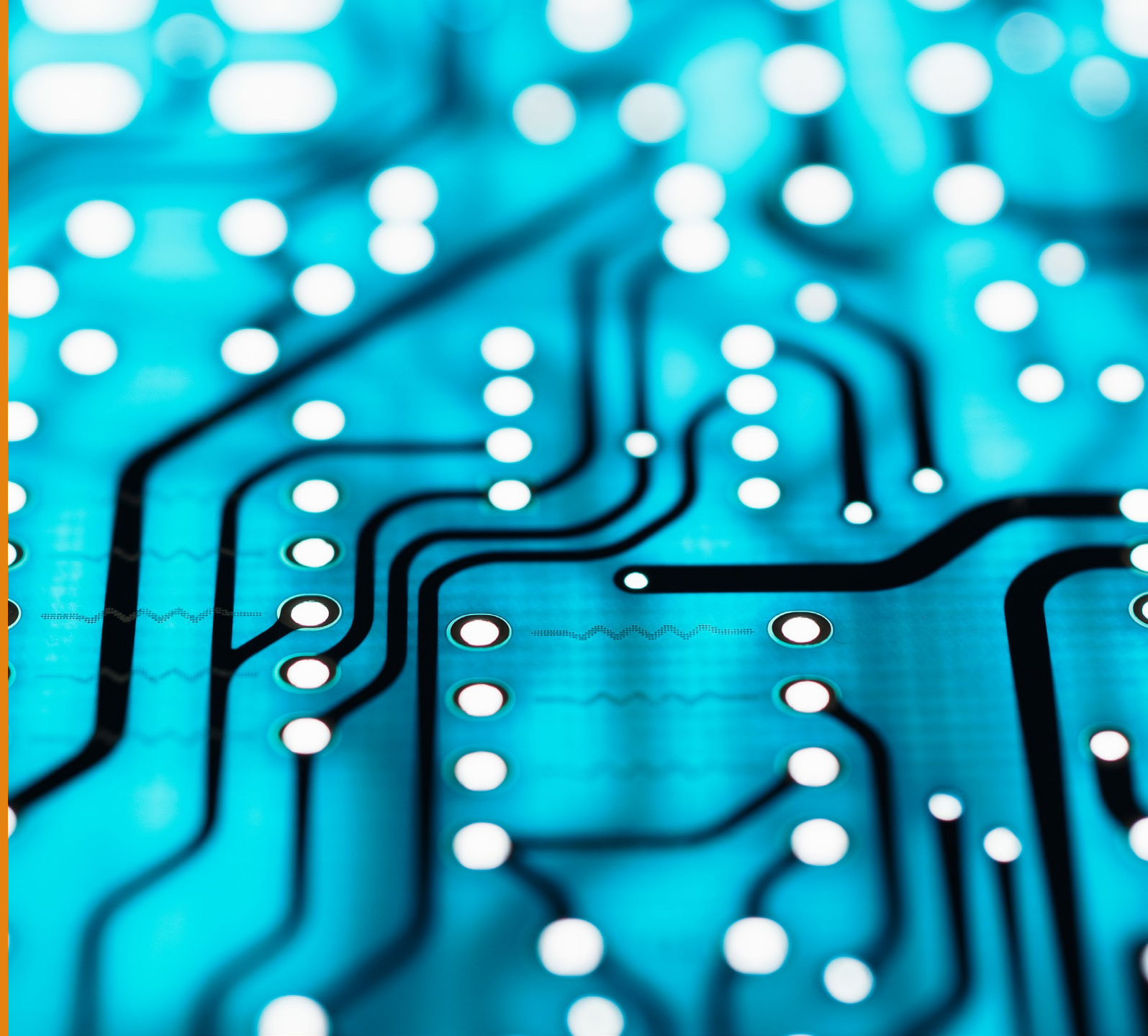
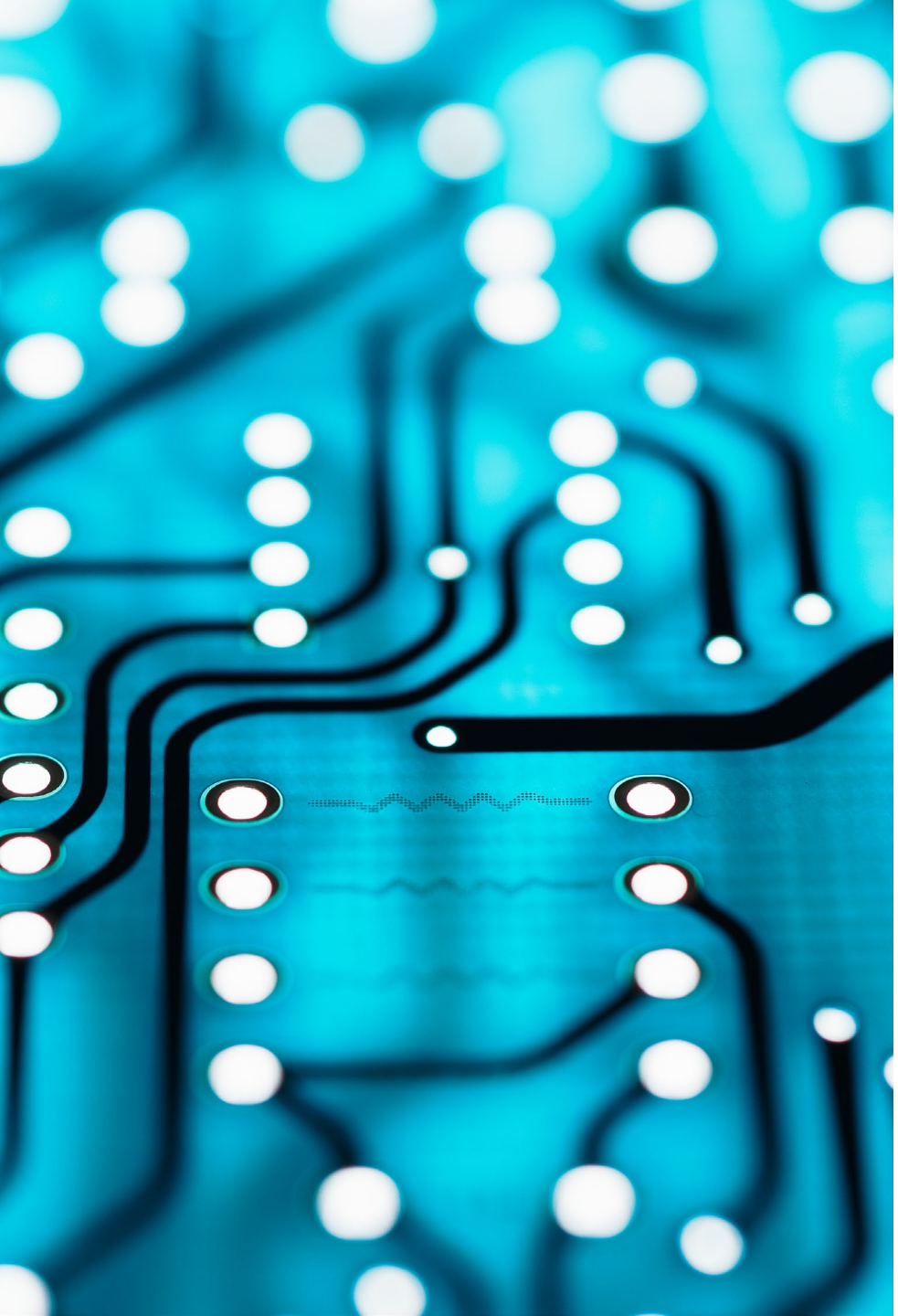
Physical Security Methods

DATA SECURITY





Physical Security

The threats and vulnerabilities we have looked at in previous lessons may appear to be a daunting task to protect ourselves against. However, by employing the right tools and techniques, as well as some common-sense practice, we can make our IT systems secure.

Physical security methods will make just as much difference in protecting our computers and data from harm as any firewall, anti-virus or user authentication system. In fact, these should be the very foundation of our cybersecurity.

In this lesson:

- Physical methods for restricting access to systems
- Backup procedures for protecting data

Physical Methods for Restricting Access

The first step in securing our IT systems and the data they store is simply to stop malicious users from being able to gain physical access to them.

We'll look at several physical security methods …

Site Security Locks

Locking the buildings and the rooms where our IT systems are contained is a very important procedure that should be implemented in businesses. In particular, your server room should be well secured by lock and key, though all rooms with IT equipment should be locked when not in use.

If someone were to gain access to your server room they would be able to cause huge damage as it will contain all the networks data, and all transmitted data will pass through the servers, routers, switches etc. that are kept there.

Card Entry & Biometrics

This ties in closely with site security locks. Instead of using a key for locking & unlocking rooms, a swipe or smart card could be used instead. Alternatively, biometrics can be used, such as a fingerprint scanner or facial recognition.

Using a card entry or biometrics system allows you to identify each person that has entered a room. This will allow for you to identify any suspicious behaviour (accessing late at night) or to investigate an attack that has occurred (identify who had entered the room at the time the attack happened).

CCTV & Security Staff

Locking the rooms to prevent access is a great starting point, however, rooms get left unlocked and keys or cards get lost/stolen. So, it's important to have surveillance in place to monitor who is accessing the rooms that contain our IT systems.

CCTV is an excellent way of doing this. They are difficult to tamper with and provide clear visual evidence of who has been in a room. This can be connected to a monitor to allow for a member of staff to constantly watch who is in the IT rooms.

Having security personnel is another great tool in performing surveillance on who is accessing rooms containing IT equipment, such as the server room.

This is because security staff will often patrol the entrances, and different areas to check if people are trying to enter. Security staff will also monitor the CCTV cameras, check identification of employees and forcefully stop people from entering if needed.

Alarms

Even with locks and good surveillance, there is still the possibility someone may gain access. Alarms will be an important tool in these situations.

These could be door and window alarms to detect when they have been forced open or motion sensor alarms triggered when an individual is within a room when no one should be.

This is particularly useful for 24-hour monitoring as the alarms can be connected to a local security company who will quickly come to the business premises to identify the cause of the alarm, potentially preventing an attack from occurring.

Protected Cabling & Cabinets

When an IT company has a lot of exposed cabling, then they are running the risk of an intruder cutting or attaching a device to the cabling.

One way around this is to use protected cabling. This is when a cable is wrapped in extra layers, rather than just rubber. The additional layers can include a woven wire mesh layer which makes it harder to cut into.

We can also use locked cabinets for keeping equipment secure. In particular, portable devices, such as laptops and tablets, and external storage devices, need to be secured when not in use. A locked cabinet is a great way of doing this.

Backup Procedures

Backups are an important process in securing your data. Should anything damage our business data we will need a quick method of recovering that data. Without a backup, many businesses will fail if they suffer a major data loss.

There are a variety of different backup procedures that we can follow, and different locations to store the backups in.

Backup

There are three main types of backup that we perform. These are:

- **Full Backup** – This is a complete backup of all your data. This provides excellent protection but is time-consuming and requires huge amounts of data storage capacity to store the backups.
- **Incremental Backup** – This is a backup of only the data that has changed since the previous backup. This is obviously much quicker and requires less storage space than a full backup.
- **Differential Backup** – A mixture of the previous two. A business takes a full backup and then takes backups of data that has changed since that last full backup. So, you might do a full back up at the start of each week and then incremental backups each day of the week.

These are normally not run manually by IT staff, but as a planned automatic backup procedure that will run regularly at a set time each day or week.

Storing Backups

There are also important differences in where we store our backups. We have three options here too:

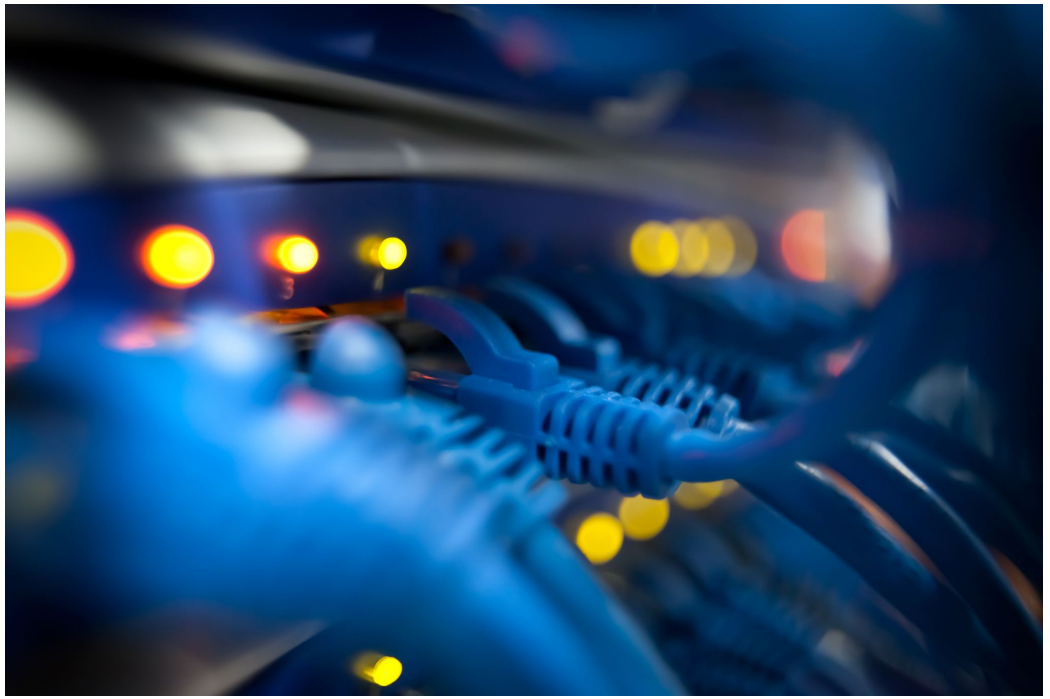
- **On-Site Backups** – stored in the same building as the original data. This makes it easy to recover the data even if the network is down but could be destroyed by whatever damaged the original data.
- **Off-Site Backups** – stored in a different location as the original data. This is generally seen as more secure as your backup will be protected from whatever damaged the original data. Recovering the data can be slow as you need to fetch the data from the off-site location.
- **Cloud Backups** – much like off-site backups your data will be stored in a different location but will be connected via the internet. With the cloud, you can have a real-time sync of data between the IT systems as the cloud storage to ensure the latest version of the data is available.

Further thought

How often do you think a large organisation will back up its data?

What about your college?

Does it backup hourly, daily or weekly?



Summary

- Physical methods for restricting access are the foundation of cybersecurity as if malicious users cannot gain access to IT systems, it is very difficult for them to cause any harm.
- Physical methods for restricting access include site security locks, card entry, biometrics, CCTV, security staff, alarms, protected cabling & cabinets.
- Backup procedures are required to help us recover from any damage caused to data.
- Backup procedures followed are usually either full backup, incremental backup or differential backup. These will normally be not manually triggered but planned automatic backups.
- Backups can be stored on-site, off-site or in the cloud. Off-site and cloud storage are generally considered more secure as on-site backups may be harmed by the same attack that damaged the original copy.