**Security Threats**

**Internal Threats**

Internal threats are the idea of threats coming from within a company. So, this can range from an employee accidentally leaking company data or purposefully deleting data.

Internal threats are the biggest vulnerability a security system can have. You can almost never prevent it. However, you can minimise its effects of the company.

**Employee Actions**

Employee actions can be accidental or intentional and can affect a company in different ways. The affects can be minimal or devastating.

***Accidental:***

* **Deleting data before it’s backed up (or without backups)**

*Deleting data that’s important to a company (like customer details) can cause money to be lost and in some scenarios, companies have gone bankrupted from data loss.*

* **Leaking company data**

*Data leaks can ruin a company in many ways. Like ideas could be copied or it can ruin their reputation if the information is controversial and/or it goes public.*

* **Unaware of unsafe practices like visiting an unsafe website or using external flash storage**

*Visiting unsafe websites can lead to data theft from viruses or disclosing information to malicious people who could use it to do damage to the company.*

* **Using file sharing apps**

*Depending on the app, it could be very insecure, and the data shared on it could be vulnerable to theft.*

* **Uploading files to the internet**

*Depending on where they are uploaded, they could unintentionally upload it to an insecure website that allow the data to be stolen.*

***Intentional:***

Firstly, intentional damaged may be cause by an employee getting bribed or disliking how their treated by the company.

* **Deleting data**

*An employee can delete data with the intention of damaging the company as much as possible. It’s especially effective if you rely on employees to back up their data.*

* **Leaking company data**

*As mentioned, a person can be bribed to leak company data, or they can just have malicious intentions to damage the company and their reputation.*

* **Overriding security systems**

*The employee can purposefully override security systems to leave the company at risk to data theft or loss.*

**Prevention/Minimise**

Different methods can be used to prevent or minimise the effects of any of the threats listed above.

***Accidental:***

* **Deleting data**

*We can prevent deletion of data by having a “recycle bin” that holds any deleted data for 30 days and/or you can have a confirm button to ensure it doesn’t take just one click to delete anything.*

* **Leaking company data**

*Limited access to data can minimise what data can be leaked and reassures that the employee will be aware of what they do with their data.*

**External Threats**

**Overview**

External threats are quite different from Internal threats in that it’s the idea that the threats come from outside the company. These threats can be a multitude of things from someone trying to breach the system or a natural disaster.

With laws in place, its rarer for hacking to occur these days. However, every country has a different outlook on hacking and the laws vary. Some countries have no laws against it, which means if someone tries to hack a company in the UK from said country, you can’t prosecute the hackers.

**Examples**

* **Viruses**

*Viruses are perfect examples of external threats. Designed to either steal data or destroy it. The overall risk of viruses is hard to generalise but it can result in a loss of data or data being stolen.*

* **DDOS**

*DDOS or Distributed Denial of Service is when someone, usually using a botnet, sends a lot of packet requests from a server and causes it to shutdown or become extremely slow from all these requests. This can create downtime for a company and lose them loads of money, even if the downtime is a short period of time.*

* **Malware**

*Malware is a good example of an external threat because it usually goes undetected for a good period of time. It’s a great risk to a company because malware is usually installed by an employee that thinks they’re downloading legitimate software because it poses as legitimate.*

* **Phishing**

*Phishing usually involves an unsuspecting employee clicking a link in an email that leads to a virus being downloaded. The risk to phishing is huge because close to half of all emails are spam. Phishing can also be a malicious website posing as a legitimate one and has the user input their details.*

**Physical threats**

**Overview**

Physical threats can be caused by many different situations. It can be natural or “man-made” realistically.

**Example**

* **Natural Disasters**

*Natural disasters are quite unpredictable and if a company is not prepared for them, it can be devastating. If backups are kept at the same place as the main storage and the whole building gets flooded or catches fire, it could mean that all the data is lost.*

* **Theft of equipment of data**

*Theft can happen in a multitude of ways. Either physically stealing the device data is stored on or using malicious software or viruses as an example*

* **Damaging hardware**

*If an employee spilt a drink of dropped a hard drive, the data stored on the device could be lost and it can be expensive to replace.*

* **Terrorist attack**

*A terrorist attack can be devastating to a business if all the data is destroyed in an attack. Examples like businesses in the Twin Tower September 11th attack never recovered because all their data was stored in the building. As much as it’s devastating to life but also businesses as well.*

**Unsafe Practices**

**Overview**

Unsafe practices are usually carried out by employees that don’t understand the risks of what they are doing.

**Examples**

* **BYOD**

*BYOD or Bring Your Own Device is an unsafe practice because it’s the weakest part in a security system. Someone storing company information on a laptop for example is unsafe because personal laptops may not have good security and the can be physically stolen. Also, there’s no restriction or monitoring what websites that person may go on and risk installing a virus*

* **Using USB**

*Using a USB stick to store information is even more risky that using a personal device. A USB is not very durable can be easily lost. Also, most people don’t encrypt data stored on a USB so if it’s stolen or lost, the information can be stolen easily.*