**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.*

* **Physically damaging hardware like spilling a drink**

*The data stored on the device could be lost and it can be expensive to replace hardware.*

* **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.*