Case Study: Heathrow Airport Cyber Attack (2017)

In **October 2017**, **Heathrow Airport**, one of the busiest airports in the world, suffered a serious **data security breach**. The incident began when a **USB memory stick** containing **confidential airport security information** was found by a member of the public on a London street.

The USB stick contained **165 files**, including:

- Security patrol routes and procedures.
- Maps and layouts of CCTV cameras.
- Details of airport ID access zones.
- Information about measures used to protect VIPs, including the Queen.

The files were **not encrypted or password protected**, meaning anyone could access them by simply plugging the device into a computer.

How the Breach Happened

- The USB drive had been **lost by an employee or contractor** working for Heathrow Airport.
- The data on the drive contained **sensitive operational and security details**, yet it had not been properly secured.
- A member of the public found the USB and handed it to a newspaper, which reported the issue.
- The newspaper alerted Heathrow Airport, and the breach was investigated immediately.

Impact of the Attack

1. **Security risk:** The information on the USB could have been exploited by threat actors to plan or assist an attack on the airport.
2. **Reputational damage:** The story made national headlines, raising questions about Heathrow's internal data handling and staff training.
3. **Regulatory and financial consequences:**
    - The **Information Commissioner's Office (ICO)** investigated the incident.
    - Heathrow Airport was fined **£120,000** for failing to protect personal and security-related data under the **Data Protection Act 1998**.
4. **Operational impact:** The airport had to review and tighten its security processes, data protection policies, and staff procedures.

Root Causes

- **Poor data management:** Sensitive information stored on removable media without encryption or access controls.
- **Lack of staff awareness:** Employees were not properly trained in handling confidential data.
- **Insufficient device control:** No central oversight of who used USB drives or what data they contained.

Lessons Learned

1. **Data encryption is essential:** Sensitive data must always be encrypted, especially when stored on portable devices.
2. **Staff training matters:** All employees and contractors should receive regular, mandatory cyber security awareness training.
3. **Access control and device policies:** Organisations should disable or tightly control USB ports and removable media.
4. **Incident response:** Organisations must have clear procedures for reporting lost devices or data breaches immediately.
5. **Compliance:** Regular reviews are needed to ensure compliance with data protection laws such as the **GDPR** (which came into effect the following year).

Recommendations

If you were part of Heathrow's cyber security team, you would recommend:

- **Banning unapproved USB devices** and introducing **secure cloud file-sharing systems**.
- Implementing **data loss prevention (DLP)** tools to monitor and control data transfers.
- Conducting **regular staff awareness campaigns** focused on data handling.
- Enforcing **encryption by default** for all removable storage devices.
- Introducing **audits and random checks** to ensure compliance with information security policies.

Summary

The Heathrow Airport incident demonstrates that **data breaches are not always caused by hackers** — sometimes they occur due to **human error and poor security practices**.

Even a small oversight, such as losing a USB stick, can have **major security, financial, and reputational consequences**.

This case highlights the need for:

- Strong **data protection policies**.
- Ongoing **staff education and awareness**.
- The use of **technical controls** to reduce human risk.