Case Study: Cyber Security at Talkative

Scenario

- Talkative is a **social media platform** for 13–21-year-olds.
- Users can **post photos, chat privately, play games, and make in-app purchases**.
- **Data** (posts, photos, messages) is stored on cloud servers.
- The company is **based in Manchester** with 50 employees.
- Staff use **staff passes, company iPhones, and laptops** for remote work.
- Staff were emailed **best practices for cyber security**, but there is **no mandatory training or confirmation of reading**.

You are part of the **Talkative security team** tasked with analysing the **current threat status** and making recommendations.

Step 1: Analyse Current Threat Status

1. **Human Factor / Insider Risk**
   - Staff may **ignore best practices**, increasing the risk of phishing or credential leaks.
   - No mandatory **IT security training** could mean low awareness.
   - Employees working remotely on laptops or iPhones may connect to **unsecure networks**.
2. **Technical Vulnerabilities**
   - Cloud servers hold sensitive user data; misconfigurations could lead to **data leaks**.
   - In-app purchase systems could be **targeted by fraud or malware**.
   - Lack of auditing of staff compliance may allow **unauthorised access**.
3. **Physical Security**
   - Staff passes could be **lost or stolen**, granting access to the office.
   - Company devices could be **lost or stolen**, exposing user data.
4. **External Threats**
   - Talkative's main user base (teenagers) makes it a **target for cyberbullying, hacking attempts, or exploitation**.

    - Social media platforms are often targeted for **DDoS attacks, malware, or phishing campaigns**.

5. **Regulatory Risk**

    - Handling data for minors (<18) increases legal obligations under **GDPR or child protection laws**.

Step 2: Recommendations to Mitigate Threats

1. Human / Staff Controls

- Implement **mandatory cyber security training** for all staff.
- Require staff to **acknowledge understanding** of security policies.
- Conduct **regular phishing simulations** and awareness campaigns.
- Limit administrative privileges based on **role necessity**.

2. Technical Controls

- Ensure **cloud servers are properly configured**, encrypted, and monitored.
- Enable **multi-factor authentication (MFA)** for staff and admin accounts.
- Regularly **patch and update devices**, apps, and operating systems.
- Implement **logging and monitoring** for suspicious activity.
- Run **periodic vulnerability scans** and penetration tests.

3. Physical Security

- Track staff passes and enforce reporting of lost/stolen cards.
- Require **device encryption** and remote wipe capability for laptops and iPhones.
- Restrict access to sensitive areas based on **need-to-know principle**.

4. User-Focused Measures

- Educate users about **safe online behavior**, including privacy settings and reporting abuse.
- Protect in-app purchases with **secure payment systems and fraud detection**.
- Monitor for **abuse or inappropriate content**, particularly for minors.

5. Policy and Governance

- Create a **formal incident response plan** to quickly handle breaches.
- Regularly review compliance with **child data protection laws** and GDPR.

- Maintain a **risk register** to track threats, likelihood, and impact.

6. Continuous Improvement

- Conduct **regular audits and risk assessments**.
- Retest systems after updates or new implementations.
- Update policies and training as new threats emerge.

Step 3: Summary

The main threats faced by Talkative are:

- Human error or insider threats.
- Data breaches or leaks from cloud servers.
- Physical theft of devices or passes.
- External attacks such as hacking, DDoS, or malware targeting users.

Mitigation requires a combination of **training, technical controls, physical security, policies, and monitoring**. Continuous review ensures Talkative remains secure as the platform grows.