Lab1

Part A – Warm-up

1. **Availability**

   Availability is usually the hardest to maintain because systems must remain accessible at all times, even during hardware failures, maintenance, or attacks such as DDoS.

2. **Insider threats**

   Insider threats are serious because insiders already have legitimate access and system knowledge, allowing them to bypass many security controls, either maliciously or accidentally.

3. **100% security**

   A system can never be 100% secure because new vulnerabilities are constantly discovered and human error can never be fully eliminated.

Part B – CIA Triad Case Studies

Meta (Facebook) Data Leak

CIA	Asset	Actor	Vulnerability	Impact
Confidentiality	Personally Identifiable Information (names, phone numbers, emails)	External attacker	Poorly protected API / data scraping weakness	Large-scale exposure of user data, privacy loss

---

NHS WannaCry Attack

CIA	Asset	Actor	Vulnerability	Impact
Availability & Integrity	Hospital IT systems and patient records	Ransomware group	Unpatched Windows systems (EternalBlue)	Systems locked, appointments cancelled, risk to patient safety

Part C – Threat, Vulnerability, Exploit (TVE) Chains

Assets

1. Coursework submission files
2. Marks and written feedback
3. Student and staff user accounts

Asset 1: Coursework Files

- **Threat:** A student attempts to view, delete, or modify another student's submission.
- **Vulnerability:** Incorrectly configured access permissions on uploaded files.
- **Exploit:** Exploiting broken access control to access files they do not own.
- **Mitigation:** Enforce strict role-based access control and file ownership checks.

Asset 2: Marks and Feedback

- **Threat:** A malicious student tries to alter their grade.
- **Vulnerability:** Weak authentication or shared staff login credentials.
- **Exploit:** Password guessing or use of leaked staff credentials.
- **Mitigation:** Strong password policy, multi-factor authentication, and audit logging.

Asset 3: User Accounts

- **Threat:** External attacker compromises student or staff accounts.
- **Vulnerability:** Users reuse weak passwords and fall for phishing emails.
- **Exploit:** Phishing email leading to credential theft.
- **Mitigation:** Phishing awareness training and mandatory MFA.

Risk Explanation

These risks arise because the **likelihood** of attacks like phishing is high, and the **impact** of compromised accounts or altered marks is significant, resulting in a high overall risk.

Part D – Threat Dragon Mini-Task

- **External entity:** Student
- **Process:** Coursework submission system
- **Data store:** Coursework database
- **Data flow:** Coursework upload

Threats & Mitigations

- **Confidentiality:** Unauthorised access to submissions → access controls and encryption
- **Integrity:** Coursework modified after submission → hashing and timestamps
- **Availability:** System unavailable near deadlines → backups and redundancy

Wrap up

1. Difference between threat, vulnerability, and exploit

- **Threat:** A potential cause of harm (e.g. a hacker or malicious insider wanting to change marks).
- **Vulnerability:** A weakness in the system (e.g. weak passwords or misconfigured access control).
- **Exploit:** The method used to take advantage of the vulnerability (e.g. phishing or password guessing).

2. Concrete example of a risk chain

- **Threat:** External attacker wants to access student marks.
- **Vulnerability:** Students/staff reuse weak passwords.
- **Exploit:** Phishing email steals login credentials.
- **Impact:** Marks are accessed or modified, damaging integrity and trust.