

Week 2 Tutorial

The need for Security

Group Discussion and Analysis (60 minutes)

Each group may have up to three members.

Once the groups are formed, you will be allocated a group topic.

Scenario topics:

- 1- An online holiday booking system.
- 2- A medium size school timetabling and attendance system
- 3- An estate agent web application
- 4- A restaurant self-service digital ordering system

Each group to present their scenario and analysis to the class.

- a) Each group will analyse their assigned scenario in the context of potential security threats.

- 1- Identify Threats
- 2- Discuss and list potential threats to the system.
- 3- Categorise these threats in three categories
 - Internal threats: Threats originating from within the organization (e.g., employees, insider attacks, misconfigurations).
 - External threats: Threats coming from outside the organization (e.g., hackers, malware, DDoS attacks).
 - Incidental threats: Threats that are accidental in nature

- b) Classify Threats by Security Tenets

- 1- Each identified threat should be analysed based on which security tenet it violates:
 - Confidentiality – Unauthorised access to sensitive data.
 - Integrity – Data is altered or manipulated in an unauthorised manner.
 - Availability – Systems and data are not accessible when needed.
 - Non-repudiation – Users can deny their actions or transactions.
 - Accountability – The ability to track user actions is compromised.

c) Discussion Questions

- 1- What are the most critical threats in this scenario?
- 2- How do these threats impact the business and its users?
- 3- Are there existing measures that mitigate these threats?
- 4- What additional security measures could be implemented?

Presentation and Class Discussion (10 minutes each)

Each group will briefly present their findings, explaining:

- 5- The identified threats and how they are categorised.
- 6- The impact of these threats on security tenets.