Lecture One

General Introduction

1. The General Model for Information Security Risk

A general model for information security risk assessment identifies risk as a function of assets, threats, and vulnerabilities, often expressed as:

Risk = Assets × Threats × Vulnerabilities.

- **Assets:** Any piece of information or IT system that has value to an organization, such as data, hardware, software, and intellectual property.
- **Threats:** Potential events or actors that could exploit vulnerabilities to harm an asset, like malware, phishing, or natural disasters.
- **Vulnerabilities:** Weaknesses or flaws in systems or processes that could be exploited by a threat.
- **Attack:** Execution of the threat.
- **Impact (Incident):** The potential harm or negative consequences that could result from a security incident, affecting the business, reputation, or operations.

2. What is Cybersecurity Risk Management?

Cybersecurity risk management is a continuous, four-step process of *identifying*, *assessing*, *controlling*, and *monitoring* potential threats, vulnerabilities, and their potential impacts on an organization's information assets and systems.

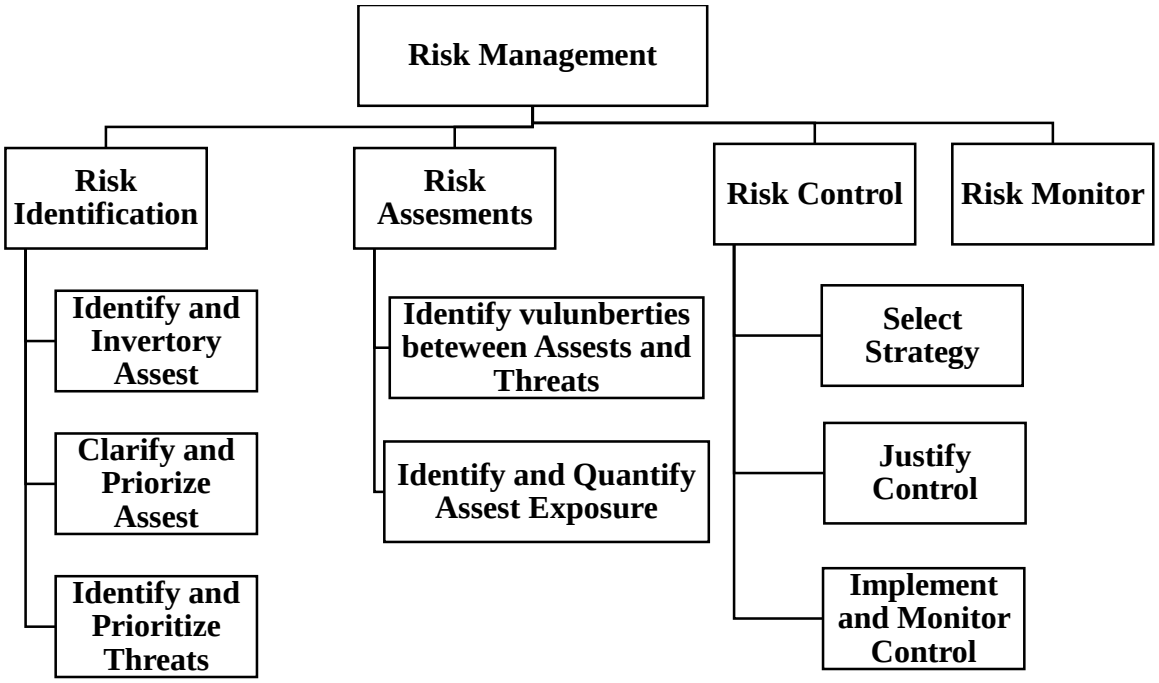

Figure 1: Components of Risk Management

The goal is to reduce the probability and impact of cyberattacks by implementing appropriate security controls, considering the organization's business goals and risk appetite, and adapting the strategy to the ever-changing threat landscape and regulatory environment.

2.1 Identify Risk:

To begin the process, risks must be identified, classified, and prioritized in terms of their probability to make an assessment and decision. The process of threat assessment identifies the risks each asset takes, after organizational assets have been identified. The components of risk identification are illustrated in Figure 2.

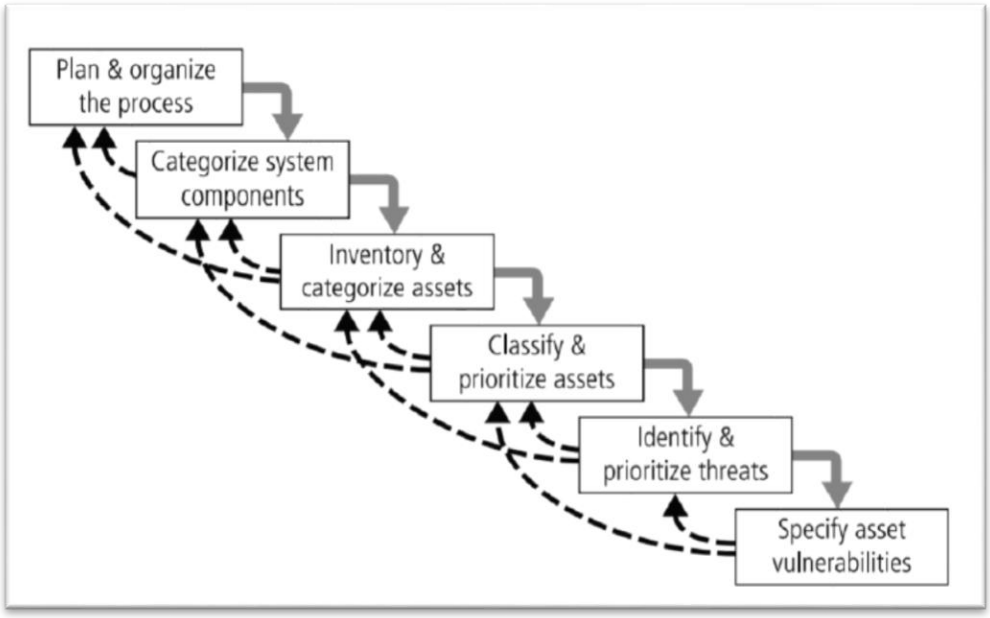

Figure 2: Components of Risk Identification

2.2 Assess Risk:

Analyze the identified risks to understand the *likelihood* of a threat exploiting a vulnerability and the potential impact on the organization.

Likelihood is the probability that an attacker would take advantage of a vulnerability. A *number* is assigned to the likelihood in a risk assessment. *Risk rating* is the result of multiplying likelihood by impact.

Risk rating = likelihood x impact

2.3 Control Risk:

Define and implement security controls, procedures, and technologies to *mitigate* the risks to an acceptable level.

The risk mitigation strategy is to minimize the impact of risks recommended from the risk assessment process. There are 3 types of plans to implement risk mitigation:

i. *Incident* response plan is a set of procedures to detect and mitigate unexpected events before or while an incident is in progress.

ii. *Disaster* recovery plan is the most common mitigation plan used to recover losses from any disaster or incident. Small to mid-sized businesses may also incorporate it as part of their business continuity plan.

iii. Business continuity plan is the most strategic plan that provides the continuation of a business in case of a natural disaster by ensuring the running of the IT system of an organization. It provides non-top running of the IT system in the midst of the crisis; however, the disaster recovery plan is focused on recovering the IT system to full functionality after a disaster occurs.

2.4 Monitor Risk:

Continuously review the effectiveness of controls and the risk landscape, making adjustments as needed to address new risks and changes in the environment.

3. Cybersecurity Risk Management Strategy

A cybersecurity risk management strategy implements four quadrants:

i. Map (Identify digital assets)

Discover and map all digital assets to quantify the attack surface. Use the map as a foundation to monitor cybercriminal activity.

ii. Monitor (Gather threat intelligence)

Search the public and dark web for threat references to your digital assets. Translate found threats into actionable threat intelligence.

iii. Mitigate (Block and remove threats)

Automated actions to block and remove identified threats to digital assets. Includes integration with other security initiatives in place.

iv. Manage (Prioritize and integrate defenses)

Manage the process used in the Map, Manage, and Mitigate quadrants. Enriching and prioritizing vulnerabilities in this step is also essential to successful digital risk protection.

4. What are the Benefits of Cybersecurity Risk Management?

Cybersecurity Risk Management provides ongoing monitoring, identification, and mitigation of the following threats:

i. Phishing Detection.
ii. VIP and Executive Protection.
iii. Brand Protection.
iv. Fraud Protection.
v. Sensitive Data Leakage Monitoring.
vi. Dark Web Activity.
vii. Automated Threat Mitigation.
viii. Leaked Credentials Monitoring.
ix. Malicious Mobile App Identification.
x. Supply Chain Risks.

5. Standards and Frameworks That Mandate a Cyber-Risk Management Approach

A risk management framework is a structured approach that organizations use to identify, assess, and mitigate risks while ensuring compliance with industry standards. These frameworks help businesses establish a systematic way to manage security, operational, financial, and regulatory risks. Popular risk management frameworks include: National Institute of Standards & Technology (NIST) Methodology, ISO 27005, ISO 31000, FAIR, OCTAVE, and COBRA.

6. Risk Categories:

Risk categorization is the process of classifying risks within an organization. By grouping similar risks.

i. **Strategic Risk:** Risks related to the organization's overall business strategy and goals, such as market changes or competitive pressures.

ii. **Operational Risk:** Risks arising from day-to-day business activities and processes, like equipment failure, human error, or supply chain disruptions.

iii. **Financial Risk:** Risks involving the organization's financial health, including credit risk, market volatility, and liquidity.

7. Examples:

Read the following scenario and answer the questions below:

a. *A hospital uses Wi-Fi to connect medical devices. The Wi-Fi network has a weak password. An unauthorized person tries to connect to the network and access patient records.*

1. What is the **asset**?
2. What is the **vulnerability**?
3. What is the **threat**?
4. What is the **attack**?
5. What is the **impact**?
6. What is the **control**?

Model Answer

1. **Asset:** Patient records and medical devices connected to the Wi-Fi.
2. **Vulnerability:** Weak Wi-Fi password.
3. **Threat:** Unauthorized person (intruder).
4. **Attack:** Intruder connects to Wi-Fi and attempts to access patient records.
5. **Impact:** Breach of patient privacy and damage to hospital reputation.
6. **Control:** Use strong Wi-Fi authentication

b) *A university professor keeps exam questions in a shared Google Drive folder without access restrictions. A student finds the link and downloads the exam before test day.*

1. What is the **asset**?
2. What is the **vulnerability**?
3. What is the **threat**?
4. What is the **attack**?
5. What is the **impact**?
6. What is the **control**?

Model Answer

1. **Asset:** Exam questions (confidential academic material).
2. **Vulnerability:** No access restrictions on the shared Google Drive folder.
3. **Threat:** Student with unauthorized access.
4. **Attack:** Student accesses and downloads the exam questions.
5. **Impact:** Loss of trust in the professor/university.
6. **Control:** Restrict file access (permissions), use secure learning management systems.