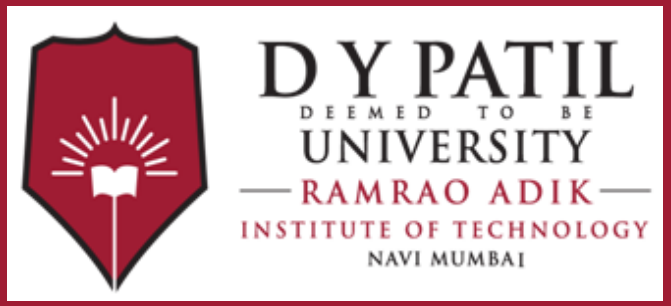


Subject Name: Information System

Unit No:01 Unit Name: Overview of Security Parameters

Faculty: Mrs. Bhavana Alte
Mr. Prathmesh Gunjgur

Implementation and Operational Issues; Security Life Cycle.

Operational Issues:

- When building security mechanisms for computer systems, it's crucial to balance **benefits** and **costs** while considering risks, laws, and societal norms.

- 1. **Cost-Benefit Analysis**
- Security mechanisms need to be worth the investment. If the cost of protecting an asset is higher than the value of the asset itself, the security mechanism might not be justified.
- **Example: Salary Database**
- **High Value**: A company's database stores salaries, used for issuing paychecks. If tampered with, employees might be paid wrong amounts, causing huge financial and reputation loss. Strong security is a must.
- **Low Value**: Copies of this database sent to branch offices . Even if altered, there's no direct impact. Protecting these copies isn't as critical.

2. Risk Analysis

- Protection decisions depend on analyzing potential threats and their likelihood. If a risk is small but the consequences are severe, prioritize it over frequent but low-impact risks.

- **Example: Database Risks**
- **On a Private Network**: If the database is only accessible within the company, the main risk is from insiders.

- **Connected to the Internet**: External attackers are now a threat. Security must address this higher risk.

3. Laws and Customs

- Legal constraints and societal norms dictate what security mechanisms can or should be implemented. A policy might be technically legal but socially unacceptable.

- **Examples:**
- **Cryptographic Laws**: In the past, U.S. companies couldn't send encryption software abroad without a government license. A system relying on encryption in a foreign office would need alternative plans.

- **Reading Files Without Permission**: System administrators tracking an attacker might inadvertently break the law by reading files they're not authorized to access. Many organizations require explicit user consent for such actions to avoid legal risks.

4. Psychological Acceptability

- If a security mechanism is too inconvenient, legally risky, or socially unacceptable, users will avoid it, rendering it useless.
- **Example:**
- Using long, complex passwords that are hard to remember may lead users to write them down, defeating the purpose of the security.
- **The balance between costs, risks, laws, and societal acceptance determines the success of security mechanisms. A system must be effective, practical, and acceptable to its users to truly protect data and resources.**

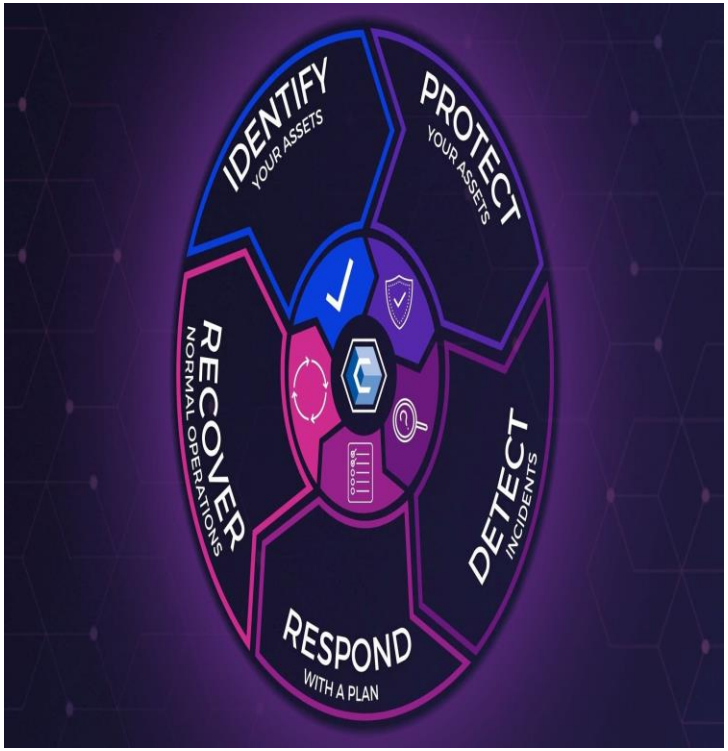
Security Life Cycle

- The **Security Life Cycle** describes the steps involved in managing security for a system or organization.
- It ensures security is not just implemented but maintained effectively over time.

Security Life Cycle

Simple Real-Life Analogy: Securing a House

- **Identify:** Determine valuables like money, documents, or jewelry that need protection.
- **Protect:** Install locks, security cameras, and an alarm system.
- **Detect:** Use motion sensors or cameras to notice intrusions.
- **Respond:** Call the police or trigger the alarm if someone breaks in.
- **Recover:** Fix broken locks and replace stolen items.
- **Review:** Regularly check the security system and upgrade locks if necessary.



The life cycle typically includes the following stages:……

- **1. Identify**
- This step involves understanding the assets that need protection, the risks they face, and the requirements for security.
- **Example:**
- A company identifies its **salary database** as a critical asset.
- It recognizes risks like unauthorized access, tampering, or data leaks.
- Security requirements include strong access controls and encryption to protect the data.

- **2. Protect**
- Once risks are identified, measures are implemented to secure the assets.
- **Example:**
- The company applies protections like:
  - Passwords for accessing the database.
  - Encryption for data stored and transmitted over the network.
  - Regular updates to the database system to fix vulnerabilities.

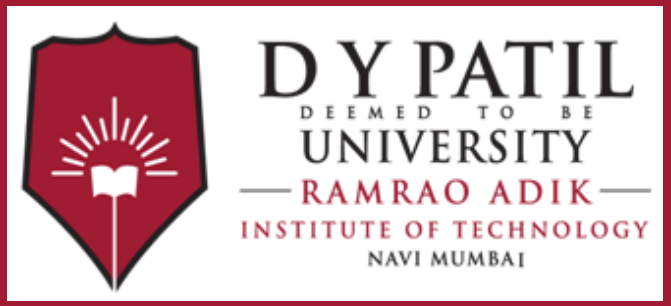
The life cycle typically includes the following stages:….

- **3. Detect**
- Even with protections in place, breaches can happen. This step involves monitoring and detecting suspicious activity.
- **Example:**
- The company installs tools to monitor database access.
- If an unusual login attempt is detected (e.g., multiple failed logins), the system sends an alert.

- **4. Respond**
- When an incident occurs, quick action is needed to minimize damage and address the issue.
- **Example:**
- If someone tries to hack into the database, the company:
  - Blocks the suspicious account immediately.
  - Investigates the source of the attack.
  - Notifies the IT team to take further action.

The life cycle typically includes the following stages:….

- **5. Recover**
- After an incident, the focus shifts to restoring normal operations and improving the system to prevent future incidents.
- **Example:**
- The company restores the database from a secure backup.
- It identifies how the breach occurred (e.g., weak passwords) and strengthens security, like requiring two-factor authentication.
- **6. Review**
- Periodically, the organization reviews its security measures to ensure they remain effective and adapt to new threats.
- **Example:**
- The company conducts a security audit every 6 months.
- New threats, like ransomware, are analyzed, and additional protections (e.g., regular backups) are implemented.
- **The Security Life Cycle is a continuous process to ensure assets are protected, risks are minimized, and security measures stay effective over time.**


D Y PATIL
DEEMED TO BE
UNIVERSITY
RAMRAO ADIK
INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

Thank You