DIPLOMA IN LAW ENFORCEMENT

DLE 2163: SECURITY RISK MANAGEMENT

Chapter 6

Identification of Threats

LEARNING OUTCOMES

Upon completion of the syllabus topics, students should be able to:

1. Identify the importance of risk management.
2. Demonstrate comprehension of various aspects of risk management.
3. Apply risk management techniques to risk management issues.
4. Demonstrate risk management skills in work.

VISION COLLEGE

TOPIC 6

Identification of Threats

VISION COLLEGE

Threat Identification

- Threat identification is a critical process in security management, aimed at recognizing and evaluating potential risks that could harm an organization, system, or individual. It involves identifying possible threats, understanding their nature, and assessing the likelihood and impact of their occurrence.

Threats to Information Security

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial of service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Example Threat List

- T01 Access (Unauthorized to System - logical)
- T02 Access (Unauthorized to Area - physical)
- T03 Airborne Particles (Dust)
- T04 Air Conditioning Failure
- T05 Application Program Change (Unauthorized)
- T06 Bomb Threat
- T07 Chemical Spill
- T08 Civil Disturbance
- T09 Communications Failure
- T10 Data Alteration (Error)
- T11 Data Alteration (Deliberate)
- T12 Data Destruction (Error)
- T13 Data Destruction (Deliberate)
- T14 Data Disclosure (Unauthorized)
- T15 Disgruntled Employee
- T16 Earthquakes
- T17 Errors (All Types)
- T18 Electro-Magnetic Interference
- T19 Emanations Detection
- T20 Explosion (Internal)
- T21 Fire, Catastrophic
- T22 Fire, Major
- T23 Fire, Minor
- T24 Floods/Water Damage
- T25 Fraud/Embezzlement
- T26 Hardware Failure/Malfunction
- T27 Hurricanes
- T28 Injury/Illness (Personal)
- T29 Lightning Storm
- T30 Liquid Leaking (Any)
- T31 Loss of Data/Software
- T32 Marking of Data/Media Improperly
- T33 Misuse of Computer/Resource
- T34 Nuclear Mishap
- T35 Operating System Penetration/Alteration
- T36 Operator Error
- T37 Power Fluctuation (Brown/Transients)
- T38 Power Loss
- T39 Programming Error/Bug
- T40 Sabotage
- T41 Static Electricity
- T42 Storms (Snow/Ice/Wind)
- T43 System Software Alteration
- T44 Terrorist Actions
- T45 Theft (Data/Hardware/Software)
- T46 Tornado
- T47 Tsunami (Pacific area only)
- T48 Vandalism
- T49 Virus/Worm (Computer)
- T50 Volcanic Eruption

Understanding the environment

- **Context Analysis**: Understand the environment you're protecting (e.g., an organization, IT system, or physical location). Identify valuable assets, such as data, physical infrastructure, intellectual property, and human resources.
- **Scope Definition**: Define the scope of what needs to be protected, including geographical locations, digital assets, and organizational processes.

Identify the potential threat

- **Internal Threats**: These originate from within the organization or system, such as insider threats (e.g., employees, contractors) or system failures.
- **External Threats**: These come from outside the organization, including hackers, competitors, natural disasters, and geopolitical events.
- **Human Threats**: Includes malicious activities like cyberattacks, espionage, and sabotage.
- **Natural Threats**: Events like earthquakes, floods, or pandemics.
- **Technological Threats**: Issues like system failures, outdated software, or vulnerabilities in technology.

Threat Analysis

- **Likelihood Assessment**: Evaluate how likely each threat is to occur. This might involve looking at historical data, current trends, and expert opinions.
- **Impact Assessment**: Analyze the potential impact of each threat if it were to materialize. Consider financial losses, reputational damage, operational disruption, and legal implications.
- **Risk Rating**: Combine the likelihood and impact assessments to prioritize threats. This helps in focusing resources on the most significant risks.

Documenting the threat

- **Threat Cataloging**: Create a detailed list or database of identified threats, including their characteristics, potential impact, and mitigation strategies.
- **Threat Modeling**: Use threat modeling techniques to map out how threats could exploit vulnerabilities, leading to different types of damage.

Ongoing Monitor and Update

Continuous Monitoring: Regularly monitor the environment for new threats or changes in existing ones.

Periodic Review: Update the threat identification process periodically to incorporate new information, such as emerging technologies, geopolitical shifts, or organizational changes.

Communication and Reporting

- **Stakeholder Communication**: Ensure that relevant stakeholders are informed about identified threats and the measures being taken to mitigate them.
- **Reporting**: Provide regular reports on threat status, including updates on mitigation efforts and any new threats.

Access Controls

- Specifically address admission of a user into a trusted area of organization.
- Access controls can be:
  - Mandatory
  - Nondiscretionary
  - Discretionary

Types of Access Controls

- **Mandatory Access Controls (MAC):**

❖ is the strictest of all levels of control.

❖ give users and data owners limited control over access to information.

❖ The design of MAC was defined, and is primarily used by the government.

❖ A user with top secret classification, for example, cannot access a resource if they are not also a member of one of the required categories for that object.

Types of Access Controls (continued)

- **Nondiscretionary controls/Role based access controls(RBAC):**

❖ managed by a central authority in organization; can be based on individual's role (role-based controls) or a specified set of assigned tasks (task-based controls).

❖ based on a user's job function within the organization to which the computer system belongs.

❖ For example, an accountant in a company will be assigned to the Accountant role, gaining access to all the resources permitted for all accountants on the system.

- **Discretionary Access Controls (DAC):**

❖implemented at discretion or option of data user.

❖allows each user to control access to their own data.

❖For example, User A may provide read-only access on one of her files to User B, read and write access on the same file to User C and full control to any user belonging to Group 1.

Documenting the Results of Risk Assessment

- Final summary comprised in ranked vulnerability risk worksheet.
- Worksheet details asset, asset impact, vulnerability, vulnerability likelihood, and risk-rating factor.
- Ranked vulnerability risk worksheet is initial working document for next step in risk management process: assessing and controlling risk.