Introduction to Risk Management

Assets, Threats, Vulnerabilities, and Risks

- An **asset** is composed of the people, property, and information within our organization (anything of value).

- A **threat** is anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

- A **vulnerability** is a weakness of an asset that can be exploited by a threat.

- A **risk** is a potential for loss, damage, or destruction of an asset when a threat exploits a vulnerability.

Risk Equation: Risk = Threat x Vulnerability

Introduction to Risk Management

The Basic Definition

- **Risk Management** is the process of identifying, assessing, monitoring and limiting risk to an acceptable level.

My Expanded Definition

- **Risk Management** provides a systematic and repeatable process for identifying, assessing, prioritizing, monitoring, tracking, and regularly communicating the status of threats, risks, issues, and actions items to management, stakeholders, and executive-level decision-makers.

Primary Goal

- Risks are reduced to a level that an organization will accept.

Risk Assessment

- A **risk assessment**, where risks are identified and assessed, is the first step in the risk management process.

- **Example Risk Assessment Process**:
    1. Identify and categorize your risks
    2. Assess each risk's probability and impact
    3. Assign each risk a risk score and prioritize accordingly
    4. Respond Accordingly

Qualitative Risk Assessment

Risk Assessment Score = Probability x Impact

- **Probability**: The likelihood that a risk will occur.
- **Impact**: The negative impact of a risk if it occurs.
- Probability and impact are given numbers to help categorize the severity of a risk, if realized.
- Based on the overall severity of risk, we can choose the appropriate risk response measure.

Impact	High (3)	3	6	9
	Moderate (2)	2	4	6
	Low (1)	1	2	3
		Low (1)	Moderate (2)	High (3)

Probability

Risk Response Categories

- **Avoidance**: The process of eliminating a risk by not engaging in an activity. We avoid a risk by eliminating its source altogether.

- **Acceptance**: Accepting an identified risk, meaning no action will be taken when a risk assessment score is low.

- **Mitigation**: The process of taking steps to minimize the impact of a risk.

- **Transference**: Transferring the responsibility of a risk to a third party, such as insurance.

- **Residual Risk**: The risk that remains when after risk mitigation or transference activities have taken place.

Exploring Risks and Threats

Exploring Risks and Threats

Risks

- Monetary
- Reputation
- Loss of Asset
- Intellectual Property
- Legal

Threats

- Natural
- Unintentional
- Intentional

Quantitative Risk Analysis

Qualitative vs. Quantitative Risk Analysis

- Qualitative and quantitative risk analysis are two different methods for analyzing risk:
    - **Qualitative**: More Subjective
    - **Quantitative**: More Objective

INSTRUCTOR
ALTON

Quantitative Risk Analysis Components

Component	Definition
Asset Value (AV)	The value of an asset.
Exposure Factor (EF)	The percentage loss of a specific asset if a risk is realized.
Single Loss Expectancy (SLE)	The monetary value expected from the occurrence of a risk on an asset. **Formula**: SLE = AV x EF
Annual Rate of Occurrence (ARO)	The estimated frequency of a threat occurring in a single year.
Annualized Loss Expectancy (ALE)	The expected monetary loss that can be expected from an asset due to a risk over a one year period. **Formula**: ALE = SLE x ARO

Quantitative Risk Analysis Example

Scenario: Your data center is valued at $500,000. If there is a major earthquake, you estimate 25% of the data center will be damaged. Your risk team estimates there will be a major earthquake once every ten years.

Would it be prudent to purchase earthquake insurance with an annual cost of $25,000?

- **AV** = $500,000
- **EF** = .25
- **SLE** = AV x EF = $500,000 x .25 = $125,000
- **ARO** = .10
- **ALE** = SLE x ARO = $125,000 x .10 = **$12,500**

No, the cost of the annual insurance premium is double the ALE, so you would be spending more than you expect to lose on an annual basis.

Attack Surface Analysis

Attack Surface Analysis

- An **attack surface** is a vulnerability. It’s any way an attacker can gain access to pose a security risk.
- There are three common attack surfaces:
  - Application
  - Network
  - User

- The greater the overall attack surface, the greater the overall risk.

Application Attack Surface

- When analyzing our applications for attack surfaces, we'll commonly look at:
  - The Amount of Code
  - Data Inputs
  - System Services
  - Network Communication Ports

Network Attack Surface

- When analyzing our network for attack surfaces, we'll commonly look at:
  - Overall Network Design
  - Placement of Mission Critical Servers & Systems
  - Placement & Configuration of Network Firewalls
  - Other Security-Related Devices & Services: IDS, IPS, VPN, etc.

User Attack Surface

- When analyzing our users for attack surfaces, we’ll commonly look at:
  - Effectiveness of Policies, Procedures and Training
  - Risk of Social Engineering
  - Potential for Human Error
  - Risk of Malicious Behavior