ITSEC

Saturday, June 11, 2022 12:30 PM

Risk Management
Risk

- potential for loss, damage or destruction of assets or data caused by a cyber threat.
- Planning

Risk Avoidance
Risk Management

- Process of identifying and controlling risks facing an org

Risk Identification

- Process of examining an org's current info tech security situation
- Identify and inventory assets
- Classify and prioritize assets
- Identify and prioritize assets

Risk Control

- Applying controls to reduce risks to an org's data and info system

Inherent Risk
Risk Management

- Risk Against Asset
- Know yourself
- Know the enemy
- Know your security posture

Risk Identification -> Risk Assessment -> Risk Control
STEPS

1. Identify
2. Classify
3. Valuate
4. Prioritize

THEN

1. Threat identify
2. Vulnerability id
3. Risk assessment

1. RISK IDENTIFICATION
   Components of RI
   a. Plan and organize the process
   b. Categorize system components
   c. Inventory and categorize assets
   d. classify and prioritize assets
   e. Identify and prioritize threats
   f. Specify asset vulnerabilities
   Examples
   a. Assets
      i. Data center
      ii. Portal
      iii. Community
      iv. Switch and router
      v. Rooms
   b. Traditional system components
      i. People
      ii. Procedure

        iii. Data
        iv. Software
        v. Hardware

2. DATA CLASSIFICATION AND MANAGEMENT
    - Varity of classification schemes used by corporate and military org
    - Info owners responsible for classifying their info assets
    - Info class must be reviewed periodically
    - For budget- prioritize
    - Confidential, internal, public data
    - Classification must be specific
    - Categories must be comprehensive
3. INFORMATION ASSET VALUATION
    - Ask questions
        - Is most criteria to organizations success
        - Generates the most revenue/profitability
        - Would be the most expensive to replace or protect
        - Would be the most embarrassing or greatest liability is revealed

4. INFORMATION PRIORITIZATION
    - Weighted factor analysis
    - Example
        - Criteria 1 - impact to revenue
        - Criteria 2 - profitability
        - Criteria 3 - public image
    - Weighted score increase also priority increase
    - Prioritizing threats
        - Threat assessment
            - Which threat present danger to assets
            - Which threat represents the most danger
        - Threat information security examples
            - Components to intellectual property
            - Explore or trespass
            - Forces of nature
            - Human error or failure
            - Info extortion

Vulnerability identification

Vulnerabilities

- Specific avenues threat agents can exploit to attack an info asset are called exploit vulnerabilities
- Examine how each threat could be perpetrated and list org's assets and vulnerabilities
- Process works best when people with diverse backgrounds within org work iteratively in a series of brainstorming sessions

Risk Assessment

- Evaluates the relative risk for each vulnerability
- Assigns a risk rating or score to each info assets
- The goal at this point create a method for evaluating the relative risk of each listed vulnerability

Risk Determination

Risk = likelihood of occurrence * value of the info asset - % of risk mitigated by current controls + uncertainty of current knowledge of vulnerability

In short R=L+AV(L)-C(L)+U(L)

Likelihood (0.1-1.0)