

Risk Management

Dr. Shahzada Khurram

Risk Management

It is a Process of identifying and assessing risk, reducing it to an acceptable level

○ **Risk Assessment** – Method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement the security controls

○ **Risk Analysis**

- The process by which the goals of risk management are achieved
- Includes examining an environment for risk, evaluating each threat event to its likelihood and the cost of damage, creating cost/benefit report for safeguards to present to management.
- Carried out after risk assessment; ensures security is cost-effective, relevant, timely and responsive to the threats
- Helps prioritize risks and shows management the amount of resources needed to protect in a sensible manner.

○ 4 main goals of risk analysis

1. Identify Assets and their values to the organization
2. Identify vulnerabilities and threats
3. Quantify the probability and business impact of these potential threats
4. Provide cost benefit analysis of the safeguard

- Risk Analysis must be supported and directed by senior management
- Management must define the purpose and scope of analysis, appoint a team to carry out assessment and allocate necessary resources
- Risk Analysis helps integrate the security objectives with the business objectives

Risk Terminologies

Asset

- Anything that has value

Threat

- Any potential occurrence that may cause an undesirable outcome on the asset

Threat Agent

- The entity that takes advantage of the vulnerability

Vulnerability

- Weakness in an asset or absence/weakness in the control measure

Exposure

- Being susceptible to asset loss due to threat; instance of threat taking advantage of vulnerability; always measured in %

Risk

- Likelihood threat will exploit the vulnerability;
 $\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{impact}$

Safeguard

- Anything that removes or reduces a vulnerability or protects against threat

Total Risk

$\text{Threat} \times \text{Vulnerability} \times \text{Asset Value}$

Residual Risk

- $= \text{Total Risk} - \text{Countermeasures.}$

Asset Valuation

- Aspects to consider when assigning value to the assets
 - Cost to acquire or develop
 - Cost to maintain and protect
 - Value to owner and users
 - Price others are willing to pay
 - Cost to replace the asset if lost
 - Operational and production activities affect if the asset is not available
 - Liability issues if the asset is compromised
 - Usefulness and role of the asset in the organization

- There are two types of Risk analysis

- Qualitative Risk Analysis

- Quantitative Risk Analysis

Qualitative Risk Analysis

- Uses a softer approach to Risk analysis

- It does not quantify the data, does not use calculations

- It is more opinion and scenario based and uses rating system

- Techniques include judgement, best practices, intuition, and experience

- Methods

- Brainstorming, storyboarding, focus groups, surveys,

- questionnaire, checklists, one-on-one meetings, Interviews

Qualitative Risk Analysis

- Qualitative Risk Analysis with the Risk Analysis Matrix.
- Pick an asset: A **laptop**.
 - How likely is one to get stolen or left somewhere? I would think possible or likely.
 - How bad is it if it happens?
- That really depends on a couple of things:
 - Is it encrypted?
 - Does it contain classified or PII/PHI content?
 - Let's say it is likely and a minor issue, that puts the loss the high-risk category.
- It is normal to move high and extreme on to quantitative risk analysis. If mitigation is implemented, we can maybe move the risk level to "Low" or "Medium".

Where the L, M, H, E is for your organization can be different from this.

L = Low, M = Medium, H = High, E = Extreme Risk

		Consequences				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Almost Certain	H	H	E	E	E
	Likely	M	H	H	E	E
	Possible	L	M	H	H	E
	Unlikely	L	L	M	H	E
	Rare	L	L	M	H	H

Quantitative Risk Analysis

Quantitative Risk Analysis – We want exactly enough security for our needs.

- This is where we put a number on that.
- We find the asset's value: How much of it is compromised, how much one incident will cost, how often the incident occurs and how much that is per year.
- Asset Value (**AV**) – How much is the asset worth?
- Exposure factor (**EF**) – Percentage of Asset Value lost?
- Single Loss Expectancy (**SLE**) – (**AV** x **EF**) – What does it cost if it happens once?
- Annual Rate of Occurrence (**ARO**) – How often will this happen each year?
- Annualized Loss Expectancy (**ALE**) – This is what it cost per year if we do nothing.
- Total Cost of Ownership (**TCO**) – The mitigation cost: upfront + ongoing cost (Normally Operational)

Quantitative Risk Analysis

- Let's look at a few examples.
- Risk Analysis: Laptop – Theft/Loss (unencrypted)**

	Value
Asset Value (AV)	\$10,000
Exposure factor (EF)	100%
Single Loss Expectancy (SLE) – (AV x EF)	\$10,000
Annual Rate of Occurrence (ARO)	25
Annualized Loss Expectancy (ALE)	\$250,000

The Laptop (\$1,000) + PII (\$9,000) per loss (AV)

(AV) It is a 100% loss, it is gone (EF)

Loss per laptop is \$10,000 (AV) x 100% EF) = (SLE)

The organization loses 25 Laptops Per Year (ARO)

The annualized loss is \$250,000 (ALE)

Data Center – Flooding

	Value
Asset Value (AV)	\$10,000,000
Exposure factor (EF)	15%
Single Loss Expectancy (SLE) – (AV x EF)	\$1,500,000
Annual Rate of Occurrence (ARO)	0.25
Annualized Loss Expectancy (ALE)	\$375,000

The Data Center is valued at \$10,000,000

If a flooding happens 15% of the DC is
compromised (EF)

Loss per Flooding is \$10,000,000 (AV) x 15% EF)= (SLE)

The flooding happens every 4 years = 0.25

The annualized loss is \$375,000 (ALE)

For the example **let's use a 4-year tech refresh cycle.**

- Full disk encryption software and support = \$75,000 initial and \$5,000 per year.
- Remote wipe capabilities for the laptop = \$20,000 initial and \$4,000 per year.
- Staff for encryption and help desk = \$25,000 per year

Doing nothing costs us \$1,000,000 per tech refresh cycle (**\$250,000 per year**).

- Implementing full disk encryption and remote wipe will cost \$231,000 per tech refresh cycle (\$57,750 per year)
- The laptop hardware is a 100% loss, regardless. What we are mitigating is the **25 x \$9,000 = \$225,000** by spending \$57,750.
- This is our ROI (Return On Investment): **TCO (\$57,750) < ALE (\$250,000)**. This makes fiscal sense, we should implement.

Types of risk responses:

- **Accept the Risk** – We know the risk is there, but the mitigation is more costly than the cost of the risk (Low risks). We ensure we have a paper trail, and this was a calculated decision.
- **Mitigate the Risk (Reduction)** – The laptop encryption/wipe is an example – acceptable level (Leftover risk = Residual).
- **Transfer the Risk** – The insurance risk approach – We could get flooding insurance for the data center, the flooding will still happen, we will still lose 15% of the infrastructure, but we are insured for cost.
- **Risk Avoidance** – We don't issue employees laptops (if possible) or we build the data center in an area that doesn't flood. (Most often done before launching new projects – this could be the data center build).
- **Risk Rejection** – You know the risk is there, but you are ignoring it. This is **never** acceptable. (You are liable).
- **Secondary Risk** – Mitigating one risk may open up another risk.

NIST 800-30

- **NIST 800-30** - National Institute of Standards and Technology. A Special Publication defines A 9-step process for Risk Management.
 1. System Characterization (Risk Management scope, boundaries, system and data sensitivity).
 2. Threat Identification (What are the threats to our systems?).
 3. Vulnerability Identification (What are the vulnerabilities of our systems?).
 4. Control Analysis (Analysis of the current and planned safeguards, controls and mitigations).
 5. Likelihood Determination (Qualitative – How likely is it to happen)?
 6. Impact Analysis (Qualitative – How bad is it if it happens? Loss of CIA).
 7. Risk Determination (Look at 5-6 and determine Risk and Associate Risk Levels).
 8. Control Recommendations (What can we do to Mitigate, Transfer, ... the risk).
 9. Results Documentation (Documentation with all the facts and recommendations).



Thank you