Sri Lanka Institute of Information Technology

Quantitative Risk Analysis - Exercise

Individual Assignment

IE3052 -Information Security Risk Management

Submitted by:

Student Registration Number	Student Name
IT19003610	**K.G.S.SHIRANTHAKA**

Date of submission:

2 May 2021

Exercise (Week 7 - Tutorial)

You are tasked with conducting a quantitative risk assessment for a local software developing organization. Key information about the organization is given and you shall use the provided data tables for your calculations. Calculate SLE, ALE and propose countermeasures for each scenario. Calculate countermeasure cost/benefit analysis by calculating the difference between the ALE prior to implementing the countermeasure to the ALE after implementing the countermeasures.
In each section you can introduce your suggestions (assets, risk factors & threat scenarios)
Note: Each team will get different answers for latter calculations. Why? Clearly state your assumptions.

Part 1

TechnoCode Pvt Ltd. is a small software developing company. An initial evaluation was done to identify critical assets of the organization along with their values.

Critical Assets & their Values

- Customer Information Server – Rs. 350,000/=
- Software Developing Platform Server – Rs. 750,000/=
- Middleware Platform (software) with licensed OS – Rs. 800,000/=
- Patented Software Design Blueprints - Rs. 1,000,000/=
- Senior Software Developer (Team Leader) – **Rs. 130, 000/=**
- **Storage Servers - Rs. 385, 000/=**
- **Air Condition System (For entire system) - Rs. 500, 000/=**

A vulnerability study has indicated that the following 5 are the top risk factors.

Top Risk factors

- DoS Attack Servers
- Virus Attacks for Software
- Intellectual Property Theft

- **Customer Information can disclosure.**
- **Phishing and Social engineering attacks and threats**
- **Failure of Air-condition system**

Data Table

Following information is extracted from various security sources.

Risk/Threat Scenario	**Source**	**ARO**	**Exposure Factor**
Denial of Service	CSI	0.4	22%
Virus Infection	Symantec	0.28	15%
Theft of Intellectual Property	CSI	0.20	8%
Information Disclosure of Customer Information	CSI	0.28	12%
Phishing and Social engineering attacks and threats	-	0.5	25%
Failure of Air-condition system	CSI	0.4	50%

Part 2

- Calculate SLE for each threat scenario.
- Calculate ALE
- Suggest suitable countermeasures.
- Conduct safeguard cost/Benefit Analysis.
- Suggest Implementation of countermeasures according to their priority & ROI.

1. Threat Scenario: Denial of Service

Assets

- Customer Information Server – Rs.350, 000/=
- Software Developing Platform Server – Rs.750, 000/=

Suitable Countermeasures

- Implement firewall and Denial of Service (DoS) protection such as Cloudflare.

Cost = Rs. 40,000/=

Calculations

Before Applying Controls	**After Applying Controls**
Asset Value = 350,000 + 750, 000 **Asset Value = 1, 100, 000**	Asset Value = 350,000 + 750, 000 **Asset Value = 1, 100, 000**

SLE = Asset Value * EF (Exposure Factor)
SLE = 1, 100, 000 * 22%
SLE = 242, 000
	SLE = Asset Value * EF (Exposure Factor)
	SLE = 1, 100, 000 * 12%
	SLE = 132, 000

ARO = 0.4	**ARO = 0.4**

ALE = SLE * ARO
ALE = 242, 000 * 0.4
ALE = 96, 800
	ALE = SLE * ARO
	ALE = 132, 000 * 0.4
	ALE = 52, 800

Calculations Summary

Key Terms	**Before Applying Controls**	**After Applying Controls**	
EF	22%	EF	12%
SLE	Rs. 242, 000	SLE	Rs.132, 000
ARO	0.4	ARO	0.4
ALE	Rs. 96, 800	ALE	Rs. 52, 800

Safeguard Cost Benefit Analysis = (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard)

= 96, 800 – (52, 800 + 40, 000) = Rs. 4, 000/=

2. **Threat Scenario: Virus Infection**

Assets

- Middleware Platform (software) with licensed OS – Rs. 800, 000/=

Suitable Countermeasures

- Implement the enterprise standard malware protection software and update the operating system.

Cost = Rs. 20, 800/=

Calculations

Before Applying Controls	**After Applying Controls**
Asset Value = 800, 000	**Asset Value = 800, 000**

SLE = Asset Value * EF (Exposure Factor)
SLE = 800, 000 * 15%
SLE = 120, 000
	SLE = Asset Value * EF (Exposure Factor)
	SLE = 800, 000 * 5%
	SLE = 40, 000

ARO = 0.28	**ARO = 0.15**

ALE = SLE * ARO
ALE = 120, 000 * 0.28
ALE = 33, 600
	ALE = SLE * ARO
	ALE = 40, 000 * 0.15
	ALE = 6, 000

Calculations Summary

Key Terms	**Before Applying Controls**	**After Applying Controls**	
EF	15%	EF	5%

SLE	Rs. 120, 000	SLE	Rs. 40, 000
ARO	0.28	ARO	0.15
ALE	Rs. 33, 600	ALE	Rs. 6, 000
Safeguard Cost Benefit Analysis = (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) **= 33, 600 – (6, 000 + 20, 800) = Rs. 6,800/=**			

3. **Threat Scenario: Theft of Intellectual Property**

Assets

- Patented Software Design Blueprints – Rs.1,000, 000/=

Suitable Countermeasures

- Prioritize Intellectual Property and Trade Secret Protection

Cost = Rs. 9, 000/=

Calculations

Before Applying Controls	**After Applying Controls**
Asset Value = 1, 000, 000	**Asset Value = 1, 000, 000**

SLE = Asset Value * EF
SLE = 1, 000, 000 * 8%
SLE = 80, 000
	SLE = Asset Value * EF
	SLE = 1, 000, 000 * 3%
	SLE = 30, 000

ARO = 0.20	**ARO = 0.20**

ALE = SLE * ARO
ALE = 80, 000 * 0.20
ALE = 16, 000
	ALE = SLE * ARO
	ALE = 30, 000 * 0.20
	ALE = 6,000

<u>Calculations</u>

Key Terms	**Before Applying Controls**	**After Applying Controls**	
EF	8%	EF	3%
SLE	Rs. 80, 000	SLE	Rs. 30, 000
ARO	0.20	ARO	0.20
ALE	Rs. 16, 000	ALE	Rs. 6, 000
Safeguard Cost Benefit Analysis = (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) **= 16, 000 – (6, 000 + 9, 000) = Rs. 1, 000/=**			

4. **Threat Scenario: Information Disclosure of Customer Information**

<u>Assets</u>

- Storage Servers – Rs. 385, 000/=

<u>Suitable Countermeasures</u>

- Upgrade the Storage Server and update server control panel regularly.

Cost = Rs. 7, 000/=

<u>Calculation Summary</u>

Before Applying Controls	**After Applying Controls**
Asset Value = 385, 000	**Asset Value = 385, 000**

SLE = Asset Value * EF
SLE = 385, 000 * 12%
SLE = 46, 200
	SLE = Asset Value * EF
	SLE = 385, 000 * 5%
	SLE = 19, 250

ARO = 0.28	**ARO = 0.15**

ALE = SLE * ARO
ALE = 46, 200 * 0.28
ALE = 12, 936
	ALE = SLE * ARO
	ALE = 19, 250 * 0.18
	ALE = 3, 465

Calculations

Key Terms	**Before Applying Controls**	**After Applying Controls**	
EF	12%	EF	5%
SLE	Rs. 46, 200	SLE	Rs. 19, 250
ARO	0.28	ARO	0.18
ALE	Rs. 12, 936	ALE	Rs. 3, 465
Safeguard Cost Benefit Analysis = (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) **= 12, 936 – (3, 465 + 7,000) = Rs. 2, 471/=**			

5. **Threat Scenario: Phishing and Social engineering attacks and threats**

Assets

- Senior Software Developers (Team Leader) – Rs. 130, 000/=

Suitable Countermeasures

- Train and maintain the workshops for security awareness.
- Deploy a SPAM filter that detects malware and virus.

Cost = Rs. 12,000/=

Calculations

Before Applying Controls	**After Applying Controls**
Asset Value = 130, 000	**Asset Value = 130, 000**

SLE = Asset Value * EF
SLE = 130, 000 * 25%
SLE = 32, 500
	SLE = Asset Value * EF
	SLE = 130, 000 * 10%
	SLE = 13, 000

ARO = 0.5	**ARO = 0.2**

ALE = SLE * ARO
ALE = 32, 500 * 0.5
ALE = 16, 250
	ALE = SLE * ARO
	ALE = 13, 000 * 0.2
	ALE = 2, 600

Calculations Summary

Key Terms	**Before Applying Controls**	**After Applying Controls**	
EF	25%	EF	10%
SLE	Rs. 32, 500	SLE	Rs.13, 000
ARO	0.5	ARO	0.2
ALE	Rs. 16, 250	ALE	Rs. 2, 600
Safeguard Cost Benefit Analysis = (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) **= 16, 250 – (2, 600 + 12, 000) = Rs. 1, 650/=**			

6. Threat Scenario: Failure of Air-Condition System

Assets

Air-condition system (for entire system) – Rs. 500, 000/=

Suitable Countermeasures

Repair the Air-Condition system.

Cost = Rs.25, 000/=

Calculation Summary

Before Applying Controls	**After Applying Controls**
Asset Value = 500, 000	**Asset Value = 500, 000**

SLE = Asset Value * EF
SLE = 500, 000 * 50%
SLE = 250, 000
	SLE = Asset Value * EF
	SLE = 500, 000 * 30%
	SLE = 150, 000

ARO = 0.4	**ARO = 0.3**

ALE = SLE * ARO
ALE = 240, 000 * 0.4
ALE = 100, 000
	ALE = SLE * ARO
	ALE = 150, 000 * 0.3
	ALE = 45, 000

Key Terms	Before Applying Controls	After Applying Controls	
EF	50%	EF	30%
SLE	Rs. 250, 000	SLE	Rs. 150, 000
ARO	0.4	ARO	0.3
ALE	Rs. 100, 000	ALE	Rs. 45, 000
Safeguard Cost Benefit Analysis = (ALE before implementing safeguard) – (ALE after			

implementing safeguard) – (annual cost of safeguard)

= 100, 000 – (45, 000 + 25, 000) = Rs. 30, 000/=

Exposure Factor (EF) Calculations

Start off with 100% for the starting exposure factor and answer each of the following questions …

1. Does the system under attack have any redundancies/ backups/ copies?

- Subtract 30% if the answer is YES.

2. Is the system under attack behind a firewall?

Subtract 10% if the answer is YES.

3. Is the attack from outside?

- Subtract 20% if the answer is YES.

4. What is the potential rate of attack? (10% damage / hour vs. 10% damage / min)

- Subtract 20% if the answer is less than 20% damage/hr
- Subtract 40% if the answer is less than 2% damage/hr

5. What is the likelihood that the attack will go undetected in time for a full recovery?

- Subtract 10% if the probability of being undetected is less than 20%
- Subtract 30% if the probability of being undetected is less than 10%

6. How soon can a countermeasure be implemented in time if at all?

- Subtract 30% if the countermeasure can be implemented within ½ hour.
- Subtract 20% if the countermeasure can be implemented within 1 hour.
- Subtract 10% if the countermeasure can be implemented within 2 hours.

<u>Suggest Implementation of countermeasures according to their priority & ROI.</u>

Threat	Assets	Countermeasures according to their priority
Denial of Service	Customer Information Server	• Implement firewall and DOS protection. • Maintain Backup regularly • Monitor the unwanted behavior of the network traffic
	Software Developing Platform Server	
Virus Infection	Middleware Platform (software) with licensed OS	• Implement the enterprise standard malware protection software and update the operating system. • Maintain the Backup regularly
Theft of Intellectual Property	Patented Software Design Blueprints	• Prioritize Intellectual Property and Trade Secret Protection • Follow the government rules and regulations. • Work and projects should be protected with copyrights act.
Information Disclosure of Customer Information	Storage Servers	• Upgrade the Storage server • Vulnerability Assessment and Penetration testing process periodically • System hardening and best security practices.
Phishing and Social engineering attacks and threats	Senior Software Developer (Team Lead)	• Create standard policies and introduce those policies to employees by conducting awareness sessions. • Implement a SPAM filter for filtering viruses.

		- Create incident response plan and team.
Failure of Air-condition system	Air-condition system (for entire system)	- Repair the System checking the status prodically. - Audit the assets periodically via internal audits and external audit process.