Assignment

Aditya Aravind Medepalli

CYBER-5230-24 Intrusion Detection and Analysis

Saint Louis University

April 1st, 2023

RISK MANAGEMENT

Complete the following tasks:

1. Asset identification and classification – Complete table below

ASSET

i. Identify assets (column A) at your company, including at least one in each:

	ASSET	Value - C,H,M,L	Numeric Value 1-10
People	CTO HR Manager	C H	10 8
Data and information	Financial Reports	C	10

Procedures	Producat development Process	H	8
Software	QuickBooks Slack	H M	7 3
Hardware	Server	C	10

ii. Value - for each asset, list whether it is critical, high, medium, or low

Asset Value		
CRITICAL	Compromise to assets would have grave consequences leading to loss of life, serious injury, or mission failure	10
HIGH	Compromise to assets would have serious consequences that could impair operations for a significant period of time	7-9
MEDIUM	Compromise to assets would have moderate consequences that could impair operations for a limited period of time	5-6
LOW	Compromise to assets would have little or no impact on the continuation of operations	1-3

iii. Asset valuation – Determine the numeric value of identified assets – Use personal judgment – Keep mission of the corporation in mind

Asset Analysis: Valuation Elements to Consider:

✓ Cost of Producing the Asset

✓ Value of the Information/Service on the Open Market

✓ Cost of Reproducing the Asset if Destroyed

✓ Benefit the Asset Brings to the company in Meeting the Mission

- ✓ Repercussion to the company if the Information and Services were not Readily Available
- ✓ Advantage Given to Someone if They Could Use, Change, or Destroy the Asset
- ✓ Cost if Information is Released, Altered, or Destroyed (Litigation)
- ✓ Loss of Confidence if Information is not Held & Processed Securely

THREATS

a. List and identify actions threats, examples:

- ✓ Act of human error or failure,
- ✓ Compromise of intellectual property
- ✓ Deliberate acts of espionage
- ✓ Deliberate acts of information extortion
- ✓ Sabotage, vandalism, theft
- ✓ Software attacks
- ✓ Forces of nature
- ✓ Technical hardware failures
- ✓ Software failures
- ✓ Technological obsolescence

	THREAT	Value - C,H,M,L	Numeric Value 1-10
	Hacking	C	9
	Insider Threat	C	9

	Employee fraud	H	8
	Lawsuit	M	6
	Embezzlement	H	7
	Property theft	M	7
	phishing	H	8

b. *Value- for each threat, list whether it is critical, high, medium, or low. The threat rating is a subjective judgment based on existence, capability, history, intention, and targeting.*

Threat Value		
Critical	Critical- Known aggressors or hazards, highly capable of causing loss or damage exist. One or more vulnerabilities are present. The threat source is known to having intent and means.	10
High	High – Known aggressors or hazards, capable of causing loss or damage to the school exist. One or more vulnerabilities are present and the aggressors are known or reasonably suspected having intent and means.	7-9
Medium	Medium - Known aggressors or hazards that may be capable of causing loss or damage exist. One or more vulnerabilities may be present; however, the aggressors are not believed to have intent.	5-6
Low	Low - Few or no aggressors or hazards exist. Their capability of causing damage is doubtful.	1-3

c. *Threat valuation – Determine the numeric value of identified assets – Use personal judgment – Keep mission of the entity in mind*

Vulnerabilities

a. List and identify vulnerabilities, examples:

- Human
- Operational – insufficient security procedures
- Informational vulnerabilities
- Facility – weak physical location and geographical
- Equipment

	Vulnerabilities	Value - C,H,M,L	Numeric Value 1-10
	Social Engineering	M	7
	Ransomware	C	10
	Unauthorized access	H	9
	Data Leakage	H	9
	Malware	H	8

	Brute Force Attacks	M	6

a. Value- for each vulnerability, list whether it is critical, high, medium, or low. The threat rating is a subjective judgment based on existence, capability, history, intention, and targeting.

Vulnerability Value		
Critical	No known countermeasures and adversary capability exists	10
High	No known countermeasures and adversary capability exists	7-9
Medium	There are effective countermeasures in place, but adversaries can exploit a weakness	5-6
Low	Multiple levels of countermeasures exist and few or no adversaries could exploit the asset	1-3

d. Vulnerability valuation – Determine the numeric value of identified assets – Use personal judgment – Keep mission of the entity in mind.

RISKS

Risk = Asset Value x Threat Rating x Vulnerability Rating

Risk	Risk Rating
>260	Critical

141-260	High
101-140	Medium
1-100	Low

Risk Rating Table

Risk Assessment: Fill out the table below based on the asset value, threat, and vulnerability assessment examples presented earlier. All italic values should be replaced with your own data. After completing, color code using the table above

	Threats				
Assets	***Threats***	**Risk = Asset Value x Threat Rating x Vulnerability Rating**		***Risk Assessment***	
Asset 1	***People***				
Asset Value Rating	**10**	**630**		**Critical**	
Threat Rating	**9**				
Vulnerability Rating	**7**				
Asset 2	***Data and Information***				
Asset Value Rating	**10**	**800**		**Critical**	
Threat Rating	**8**				
Vulnerability Rating	**10**				
Asset 3	***Procedures***				
Asset Value Rating	**8**	**432**		**Critical**	
Threat Rating	**6**				
Vulnerability Rating	**9**				