Lab 4: Perform a Qualitative Risk Assessment for an IT Infrastructure

Course Name: Risk Management in Information Systems (IAA202)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 8/2/2023

Part A – Perform a Qualitative Risk Assessment for an IT Infrastructure

Overview
The following risks, threats, and vulnerabilities were found in an IT infrastructure. Your Instructor will assign you one of four different scenarios and vertical industries each of which is under a unique compliance law.

1. Scenario/Vertical Industry:
   a. Healthcare provider under HIPPA compliance law

2. Given the list, perform a qualitative risk assessment by assigning a risk impact/risk factor to each of identified risks, threats, and vulnerabilities throughout the seven domains of a typical IT infrastructure that the risk, threat, or vulnerability resides

Risk – Threat – Vulnerability	Primary Domain Impacted	Risk Impact/Factor
Unauthorized access from public Internet	Remote Access	1
User destroys data in application and deletes all files	System/Application	3
Hacker penetrates your IT infrastructure and gains access to your internal network	LAN-to-WAN	1
Intra-office employee romance gone bad	User	3
Fire destroys primary data center	System/Application	1
Service provider SLA is not achieved	WAN	3
Workstation OS has a known software vulnerability	Workstation	2
Unauthorized access to	Workstation	1

organization owned workstations		
Loss of production data	System/Application	2
Denial of service attack on organization DMZ and e-mail server	LAN-to-WAN	1
Remote communications from home office	Remote Access	2
LAN server OS has a known software vulnerability	LAN	2
User downloads and clicks on an unknown	User	1
Workstation browser has software vulnerability	Workstation	3
Mobile employee needs secure browser access to sales order entry system	User	3
Service provider has a major network outage	WAN	2
Weak ingress/egress traffic filtering degrades performance	LAN-to-WAN	3
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	User	2
VPN tunneling between remote computer and ingress/egress router is needed	LAN-to-WAN	2
WLAN access points are needed for LAN connectivity within a warehouse	LAN	3
Need to prevent eavesdropping on WLAN due to customer privacy data access	LAN	1
DoS/DDoS attack from the WAN/Internet	WAN	1

3. For each of the identified risks, threats, and vulnerabilities, prioritize them by listing a “1”, “2”, and “3” next to each risk, threat, vulnerability found within each

of the seven domains of a typical IT infrastructure. “1” = Critical, “2” = Major, “3” = Minor.

- **User Domain Risk Impacts:** 4
- **Workstation Domain Risk Impacts:** 3
- **LAN Domain Risk Impacts:** 3
- **LAN-to-WAN Domain Risk Impacts:** 4
- **WAN Domain Risk Impacts:** 4
- **Remote Access Domain Risk Impacts:** 2
- **Systems/Applications Domain Risk Impacts:** 3

4. Craft an executive summary for management using the following 4-paragraph format.

From Exercise 3, skilled were issues accompanying all of the seven domains of the IT infrastructure the User Domain Risk Impacts was about four; Workstation Domain Risk Impacts was about three; LAN Domain Risk Impacts were about three; LAN-to-WAN Domain Risk Impacts were about four; WAN Domain Risk Impact were about four; Remote Access Domain Risk Impact were about two; and Systems/Applications Domain Risk Impacts were about three. These risks, dangers and exposures that were raised inside your IT foundation are categorized from the detracting to the acquired information type. These risks, threats and vulnerabilities will be examined later in more detail in this summary of our finds for your institution.

The following risks, threats and vulnerabilities were erect to inside your arrangement of these skilled were six accompanying a grade fault-finding; unauthorized access from public Internet; fire destroys primary data center; denial of service attack on organization DMZ and e-mail server; Hackers penetrates your IT infrastructure and gain access to your internal network; service provider has a major network outage; LAN server OS has a known software vulnerability and DoS/DDoS attack from the WAN/Internet. These critical range risks, threats and vulnerabilities need expected discussed first before some remainder of something. Skilled needs expected plans sink motion to address these issues start cognizant area and the habit until above administration. The following risks, threats and vulnerabilities were raise to inside your institution of these skilled were five accompanying a grade big; user destroys data in application and deletes all files; user destroys data in application and deletes all files; loss of production data; workstation browser has software vulnerability; VPN tunneling between remote computer and ingress/egress router is needed and WLAN access points are needed for LAN connectivity within a warehouse. These detracting range risks, threats and

vulnerabilities need expected called second before some remainder of something. Skilled needs expected plans implant motion to address these issues start cognizant area and the habit until above administration. Minor range risks, threats and vulnerabilities need expected called second before some possible choice. Skilled needs expected plans sink motion to address these issues start cognizant area and the habit until above administration.

The verdicts of the amount establish that skilled was enough to affect all of the IT rules for this institution. Few of these risks, warnings and exposures manage to have a negative effect on institution development in the misfortune of loss of data, profits and company integrity.

The next steps would be to address the critical issues first base on the impact on the IT network of the organization and weighing the cost of these issues.

PART B - Perform a Qualitative Risk Assessment for an IT Infrastructure

Overview

Answer the following Lab #4 – Assessment Worksheet questions pertaining to your qualitative IT risk assessment you performed.

Lab Assessment Questions

1. What is the goal or objective of an IT risk assessment?

- To mitigate risks to prevent security incidents and to define how the risk will be managed, controlled, and monitored.

2. Why is it difficult to conduct a qualitative risk assessment for an IT infrastructure?

- Cause administering a qualitative risk assessment need the emotional belief of many specialists, and they occasionally have various knowledge and information, it is hard to judge the administering.

3. What was your rationale in assigning "1" risk impact/ risk factor value of "Critical" for an identified risk, threat, or vulnerability?

- The critical risk factor is a risk, threat, or vulnerability that impacts compliance and places the organization in a position of increased liability

4. When you assembled all of the "1" and "2" and "3" risk impact/risk factor values to the identified risks, threats, and vulnerabilities, how did you prioritize the "1", "2", and "3" risk elements? What would you say to executive management in regards to your final recommended prioritization?

- "1" Critical - a risk, threat, or vulnerability that impacts compliance and places the organization in a position of increased liability.
- "2" Major - a risk, threat, or vulnerability that impacts the C-I-A of an organization's intellectual.
- "3" Minor - a risk, threat, or vulnerability that can impact user or employee productivity or availability of the IT infrastructure.

5. Identify a risk mitigation solution for each of the following risk factors:

User downloads and clicks on an unknown e-mail attachment
- Training for employees on internet browsing and dangers.

Workstation OS has a known software vulnerability
- Apply the latest OS patches and updates to eliminate software vulnerabilities.

Need to prevent eavesdropping on WLAN due to customer privacy data access
- NIC, Ethernet LAN, LAN switch, file and print server and system administration

Weak ingress/egress traffic filtering degrades performance
- Strengthen firewall filtering

DoS/DDoS attack from the WAN/Internet
- Network engineer would be needed to set up defined security controls according to the already defined policy.

Remote access from home office
- Apply first level and second level security for remote access to sensitive systems, applications and data.

Production server corrupts database
- Implement daily data backups and off-site data storage for monthly data archiving. Define data recovery procedures based on defined RTOs