Lab #4: Assessment Worksheet

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

Course Name: IAA202

Student Name: Huynh Ngoc Quang

Instructor Name: Mr. Mai Hoang Dinh

Lab Due Date: September 25, 2024

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
    b. Regional bank under GLBA compliance law
    c. Nationwide retailer under PCI DSS standard requirements
    d. Higher-education institution under FERPA 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	LAN-to-WAN	Critical (1)
User destroys data in application and deletes all files	System/Application	Critical (1)
Hacker penetrates your IT infrastructure and gains access to your internal network	LAN	Critical (1)
Intra-office employee romance gone bad	User	Minor (3)
Fire destroys primary data center	System/Application	Critical (1)
Service provider SLA is not achieved	WAN	Major (2)
Workstation OS has a known software vulnerability	Workstation	Major (2)

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

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. Define the following qualitative risk impact/risk factor metrics:

- ❖ **"1" Critical** – a risk, threat, or vulnerability that impacts compliance (i.e., privacy law requirement for securing privacy data and implementing proper security controls, etc.) 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 property assets and IT infrastructure.
- ❖ **"3"Minor** – a risk, threat, or vulnerability that can impact user or employee productivity or availability of the IT infrastructure.

- **User Domain Risk Impacts**: 1, 2, 3
- **Workstation Domain Risk Impacts**: 2, 3
- **LAN Domain Risk Impacts**: 1, 2, 3
- **LAN-to-WAN Domain Risk Impacts**: 1, 2
- **WAN Domain Risk Impacts**: 1, 2
- **Remote Access Domain Risk Impacts**: 2
- **Systems/Applications Domain Risk Impacts**: 1

4. Craft an executive summary for management using the following 4-paragraph format. The executive summary must address the following topics:
    - Paragraph #1: Summary of findings: risks, threats, and vulnerabilities found throughout the seven domains of a typical IT infrastructure
    - Paragraph #2: Approach and prioritization of critical, major, minor risk assessment elements
    - Paragraph #3: Risk assessment and risk impact summary to the seven domains of a typical IT infrastructure
    - Paragraph #4: Recommendations and next steps for executive management

Summary of Findings: The qualitative risk assessment identified multiple risks, threats, and vulnerabilities across the seven domains of the IT infrastructure. The most critical risks include unauthorized access, denial of service (DoS/DDoS) attacks, and vulnerabilities in the operating systems of critical servers. These risks pose a significant threat to patient data and compliance with HIPAA.

Approach and Prioritization: The identified risks were categorized as Critical (1), Major (2), and Minor (3). Priority was given to critical risks that could lead to non-compliance with HIPAA regulations or major data breaches. Major risks include potential vulnerabilities in operating systems and secure access mechanisms.

Risk Assessment and Impact Summary: Critical risks, such as fire damage to the data center and external hacker attacks, were identified as having the highest potential for system downtime and data loss. Major risks included known software

vulnerabilities in workstations and servers, which could compromise the confidentiality and availability of patient information.

Recommendations and Next Steps: Immediate actions should be taken to address critical risks, such as improving firewall protections, applying software patches, and ensuring secure VPN access. Long-term strategies should include regular system audits, enhanced network monitoring, and continuous staff training to mitigate human error risks.

Lab #4: Assessment Worksheet

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.

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

The goal is to identify, assess, and prioritize risks, threats, and vulnerabilities that could impact the confidentiality, integrity, and availability of the IT infrastructure and to propose mitigation strategies.

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

Qualitative risk assessments can be challenging due to the subjective nature of risk impact evaluation, the complexity of interconnected systems, and the difficulty in estimating the likelihood and potential impact of each risk.

3. What is your rationale in assigning "1" as the risk impact for a critical risk?

Risks such as unauthorized access or data breaches are assigned a "1" because they could lead to severe consequences like data loss, legal repercussions under HIPAA, and a significant financial impact on the organization.

4. How did you prioritize risk elements "1", "2", and "3"?

The prioritization was based on the potential damage to the organization's operations and compliance. Risks that directly threatened patient privacy or regulatory compliance

were given top priority (1), followed by those affecting the IT infrastructure's stability (2), and then risks impacting user productivity (3).

5. Risk mitigation solutions for specific scenarios:

- User downloads and clicks on an unknown email attachment: Implement email filtering, regular training on phishing, and antivirus software.
- Workstation OS has a known software vulnerability: Apply patches and updates immediately.
- Need to prevent eavesdropping on WLAN: Encrypt all wireless communications and apply strong access controls.
- DoS/DDoS attack from the WAN/Internet: Use firewall rules and traffic filtering to mitigate large traffic spikes.
- Remote access from home office: Secure the VPN with multi-factor authentication and ensure encryption.