Lab #4: Assessment Worksheet

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

Course Name: IAA202

Student Name: Đặng Văn Long

Instructor Name: Hoàng Mạnh Đức

Lab Due Date: 15/06/2024

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	Remote Access domain	1
User destroys data in application and deletes all files	System/Application domain	3
Hacker penetrates your IT infrastructure and gains access to your internal network	LAN-to-WAN domain	1
Intra-office employee romance gone bad	User domain	3
Fire destroys primary data center	System/Application domain	1

Service provider SLA is not achieved	WAN domain	3
Workstation OS has a known software vulnerability	Workstation domain	2
Unauthorized access to organization owned Workstation		1
Loss of production data	System/Application domain	2
Denial of service attack on organization DMZ and e-mail server	LAN-to-WAN domain	1
Remote communications from home office	Remote Access domain	2
LAN server OS has a known software vulnerability	LAN domain	2
User downloads and clicks on an unknown	User domain	1
Workstation browser has software vulnerability	Workstation domain	3
Mobile employee needs secure browser access to sales order entry system	Remote Access domain	3
Service provider has a major network outage	WAN domain	2
Weak ingress/egress traffic filtering domain degrades performance	LAN-to-WAN	3
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	User domain	2
VPN tunneling between remote computer domain and ingress/egress router is needed	LAN-to-WAN	2
WLAN access points are needed for LAN domain connectivity within a warehouse	LAN	3
Need to prevent eavesdropping on WLAN domain due to customer privacy data access	LAN	1

DoS/DDoS attack from the WAN/Internet	WAN domain

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. User downloads and clicks on an unknown e-mail attachment.
2. User inserts CDs and USB hard drives with personal photos, musics, and videos on organization owned computers.
3. Intra-office employee romance gone bad.

Workstation Domain Risk Impacts:

1. Unauthorized access to organization owned workstations.
2. Workstation OS has a known software vulnerability.
3. Workstation browser has software vulnerability.

LAN Domain Risk Impacts:

1. Need to prevent eavesdropping on WLAN due to customer privacy data access.
2. LAN server OS has a known software vulnerability.
3. WLAN access points are needed for LAN connectivity within a warehouse.

LAN-to-WAN Domain Risk Impacts:

1. Denial of service attack on organization DMZ and e-mail server.
2. VPN tunneling between remote computer and ingress/egress router is needed.
3. Weak ingress/egress traffic filtering degrades performance.

WAN Domain Risk Impacts:

1. DoS/DDoS attack from the WAN/Internet.
2. Service provider has a major network outage.
3. Service provider SLA is not achieved.

Remote Access Domain Risk Impacts:

1. Unauthorized access from public Internet.
2. Remote communications from home office.
3. Mobile employ Systems/Applications

Systems/Applications Domain Risk Impacts:

1. Fire destroys primary data center.
2. Loss of production data.
3. User destroys data in application and deletes all files.

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

Executive Summary

Paragraph 1: Summary of Findings

Our risk assessment identified several risks, threats, and vulnerabilities across the IT infrastructure, specifically for a healthcare provider under HIPAA compliance. Key issues include unauthorized access from the public Internet, potential data destruction by users, hacker intrusions, internal conflicts, and physical threats such as fire destroying the primary data center. Other notable risks include service provider SLA failures, software vulnerabilities, and secure remote communications needs.

Paragraph 2: Approach and Prioritization

We prioritized risks based on their impact on compliance, the CIA of IT assets, and user productivity. Critical risks, like unauthorized access and data breaches, impact HIPAA compliance and liability. Major

risks affect IT asset security, such as software vulnerabilities and data loss. Minor risks impact productivity, like unauthorized use of external devices.

Paragraph 3: Risk Assessment and Impact Summary

Our assessment across the seven domains showed significant risks: user domain issues like unauthorized access, workstation vulnerabilities, LAN internal threats, LAN-to-WAN and WAN external threats like DDoS attacks, remote access security needs, and application domain software vulnerabilities. Each domain requires targeted mitigation strategies.

Paragraph 4: Recommendations and Next Steps

We recommend implementing strong encryption and access controls, regular software updates, enhanced physical security, robust network security measures, and strict external device policies. Training employees on security protocols is also crucial. Prioritizing these steps will help mitigate risks, ensure HIPAA compliance, and protect our IT infrastructure.

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.

Lab Assessment Questions

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

The primary goal of an IT risk assessment is to identify, evaluate, and prioritize potential risks, threats, and vulnerabilities within an IT infrastructure. This process aims to understand the impact of these risks on the organization's assets, including compliance with relevant laws and regulations, and to develop strategies to mitigate or manage these risks effectively. In the context of a healthcare provider under HIPAA compliance, the objective is to protect patient data, ensure the confidentiality, integrity, and availability (CIA) of IT systems, and maintain compliance with regulatory requirements.

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

Conducting a qualitative risk assessment for an IT infrastructure is challenging due to several factors:

- Complexity and Diversity: IT infrastructures are complex and consist of numerous interconnected components, each with its own set of potential vulnerabilities.

- Subjectivity: Qualitative assessments rely on subjective judgments to determine the likelihood and impact of risks, which can vary among different assessors.

- Evolving Threat Landscape: The IT threat landscape is constantly changing, with new vulnerabilities and threats emerging regularly.

- Data Sensitivity: In environments like healthcare, data sensitivity and privacy regulations add additional layers of complexity to the risk assessment process.

- Resource Constraints: Limited resources, including time, budget, and expertise, can hinder the thoroughness of the risk assessment.

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

A "Critical" risk impact value of "1" was assigned to risks, threats, or vulnerabilities that directly impact HIPAA compliance and the protection of sensitive patient data. These critical risks are those that, if exploited, could result in significant legal, financial, and reputational damage to the organization. For example, unauthorized access to patient medical records from the public Internet was considered critical due to its severe implications for data privacy and potential violation of HIPAA regulations.

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?

Risks were prioritized based on their impact on compliance, the CIA of IT assets, and user productivity. "1" risks were considered critical due to their direct impact on regulatory compliance and liability. "2" risks were major, affecting the overall security and functionality of IT systems. "3" risks were minor, primarily affecting user productivity. To executive management, I would recommend prioritizing mitigation efforts towards "1" risks to ensure compliance and protect sensitive data. Addressing "2" and "3" risks subsequently will further enhance the overall security and efficiency 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:

  - Mitigation Solution: Implement and enforce email filtering and anti-phishing solutions. Provide regular security awareness training for employees to recognize and avoid phishing attempts.

- Workstation OS has a known software vulnerability:

  - Mitigation Solution: Ensure that all workstations are regularly updated with the latest security patches and software updates. Implement a robust patch management system.

- Need to prevent eavesdropping on WLAN due to customer privacy data access:

  - Mitigation Solution: Use strong encryption protocols such as WPA3 for WLAN security. Implement secure access controls and regularly monitor network traffic for suspicious activity.

- Weak ingress/egress traffic filtering degrades performance:

  - Mitigation Solution: Configure and regularly update firewall rules to improve traffic filtering. Use advanced threat detection and prevention systems to monitor and manage network traffic effectively.

- DoS/DDoS attack from the WAN/Internet:

  - Mitigation Solution: Implement DDoS protection solutions such as traffic analysis and rate limiting. Use cloud-based DDoS mitigation services to absorb and deflect attack traffic.

- Remote access from home office:

  - Mitigation Solution: Deploy a secure VPN solution for remote access. Enforce multi-factor authentication (MFA) and ensure that remote endpoints comply with security policies.

- Production server corrupts database:

  - Mitigation Solution: Implement regular backup procedures and data integrity checks. Use database replication and redundancy to ensure data availability and quick recovery in case of corruption.