**Lab #4: Assessment Worksheet**

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

**Course Name: IAA202**____________________________________________________________

**Student Name: Trần Minh Triết**____________________________________________________________

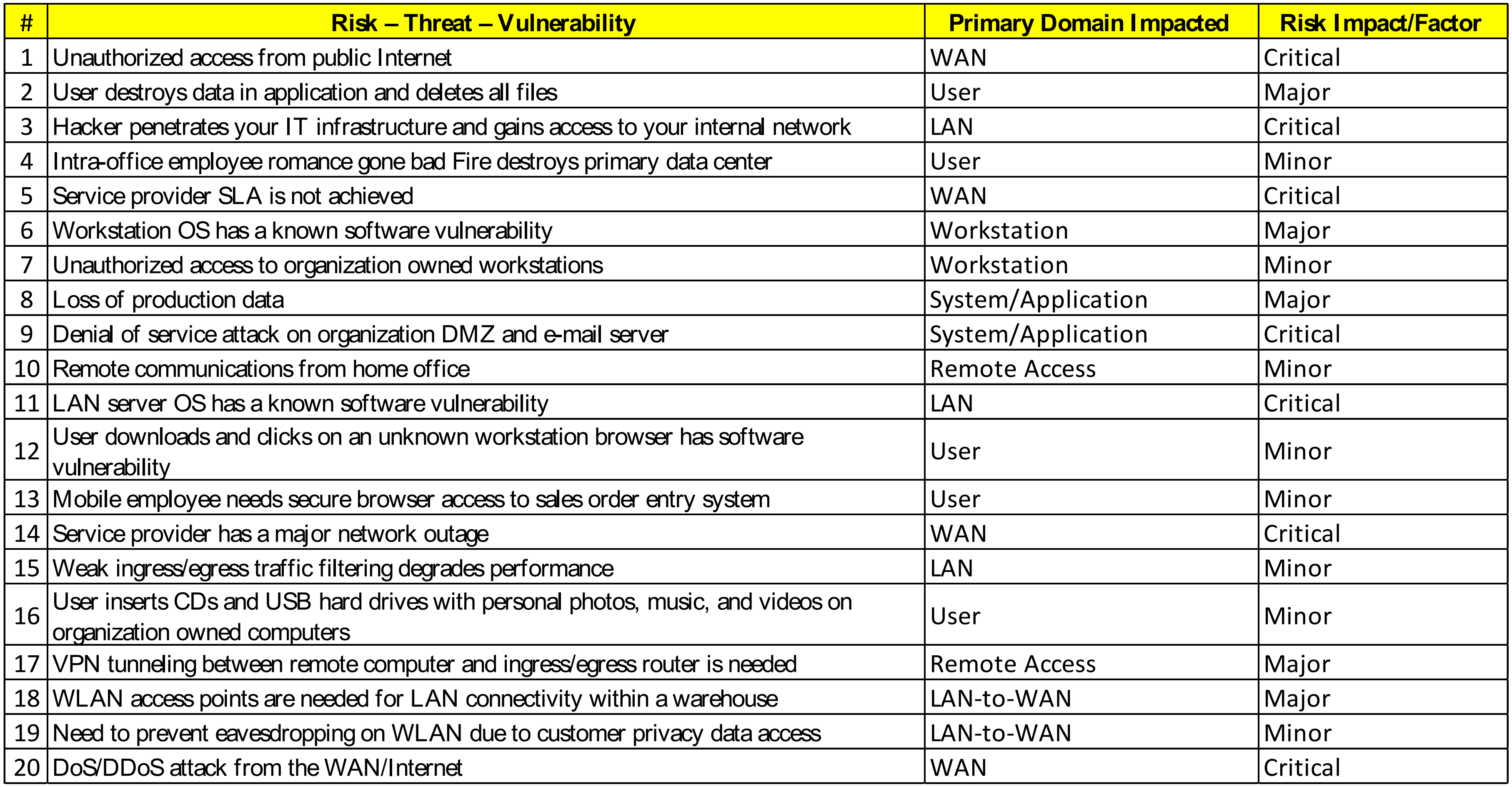
**Lab Due Date: 01/06/2023**____________________________________________________________

## Overview

The following risks, threats, and vulnerabilities were found in an IT infrastructure.

Scenario / industry vertical given: **Healthcare provider under HIPPA compliance law**

1. 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 |
|---|---|---|---|
| 1 | Unauthorized access from public Internet | WAN | Critical |
| 2 | User destroys data in application and deletes all files | User | Major |
| 3 | Hacker penetrates your IT infrastructure and gains access to your internal network | LAN | Critical |
| 4 | Intra-office employee romance gone bad Fire destroys primary data center | User | Minor |
| 5 | Service provider SLA is not achieved | WAN | Critical |
| 6 | Workstation OS has a known software vulnerability | Workstation | Major |
| 7 | Unauthorized access to organization owned workstations | Workstation | Minor |
| 8 | Loss of production data | System/Application | Major |
| 9 | Denial of service attack on organization DMZ and e-mail server | System/Application | Critical |
| 10 | Remote communications from home office | Remote Access | Minor |
| 11 | LAN server OS has a known software vulnerability | LAN | Critical |
| 12 | User downloads and clicks on an unknown workstation browser has software vulnerability | User | Minor |
| 13 | Mobile employee needs secure browser access to sales order entry system | User | Minor |
| 14 | Service provider has a major network outage | WAN | Critical |
| 15 | Weak ingress/egress traffic filtering degrades performance | LAN | Minor |
| 16 | User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers | User | Minor |
| 17 | VPN tunneling between remote computer and ingress/egress router is needed | Remote Access | Major |
| 18 | WLAN access points are needed for LAN connectivity within a warehouse | LAN-to-WAN | Major |
| 19 | Need to prevent eavesdropping on WLAN due to customer privacy data access | LAN-to-WAN | Minor |
| 20 | DoS/DDoS attack from the WAN/Internet | WAN | Critical |

2. 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.

**1. User Domain Risk Impacts:**

- **Impact Level: Major**
- **Explanation: User domain risks typically involve human actions, such as accidental or intentional data breaches, weak passwords, or social engineering attacks. While these risks can have significant impacts on security and privacy, they are typically mitigated through user awareness training and security policies. However, if a user's account with elevated privileges is compromised or if sensitive information is leaked, it could result in a major impact, such as unauthorized access to critical systems or loss of sensitive data.**

**2. Workstation Domain Risk Impacts:**

- **Impact Level: Minor**
- **Explanation: Workstation domain risks pertain to the security and functionality of individual workstations. These risks can include malware infections, hardware failures, or unauthorized access to workstations. While these risks can disrupt individual users' productivity and compromise local data, they generally have a minor impact on the overall network or system infrastructure. Workstation security measures like antivirus software and regular backups can help mitigate these risks effectively.**

3. LAN Domain Risk Impacts:

- Impact Level: Major
- Explanation: Local Area Network (LAN) domain risks affect the network infrastructure within an organization. Examples include network equipment failures, unauthorized access to network resources, or compromised LAN security measures. LAN disruptions can have a major impact on an organization's ability to communicate, access shared resources, or maintain network services. These risks can result in significant downtime, loss of productivity, and potential exposure of sensitive information if not properly addressed.

4. LAN-to-WAN Domain Risk Impacts:

- Impact Level: Critical
- Explanation: LAN-to-WAN domain risks involve the connection between the local network and the wide area network (WAN), typically the internet. Risks in this domain can include external attacks targeting the organization's network, data breaches, or network outages affecting WAN connectivity. A critical impact level is assigned due to the potential for widespread disruption, compromise of sensitive data on a larger scale, and significant financial and reputational damage if not adequately addressed.

5. WAN Domain Risk Impacts:

- Impact Level: Major
- Explanation: Wide Area Network (WAN) domain risks encompass potential issues in the organization's wide-area network infrastructure, including the connections between multiple sites, cloud services, or third-party networks. Examples of risks include network outages, service provider failures, or vulnerabilities in WAN equipment. While these risks can have a major impact on an organization's ability to communicate and access resources, they are usually more localized than the critical risks associated with LAN-to-WAN connectivity.

6. Remote Access Domain Risk Impacts:

- Impact Level: Major
- Explanation: Remote Access domain risks involve the security of remote connections to an organization's network, such as virtual private network (VPN) access or remote desktop services. Risks can include unauthorized access to remote systems, exploitation of vulnerabilities in remote access technologies, or compromised user credentials. These risks have a major impact as they can lead to unauthorized access to critical systems, data breaches, or disruption of remote work capabilities, potentially affecting a large number of users and the organization's overall operations.

7. Systems/Applications Domain Risk Impacts:
   - Impact Level: Critical
   - Explanation: Systems and applications domain risks encompass vulnerabilities and threats associated with the organization's software systems, including operating systems, databases, and applications. Risks in this domain can range from software vulnerabilities, insufficient access controls, to data corruption or loss. Given the critical role of systems and applications in an organization's operations, a risk in this domain can have a severe impact, leading to service disruptions, loss or manipulation of data, or even compromise of the entire infrastructure if not adequately mitigated.

**Lab Assessment Questions**

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

**Answer:**

It's used to identify and evaluate risks based on an analysis of threats and vulnerabilities to assets. Risks are quantified based on their importance or impact severity. These risks are then prioritized.

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

**Answer:**

This is based on the probability and impact of a risk. It is not based on dollar values; it instead is done by gathering opinions of experts. They could all have a different opinion or priority which could cause an issue.

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

**User downloads and clicks on an unknown e-mail attachment – Disconnect the workstation from the network, then run a virus scan to check for issues and make fixes, then provide training to the employee on email polices.**

**Workstation OS has a known software vulnerability – Find the patch to fix the vulnerability and push it out to all workstations.**

**Need to prevent eavesdropping on WLAN due to customer privacy data access – First a password needs to be set on the Wi-Fi. Next the Wi-Fi can be hidden so that only someone that knows the exact name can pull it up. The distance that the Wi-Fi extends to should not exceed the exterior walls. Depending on how many devices are allowed access, MAC filtering can also be set up.**

**Weak ingress/egress traffic filtering degrades performance – New filtering methods need to be implemented.**

**DoS/DDoS attack from the WAN/Internet – Make sure there is a firewall in place, have it set up so that after 3 failed attempts to lock out that IP, or a third party software can be purchased to monitor DoS attacks.**

**Remote access from home office – I will use digital certificate technology to simplify the authentication process required to establish multiple IP tunnels. I can use IPsec VPN or SSL VPN. Delete staff remote access privileges once they are not needed.**

**Production server corrupts database – You can increase the performance of your external firewall. Although there are viruses that are undetected, which means if your server becomes corrupted, then you would have to rely on backups. That means backing up more frequently.**