# Lab #1: Assessment Worksheet

## Part A – List of Risks, Threats, and Vulnerabilities

## Commonly Found in 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:** 7/1/2023

| Risk – Threat – Vulnerability | Primary Domain Impacted |
|---|---|
| Unauthorized access from public Internet | LAN-to-WAN |
| User destroys data in application and deletes all files | System/Application |
| Hacker penetrates your IT infrastructure and gains access to your internal network | LAN-to-WAN |
| Intra-office employee romance gone bad | User |
| Fire destroys primary data center | System/Application |
| Communication circuit outages | WAN |
| Workstation OS has a known software vulnerability | Workstation |
| Unauthorized access to organization owned Workstations | Workstation |
| Loss of production data | System/Application |
| Denial of service attack on organization e-mail Server | LAN-to-WAN |
| Remote communications from home office | Remote Access |
| LAN server OS has a known software vulnerability | LAN |
| User downloads an unknown e –mail attachment | User |
| Workstation browser has software vulnerability | Workstation |
| Service provider has a major network | WAN |

| | |
|---|---|
| outage | |
| Weak ingress/egress traffic filtering degrades Performance | LAN-to-WAN |
| User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers | User |
| VPN tunneling between remote computer and ingress/egress router | LAN-to-WAN |
| WLAN access points are needed for LAN connectivity within a warehouse | LAN |
| Need to prevent rogue users from unauthorized WLAN access | LAN |

## **PART B -** Assessment Questions and Answers

### **Lab Assessment Questions**

Given the scenario of a healthcare organization, answer the following Lab #1 assessment questions from a risk management perspective:

1. Healthcare organizations are under strict compliance to HIPPA privacy requirements which require that an organization have proper security controls for handling personal healthcare information (PHI) privacy data. This includes security controls for the IT infrastructure handling PHI privacy data. Which one of the listed risks, threats, or vulnerabilities can violate HIPPA privacy requirements? List one and justify your answer in one or two sentences.

- Denial of service attack on organization e-mail Server. Hacker attack the Platform via a denial-of-service attack or a distributed denial-of-service attack; or Impersonate or attempt to impersonate the Company, a Company employee, another user or any other person or entity.

2. How many threats and vulnerabilities did you find that impacted risk within each of the seven domains of a typical IT infrastructure?
User Domain: 3
Workstation Domain: 3
LAN Domain: 3
LAN-to-WAN Domain: 5
WAN Domain: 2

Remote Access Domain: 1
Systems/Application Domain: 3

3. Which domain(s) had the greatest number of risks, threats, and vulnerabilities?
- LAN-to-WAN Domain

4. What is the risk impact or risk factor (critical, major, minor) that you would qualitatively assign to the risks, threats, and vulnerabilities you identified for the LAN-to-WAN Domain for the healthcare and HIPPA compliance scenario?
- Cyber attacks can compromise electronic protected health information (ePHI) in a variety of ways: Denial of service attack on organization's e-mail server, or VPN tunneling between a remote computer and ingress/egress router. Weak traffic filtering degrades performance, but can be mitigated by using a firewall to filter out malicious traffic.

5. Of the three Systems/Application Domain risks, threats, and vulnerabilities identified, which one requires a disaster recovery plan and business continuity plan to maintain continued operations during a catastrophic outage?
- Fire destroys primary data center

6. Which domain represents the greatest risk and uncertainty to an organization?
- User Domain

7. Which domain requires stringent access controls and encryption for connectivity to corporate resources from home?
- Remote Access Domain

8. Which domain requires annual security awareness training and employee background checks for sensitive positions to help mitigate risk from employee sabotage?
- User Domain

9. Which domains need software vulnerability assessments to mitigate risk from software vulnerabilities?
- System/Application Domain, Workstation Domain, LAN Domain, LAN-to-WAN Domain

10. Which domain requires AUPs to minimize unnecessary User initiated Internet traffic and can be monitored and controlled by web content filters?
- Workstation Domain, WAN Domain

11. In which domain do you implement web content filters?
- LAN-to-WAN

12. If you implement a wireless LAN (WLAN) to support connectivity for laptops in the Workstation Domain, which domain does WLAN fall within?
- Lan Domain

13. A bank under Gramm-Leach-Bliley-Act (GLBA) for protecting customer privacy has just implemented their online banking solution allowing customers to access their accounts and perform transactions via their computer or PDA device. Online banking servers and their public Internet hosting would fall within which domains of security responsibility?
- System/Application Domain, LAN-to-WAN Domain

14. Customers that conduct online banking using their laptop or personal computer must use HTTPS:, the secure and encrypted version of HTTP: browser communications. HTTPS:// encrypts webpage data inputs and data through the public Internet and decrypts that webpage and data once displayed on your browser. True or False.
- True

15. Explain how a layered security strategy throughout the 7-domains of a typical IT infrastructure can help mitigate risk exposure for loss of privacy data or confidential data from the Systems/Application Domain
- By examining where privacy data and confidential data reside and are accessed, organizations can design a layered security solution. By implementing proper security controls within the User Domain and Workstation Domain, users and their point-of-entry are granted access to systems and data. Risks, threats, and vulnerabilities can be mitigated within the System/Application Domain.