## Lab #1: Assessment Worksheet

### Part A – List of Risks, Threats, and Vulnerabilities Commonly Found in an IT Infrastructure

**Course Name: IA1502 - IAA202**

**Student Name:**  Phan Tuấn Minh

**Lab Due Date: 07/09/2021**

**Overview**

The following risks, threats, and vulnerabilities were found in a healthcare IT infrastructure servicing patients with life-threatening situations. Given the list, select which of the seven domains of a typical IT infrastructure is primarily impacted by the risk, threat, or vulnerability.

|  |  |
| --- | --- |
| **Risk – Threat – Vulnerability** | **Primary Domain Impacted** |
| Unauthorized access from public Internet | Remote Access Domain |
| User destroys data in application and deletes all files | System/Application Domain |
| Hacker penetrates your IT infrastructure and gains access to your internal network | LAN-to-WAN Domain |
| Intra-office employee romance gone bad | User Domain |
| Fire destroys primary data center | System/Application Domain |
| Communication circuit outages | WAN Domain |
| Workstation OS has a known software vulnerability | Workstation Domain |
| Unauthorized access to organization owned | Workstation Domain |
| Workstations | Workstation Domain |
| Loss of production data | System/Application Domain |
| Denial of service attack on organization e-mail Server | LAN-to-WAN Domain |
| Remote communications from home office | Remote Access Domain |
| LAN server OS has a known software vulnerability User downloads an unknown e –mail attachment | LAN Domain  User Domain |
| Workstation browser has software vulnerability | Workstation Domain |
| Service provider has a major network outage | WAN Domain |
| Weak ingress/egress traffic filtering degrades Performance | LAN-to-WAN Domain |
| User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers | User Domain |
| VPN tunneling between remote computer and ingress/egress router | LAN-to-WAN Domain |
| WLAN access points are needed for LAN connectivity within a warehouse | LAN Domain |
| Need to prevent rogue users from unauthorized WLAN access | LAN Domain |

**Part B – List of Risks, Threats, and Vulnerabilities**

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

1. Which domain(s) had the greatest number of risks, threats, and vulnerabilities?

LAN-to-WAN Domain.

1. 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?

- Hacker penetrates IT infrastructure and gains access to your internal network: **Critical**, PHI can be compromised

- Denial of service attack on organization's e-mail server: **Minor**, can be mitigated

- Weak ingress/egress traffic filtering degrades performance: **Minor**, can be mitigated

- VPN tunneling between the remote computer and ingress/egress router: **Major**, if electronic protected health information (ePHI) is being accessed remotely

1. 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:4

WAN Domain:2

1. In which domain do you implement web content filters?

LAN-to-WAN Domain

1. Which domains need software vulnerability assessments to mitigate risk from software vulnerabilities?

Workstation Domain (workstation, corporate-issued mobile devices)

LAN Domain(regarding the network devices)

System/Application Domain (servers, storage area network (SAN), network attached storage (NAS), backup devices)

**Risk – Threat – Vulnerability**

**Primary Domain Impacted**

Remote communications from home office

LAN server OS has a known software vulnerability

User downloads an unknown e –mail attachment

Workstation browser has software vulnerability

Service provider has a major network outage

Weak ingress/egress traffic filtering degrades Performance

User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers

VPN tunneling between remote computer and ingress/egress router

WLAN access points are needed for LAN connectivity within a warehouse

Need to prevent rogue users from unauthorized WLAN access

Remote Access Domain

LAN Domain

User Domain

Workstation Domain

WAN Domain

LAN-to-WAN Domain

User Domain

LAN-to-WAN Domain

LAN Domain

LAN Domain