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

**Identify Threats and Vulnerabilities in an IT Infrastructure**

**Course Name: IAA202\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Student Name: Vu Hoang\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Instructor Name: Ho Hai\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Lab Due Date:** **Sunday, 24 May** **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Overview**

One of the most important first steps to risk management and implementing a risk mitigation strategy is to

identify known risks, threats, and vulnerabilities and organize them. The purpose of the seven domains of

a typical IT infrastructure is to help organize the roles, responsibilities, and accountabilities for risk

management and risk mitigation. This lab requires students to identify risks, threats, and vulnerabilities

and map them to the domain that these impact 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.

Answer is : System/Application Domain- because a hacker can gain access and read the entire database of customer information with a SQL Injection Attack

1. How many threats and vulnerabilities did you find that impacted risk within each of the seven domains of a typical IT infrastructure?

Answer:

a.User Domain 1

b.Workstation Domain 5

c.LAN Domain 3

d.LAN-to-WAN Domain 3

e.WAN Domain 2

f.Remote Access Domain 2

g.Systems/Application Domain 4

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

Answer: Workstation 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?

Answer: I would consider the both of them minor for the most part, unless performance becomes production stoppage, both would be considered minor in relation to HIPPA.

1. 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?

Answer: Loss of production data.

1. Which domain represents the greatest risk and uncertainty to an organization?

Answer: User Domain

1. Which domain requires stringent access controls and encryption for connectivity to corporate resources from home ?

Answer: Remote Access Domain

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

Answer: User Domain

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

Answer: Workstation, LAN, & Systems/Application

1. Which domain requires AUPs to minimize unnecessary User initiated Internet traffic and can be monitored and controlled by web content filters?

Answer: User Domain

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

Answer: LAN-to-WAN Domain

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

Answer: LAN Domain

1. 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

Answer: LAN-to-WAN Domain

1. 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

Answer: True

1. 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.

Answer: As you travel through the layers, each layer should add a more secure features to help protect the IT assets. When you come to the Systems/Application Domain, the applications should work with the network based on how the other layers were set up.