Lab #1: Assessment Worksheet
Part A – List of Risks, Threats, and Vulnerabilities
Commonly Found in an IT Infrastructure

Course Name: IAA202
Student Name: Dang Hoang Nguyen
Instructor Name: Mrs. Pham Yen Thao
Lab Due Date: May 13, 2023

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 **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**	LAN Domain
User downloads an unknown e –mail attachment	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

Current Version Date: 07/30/2011 *www.jblearning.com*

Lab #1: Assessment Worksheet

Identify Threats and Vulnerabilities in an IT Infrastructure

Course Name: IAA202
Student Name: Dang Hoang Nguyen
Instructor Name: Mrs. Pham Yen Thao
Lab Due Date: May 13, 2023

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.

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.

    I think that is "Unauthorized access to organization owned Workstations". Because when a workstation that contain all the PHI of the patient and accessed by an Unauthorized user. This could lead to the leak of security data breach and put the privacy of the patient at risk (HIPPA violation)

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: 03

   Workstation Domain: 03

   LAN Domain: 03

   LAN-to-WAN Domain: 04

   WAN Domain: 02
   Remote Access Domain: 02

   Systems/Application Domain: 03

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?

Risk – Threat – Vulnerability	Risk impact or risk factor
Hacker penetrates your IT infrastructure and gains access to your internal network.	Critical. Because hacker can get access to data security breach
Denial of service attack on organization e-mail Server	Three of them, depend on the situation. Hacker can make disruption of business operation, data breach or financial loss
Weak ingress/egress traffic filtering degrades Performance.	Minor to major. Minor: reduce the performance

	Major: security risk, compliance violation
VPN tunneling between remote computer and ingress/egress router.	Major: Error when configurating → get network's vulnerable to attack by malware, etc. Insider threat, communication interception

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 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 and LAN to WAN domains

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

    User Domain

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

   LAN to WAN Domain

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?

   It would fall within WAN as well as Remote Access Domains of security responsibility.

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. HTTPS encrypts webpage data inputs and data through the public Internet and decrypts that webpage and data once displayed on your browser.

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 integrating several security controls at various layers of the infrastructure, a layered security approach throughout the seven domains of a typical IT infrastructure

can assist reduce the risk exposure for loss of privacy data or secret data from the Systems/Application Domain. To offer defense-in-depth and lessen the risk and consequence of a security breach, various domains can install access controls, encryption, firewalls, intrusion detection/prevention systems, monitoring, and logging.