Lab # 1 — Assessment Worksheet

**Course Name and Number: IAA202**

**Student Name: Tran Thanh Tuan**

**Student Id: SE161095**

**Instructor Name: Mai Hoang Dinh**

# **How to Identify Threats & Vulnerabilities in an IT Infrastructure**

***Risks, Threats, and Vulnerabilities Commonly Found Throughout the Seven Domains of a Typical IT Infrastructure***

1. **User Domain**

* Unauthorized Access

**→** Users must be made aware of phishing emails, pretexting or cons, keyboard loggers, and perpetrators impersonating an IT or delivery person in an attempt to obtain logon ID and password credentials.

* Lack of User Awareness

**→** Conduct security awareness training, display security awareness posters, insert reminders in banner greetings, and send email reminders to employees.

* User insertion of CD's and USB Drives with Personal Photos, Music, and Videos

→ Disable internal CD drives and USB ports. Enable automatic antivirus scans for inserted media drives, files, and email attachments. An antivirus scanning system examines all new files on your computer's hard drive for viruses. Set up antivirus scanning for emails with attachments.

* User Destruction of Organizations Systems, Applications, or Data

→ Restrict users' access to only those systems, applications, and data needed to perform their jobs. Minimize write/delete permissions to the data owner only.

* Attacks on the Organization or Acts of Sabotage by Disgruntled Employees

→ Track and monitor abnormal employee behavior, erratic job performance, and use of IT infrastructure during off-hours. Begin IT access control lockout procedures based on AUP monitoring and compliance.

* User Downloads of Photos, Music and Videos

→ Enable content filtering and antivirus scanning for email attachments. Content-filtering network devices are configured to permit or deny specific domain names in accordance with AUP definitions.

1. **Workstation Domain**

* Unauthorized access to workstation

→ Enable password protection on workstation for access.

* Unauthorized access to systems, applications & data

→Define strict access control policies, standards, procedures, & guidelines. Implement a second-level test to verify a user's right to gain access.

* Desktop or laptop computer operating system software vulnerabilities

→ Define a workstation application software vulnerability window policy. Update application software and security patches according to defined policies, standards, procedures & guidelines.

* Infection of a user's workstation or laptop computer by viruses, malicious code, or malware

→ Use workstation antivirus and malicious code policies, standards, procedures & guidelines. Enable an automated antivirus protection solution that scans & updates individual workstations with proper protection.

* User insertion of CDs, DVDs, or USB thumb drives into the organization's computers

→ Deactivate all CD, DVD, & USB ports. Enable automatic antivirus scans for inserted CDs, DVDs, & USB thumb drives that have files.

* Desktop or laptop application software vulnerabilities or patches

→ To prevent known vulnerabilities from being exploited, all of this software must be kept up to date. This means installing patches released by the software developers to close security holes found in their products.

1. **LAN Domain**

* Unauthorized physical access to LAN
* Unauthorized access to systems, applications, and data
* LAN server operating system vulnerabilities
* LAN server application software vulnerabilities and software patchupdates
* LAN servers with different hardware, operating systems, and software make them difficult to manage and troubleshoot

1. **LAN-to-WAN Domain**

* Unauthorized probing and port scanning
* Unauthorized access through the LAN-to-WAN Domain
* IP router, firewall, and network appliance operating system software vulnerability
* Local users downloading unknown file types from unknown sources
* Download of unknown file type attachments from unknown sources

1. **WAN Domain**

* Vulnerable to corruption of information and data
* Open, public, and accessible data
* Vulnerable to eavesdropping
* Vulnerable to DoS, DDoS, TCP SYN flooding, and IP spoofing attacks
* Hackers and attackers e-mailing Trojans, worms, and malicious software freely and constantly

1. **Remote Access Domain**

* Brute-force user ID and password attacks
* Multiple logon retries and access control attacks
* Private data or confidential data compromised remotely
* Data leakage in violation of data classification standards
* Unauthorized remote access to IT systems, applications, and data

1. **System/Application Domain**

* Unauthorized access to data centers, computer rooms and wiring closets
* Downtime of servers to perform maintenance
* Data breach where private data of individuals are compromised Corruption or loss of data
* Difficult-to-manage servers that require high availability

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

***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.

|  |  |  |
| --- | --- | --- |
| **Id** | **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 | 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 | Remote Access Domain |
|  | WLAN access points are needed for LAN connectivity within a warehouse | LAN-to-WAN Domain |
|  | Need to prevent rogue users from unauthorized WLAN access | LAN-to-WAN Domain |

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

***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.**

Unauthorized access to organization-owned workstations. Access to a workstation "already connected" may grant a perpetrator immediate access to sensitive information, including HIPAA PHI privacy data. The risk factor to consider here is what would happen if this PHI privacy data were compromised and exposed.

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

Remote Access Domain: 2

Systems/Application Domain: 3

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. **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?**

The risk of "Fire destroys primary data center".

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

The User Domain represents the greatest risk and uncertainty because human behavior is unreliable and influenced by factors uncontrolled by policy.

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

The Remote Access Domain requires stringent access controls and encryption because of risks inherent in connectivity from home.

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

User 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).

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

User Domain.

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

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?**

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?**

System/Application Domain & 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.**

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.**

By examining where privacy data and confidential data reside and are accessed, organizations can design a layered security solution, providing multiple security countermeasures and security controls at key points throughout the entire IT infrastructure. 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 according to their access control requirements. Within the IT infrastructure, additional security countermeasures and security controls in the LAN Domain and LAN-to-WAN Domain can provide access controls to servers, drives, folders, and data to authorized users. Finally, by ensuring servers, operating systems, and application software are patched with the latest software updates, risks, threats, and vulnerabilities can be mitigated within the System/Application Domain.