## Lab #4: Assessment Worksheet

**Perform a Qualitative Risk Assessment for an IT Infrastructure**

**Course Name: IAA202**

**Student Name: Phan Tuấn Minh**

**Lab Due Date:**

**Overview**

The following risks, threats, and vulnerabilities were found in an IT infrastructure. Your Instructor will assign you one of four different scenarios and vertical industries each of which is under a unique compliance law.

**1. Scenario/Vertical Industry: Healthcare provider under HIPAA compliance law**

**2. Given the list, perform a qualitative risk assessment by assigning a risk impact/risk factor to each of identified risks, threats, and vulnerabilities throughout the seven domains of a typical IT infrastructure that the risk, threat, or vulnerability resides**

|  |  |  |
| --- | --- | --- |
| **Risk-Threat-Vulnerability** | **Primary Domain Impacted** | **Risk Impact/Factor** |
| Unauthorized access from public Internet | REMOTE ACCESS | 1 |
| User destroys data in application and deletes all files | SYSTEM/APPLICATION | 2 |
| Hacker penetrates your IT infrastructure and gains access to your internal network | LAN-to-WAN | 1 |
| Intra-office employee romance gone bad | USER | 3 |
| Fire destroys primary data center | SYSTEM/APPLICATION | 3 |
| Service provider SLA is not achieved | WAN | 3 |
| Workstation OS has a known software vulnerability | WORKSTATION | 2 |
| Unauthorized access to organization owned workstations | WORKSTATION | 1 |
| Loss of production data | SYSTEM/APPLICATION | 2 |
| Denial of service attack on organization DMZ e-mail server | LAN-to-WAN | 1 |
| Remote communications from home office | REMOTE ACCESS | 2 |
| LAN server OS has a known software vulnerability | LAN | 2 |
| User downloads and clicks on an unknown | USER | 3 |
| Workstation browser has a software vulnerability | WORKSTATION | 2 |
| Mobile employee needs secure browser access to sales order entry system |  |  |
| Service provider has a major network outage | WAN | 3 |
| Weak ingress/egress traffic filtering degrades performance | WAN | 3 |
| User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers | USER | 3 |
| VPN tunneling between remote computer and ingress/egress router is needed | LAN-to-WAN | 2 |
| WLAN access points are needed for LAN connectivity within a warehouse | LAN-to-WAN | 2 |
| Need to prevent eavesdropping on WLAN due to customer privacy data access | LAN-to-WAN | 3 |
| DoS/DDoS attack from the WAN/Internet | WAN | 1 |

**3. For each of the identified risks, threats, and vulnerabilities, prioritize them by listing a “1”, “2”, and “3” next to each risk, threat, vulnerability found within each of the seven domains of a typical IT infrastructure. “1” = Critical, “2” = Major, “3” = Minor. Define the following qualitative risk impact/risk factor metrics:**

* 1. **“1” Critical** – a risk, threat, or vulnerability that impacts compliance (i.e., privacy law requirement for securing privacy data and implementing proper security controls, etc.) and places the organization in a position of increased liability.
  2. **“2” Major** – a risk, threat, or vulnerability that impacts the C-I-A of an organization’s intellectual property assets and IT infrastructure.
  3. **“3”Minor –** a risk, threat, or vulnerability that can impact user or employee productivity or availability of the IT infrastructure.

**User Domain Risk Impacts: 2 (refer to previous chart)**

1). Intra-office employee romance gone bad: When the relationship between the hospital staff goes bad, they can get in the way of each other's work

2). User downloads and clicks on an unknown: Facilitating viruses and spyware to steal information as well as monitor the work of hospital staff

3). User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers : Facilitating viruses and spyware to steal information as well as monitor the work of hospital staff

**Workstation Domain Risk Impacts: 1 (refer to previous chart)**

1).Workstation OS has a known software vulnerability : Hackers will know and start exploiting

2).Unauthorized access to organization owned workstations : Leads to escalating privileges and illegal access

3).Workstation browser has a software vulnerability : Hackers will know and start exploiting

**LAN Domain Risk Impacts: 2 (refer to previous chart)**

1).LAN server OS has a known software vulnerability : Hackers will know and start exploiting, and they can accesss to other domain or other staff’s computer

**LAN-to-WAN Domain Risk Impacts: 2 (refer to previous chart)**

1).Hacker penetrates your IT infrastructure and gains access to your internal network : Hackers access the records, data of medical staff, patients' medical records, thereby selling information out to medical companies. More serious is destroying IT assets

2). Denial of service attack on organization DMZ e-mail server : Hackers knows confidential information

3). VPN tunneling between remote computer and ingress/egress router is needed : Guaranteed Confidentiality

4). Need to prevent eavesdropping on WLAN due to customer privacy data access

**WAN Domain Risk Impacts: 1 (refer to previous chart)**

1). Service provider SLA is not achieved : Disruption of the network system, causing delays in solving work as well as saving patients

2). Service provider has a major network outage : Disruption of the network system, causing delays in solving work as well as saving patients, can sometimes cause data loss

3). Weak ingress/egress traffic filtering degrades performance : Disruption of the network system, causing delays in solving work as well as saving patients

4). DoS/DDoS attack from the WAN/Internet : Disruption of the network system, causing delays in solving work as well as saving patients

**Remote Access Domain Risk Impacts: 2 (refer to previous chart)**

1). Unauthorized access from public Internet : Untraceable and unmanageable

2). Remote communications from home office: Risk of revealing passwords and important information

**Systems/Applications Domain Risk Impacts: 3 (refer to previous chart)**

1).User destroys data in application and deletes all files : Unrecoverable unless archived, damaging the honor and reputation of the hospital

2). Fire destroys primary data center : Unrecoverable unless archived