**Lab #4: Assessment Worksheet**

**Part A – Perform a Qualitative Risk Assessment for an IT Infrastructure**

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

**Student Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Instructor Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**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:

a. Healthcare provider under HIPPA compliance law

b. Regional bank under GLBA compliance law

c. Nationwide retailer under PCI DSS standard requirements

d. Higher-education institution under FERPA 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

User destroys data in application and deletes

all files

Hacker penetrates your IT infrastructure

and gains access to your internal network

Intra-office employee romance gone bad

Fire destroys primary data center

Service provider SLA is not achieved

Workstation OS has a known software

Vulnerability

Unauthorized access to organization owned

Workstations

Loss of production data

Denial of service attack on organization

DMZ and e-mail server

Remote communications from home office

LAN server OS has a known software

Vulnerability

User downloads and clicks on an unknown

Workstation browser has software vulnerability

Mobile employee needs secure browser access

to sales order entry system

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 is needed

WLAN access points are needed for LAN

connectivity within a warehouse

Need to prevent eavesdropping on WLAN

due to customer privacy data access

DoS/DDoS attack from the WAN/Internet

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” 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” Major** – a risk, threat, or vulnerability that impacts the C-I-A of an organization’s intellectual property assets and IT infrastructure.

**“3”Minor –** a risk, threat, or vulnerability that can impact user or employee productivity or availability of the IT infrastructure.

**User Domain Risk Impacts:**

**Workstation Domain Risk Impacts:**

**LAN Domain Risk Impacts:**

**LAN-to-WAN Domain Risk Impacts:**

**WAN Domain Risk Impacts:**

**Remote Access Domain Risk Impacts:**

**Systems/Applications Domain Risk Impacts:**

**Lab #4: Assessment Worksheet**

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

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

**Student Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Instructor Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Lab Due Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Overview**

Answer the following Lab #4 – Assessment Worksheet questions pertaining to your qualitative IT risk

assessment you performed.

**Lab Assessment Questions:**

1. What is the goal or objective of an IT risk assessment?

The goal of the 3A is to identify and mitigate risks.

2. Why is it difficult to conduct a qualitative risk assessment for an IT infrastructure?

It is difficult to conduct a !ualitative risk assessment for an IT infrastructure because it is hard to tell what kind of impact a given attack will have on the infrastructure.

3. What was your rationale in assigning “1” risk impact/ risk factor value of “Critical” for an identified risk, threat, or vulnerability?

Assigned critical impact values for threats that severely compromise patient data or that made the system useless such as Do- attacks.

4. When you assembled all of the “1” and “2” and “3” risk impact/risk factor values to the identified risks, threats, and vulnerabilities, how did you prioritize the “1”, “2”, and “3” risk elements? What would you say to executive management in regards to your final recommended prioritization?

Management should acquire a SLA so that ours systems will always will always be funtioning optimally. I would also recommend that the appropriate countermeasures for threats are in place.

5. Identify a risk mitigation solution for each of the following risk factors:

User downloads and clicks on an unknown e-mail attachment –The organization should provide training to all employees in the proper handling of e-mail attachments and hyperlinks. Never open any attachments or click on links from unknown sources.

Workstation OS has a known software vulnerability – Apply the latest OS patches and updates to eliminate software vulnerabilities.

Need to prevent eavesdropping on WLAN due to customer privacy data access – Ensure all unused ports are disabled on the edge routers. Use packet tracer equipment to find and block any suspicious traffic found on WAN circuits.

Weak ingress/egress traffic filtering degrades performance – Update and apply all router OS patches. Build filters to block employees from music and movie torrent databases. These databases are notorious for having spyware, malware and viruses that all degrade network performance.

DoS/DDoS attack from the WAN/Internet – Ensure the internal systems administrators are aware of any suspicious traffic sources that have been reviewed and are known to launch DDos attacks. If a DDos is occurring it is vital that the proper engineering resources are notified immediately so that they can locate the offending IP addresses and block them at the organization firewalls.

Remote access from home office –Ensure that all employees are again notified and trained on proper use of the VPN connections. They should never share the VPN with any public access terminals such as internet café’s or any unknown wireless networks. They also need to aware that no usb drives are allowed connection to their home PCs or laptops. The home PCs have to have the necessary anti-virus/malware programs to ensure the home PCs do not infect the organizations systems via the VPN.

Production server corrupts database – The server needs to be brought down and anti-virus tools need to be implemented to remove the corrupted data. Any corrupted data will then be re-imaged from the back up data the company has been storing at an offsite facility. The data can also be restored from a stand-alone server that functions as a hot standby for occasions that the organization finds itself dealing with corrupted servers.