**Lab #4: Assessment Worksheet**

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

**Chapter 5 and Chapter 6 of the Text Book**

**Course Name: IAA202**

**Student Name: Vu Hoang**

**Instructor Name: Haih5**

**Lab Due Date: 06/11/2020**

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

1. 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:** *(refer to previous chart)*

1) User downloads and clicks on an unknown e-mail attachment.

2) User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers.

3) Intra-office employee romance gone bad.

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

1) Unauthorized access to organization owned workstations.

2) Workstation OS has a known software vulnerability.

3) Workstation browser has software vulnerability.

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

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

2) LAN server OS has a known software vulnerability.

3) WLAN access points are needed for LAN connectivity within a warehouse.

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

1) Denial of service attack on organization DMZ and e-mail server.

2) VPN tunneling between remote computer and ingress/egress router is needed.

3) Weak ingress/egress traffic filtering degrades performance.

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

1) DoS/DDoS attack from the WAN/Internet.

2) Service provider has a major network outage.

3) Service provider SLA is not achieved.

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

1) Unauthorized access from public Internet.

2) Remote communications from home office.

3) Mobile employee needs secure browser access to sales order entry system.

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

1) Fire destroys primary data center.

2) Loss of production data.

3) User destroys data in application and deletes all files.

**Lab #4: Assessment Worksheet**

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

**Chapter 5 and Chapter 6 of the Text Book**

**Course Name: IAA202**

**Student Name: Vu Hoang**

**Instructor Name: Haih5**

**Lab Due Date: 06/11/2020**

**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?
   1. To Identify and evaluate risks. Risks are then quantified based on their importance or impact severity. Then the risks are prioritized. They are a major part of an overall risk management program and they help identify which risks are most important.
2. ***True/False***: It is difficult to conduct a qualitative risk assessment for an IT infrastructure because obtaining accurate cost elements and potential liabilities is difficult to identify for an organization. Hence, many organizations opt to perform quantitative risk assessments based on assessing the risk impact/risk factor of identified threats and vulnerabilities to an organization.
   1. True
3. ***True/False***: The rationale behind assigning “1” risk impact/risk factor value of “Critical” for an identified risk, threat, or vulnerability is because anything that impacts an organization’s legal compliance and potential liabilities from customers for non-compliance is the greatest risk to an organization.
   1. True
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?
   1. First you identify the risks by surveys and interviewing experts and then assign probability and impact values to the risks. Then compile and summarize so put in number value. I would tell the executive management that Risk level 3 needs to be attended to as soon as possible in order for the others to be completed.
5. Identify a risk mitigation solution for each of the following risk factors:
   1. 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.

* 1. Workstation OS has a known software vulnerability –

Apply the latest OS patches and updates to eliminate software vulnerabilities.

* 1. 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.

* 1. 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.

* 1. 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.

* 1. Remote access from home office –remote policies,

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.

* 1. 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.