Lab # 6 — Assessment Worksheet

**Course Name and Number: IAA202**

**Student Name: Tran Thanh Tuan**

**Student Id: SE161095**

**Instructor Name: Mai Hoang Dinh**

## **Develop a Risk Mitigation Plan Outline for an IT Infrastructure**

***Overview***

After you have completed your qualitative risk assessment and identification of the critical “1” risks, threats, and vulnerabilities, mitigating them requires proper planning and communication to executive management. Students are required to craft a detailed IT risk management plan consisting of the following major topics and structure:

1. **Executive summary**

The detected threats, vulnerabilities, and hazards have been categorized as critical, significant, and minor. Each risk, hazard, and vulnerability belongs to a certain domain and is categorized into several categories. A risk, hazard, or vulnerability that affects compliance (e.g., privacy legislation requirements for safeguarding privacy data and installing adequate security measures, etc.) and puts the company in a position of heightened responsibility is classified as critical (1). A risk, threat, or vulnerability that affects the C-I-A of an organization's intellectual property assets and IT infrastructure is referred to as a major (2). Minor (3) refers to a risk, threat, or vulnerability that might affect user or staff productivity or the IT infrastructure's availability. Each risk, hazard, and vulnerability was assigned to a category, along with the domain to which it belonged. For each category, the remediation processes for reducing all significant, major, and minor risks, threats, and vulnerabilities are almost identical. The first step is to double-check that all of your equipment is operational. If any of the equipment fails, your network will be exposed to risks, threats, and vulnerabilities. The second stage is for users to be compelled to use complicated passwords and even a dual-factor authentication mechanism, which requires both a password and a token to get access to the system. Encrypting all sensitive data would be the third stage. The next step is to ensure that your anti-virus software is up to date, as well as that all of your software is patched. The next step is to add layers of protection by installing a host-based and network-based firewall. The third step would be for all workers to participate in some form of security awareness training to ensure that no passwords are shared. Ongoing IT risk mitigation for the seven domains displayed per domain and the company's current mitigation plan. HIPPA compliance regulations must be followed by the firm. The business is a medical school that handles medical records. The medical records of patients must be kept private. The cost magnitude determines how much effort firms are willing to put in. The medical firm prefers to stick to a reasonable budget. As a result, everything will be in the middle, not too expensive but not too cheap. The medical firm is looking for the finest for the greatest price. The implementation plan is a list of all the major hazards that need to be addressed. The strategy outlines the job, action plan, time range, and risk priority for each risk. This is a highly thorough strategy that outlines the steps that will be done.

1. **Prioritization of identified risks, threats, and vulnerabilities organized into the seven domains**

* Critical – 1

Unauthorized access from public internet, Hacker penetrates your IT Infrastructure and gains access to your internal network, Unauthorized access to organization owned workstations, Denial of service attack on organization DMZ and e-mail server, Need to prevent eavesdropping on WLAN due to customer privacy data access, DoS/DDoS attack from the WAN/ Internet.

* Major – 2

Workstation OS has a known software vulnerability, Loss of production data, Service provider has a major network outage, VPN tunneling between remote computer and ingress/egress router is needed, Remote communications from home office, LAN server OS has a known software vulnerability, User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers.

* Minor – 3

Intra-office employee romance gone bad, Workstation browser has software vulnerability, Mobile employee needs secure browser access to sales order entry system, Weak ingress/egress traffic filtering degrades performance, WLAN access points are needed for LAN connectivity within a warehouse, User destroys data in application and deletes all files, Service provider SLA is not achieved.

1. **Critical “1” risks, threats, and vulnerabilities identified throughout the IT infrastructure**

* Unauthorized access from public internet – Remote Access Domain
* Hacker penetrates your IT Infrastructure and gains access to your internal network – LAN to WAN Domain
* Unauthorized access to organization owned workstations – Workstation Domain
* Denial of service attack on organization DMZ and e-mail server – LAN to WAN Domain
* Need to prevent eavesdropping on WLAN due to customer privacy data access – LAN to WAN Domain
* DoS/DDoS attack from the WAN/ Internet – WAN Domain
* Fire destroys primary data center – Systems/Application

1. **Remediation steps for mitigating critical “1” risks, threats, and vulnerabilities**

* **Unauthorized access from public internet**

The first step in preventing this is to set up a difficult password on the network. The next step would be to install a network-based host-based firewall. If you wanted to add an extra layer of security, you might install a network-based firewall to make it more difficult for an attacker to get access to your network. The final step is to ensure that the server and router both have difficult passwords.

* **Hacker penetrates your IT Infrastructure and gains access to your internal network**

The first step in reducing this risk would be to determine how the hacker gained access to your IT infrastructure. This is a critical phase in the process, since it is at this time that the IT Infrastructure that was breached must be repaired so that it does not happen again. The next step is to double-check all of the equipment to ensure that it is up-to-date and that the vulnerability was not caused by a flaw in the equipment that allowed the attacker access to the infrastructure. The next step would be to review all of the event logs to ensure that the breach did not originate from within the company. The final step would be to reset all passwords and make them more complicated in order to make it much harder for the hacker to get access to the system.

* **Unauthorized access to organization owned workstations**

The first step in reducing this danger will be to figure out how they got into the workstation in the first place. After that, passwords will need to be updated, and lastly, all workers will be required to undergo security awareness training.

* **Fire destroys primary data center**

Backing up all files and data is one approach to reduce the danger of this situation. Off-site storage of files and data is recommended. The data and files will not be harmed by the fire as a result of this.

* **Denial of service attack on organization DMZ and e-mail server**

To begin, check to see if your anti-virus software is up to date. If the anti-virus software is out of current, the DMZ and email server will be vulnerable to attack. The next step is to double-check that the firewall is still up and running. The DMZ sits between the firewall and the server, so if an attack gets past the DMZ and into the server, there's a chance the firewall isn't working properly.

* **Need to prevent eavesdropping on WLAN due to customer privacy data access**

The first step in mitigating this risk would be to encrypt all data in transit and at rest. Another step would be to verify that the firewalls are operational and that the network is complicated.

* **DoS/DDoS attack from the WAN/ Internet**

The first step in reducing this danger is to ensure that your anti-virus software is up to date. If your antivirus software is up to date, it should be able to detect a DoS/DDoS attack and alert you. The next step is to double-check that the firewall is still active. To assist avoid any further harm to the network and systems caused by this assault, the WAN/Internet should be unplugged. The next stage is to assess the system and network to determine how the attack took place and how it may be avoided in the future.

1. **Remediation steps for mitigating major “2” and minor “3” risks, threats, and vulnerabilities**

The following measures would be taken to minimize significant and small risks, threats, and vulnerabilities:

1. Check the equipment to make sure the risk, danger, or vulnerability was not caused by malfunctioning or failing equipment, such as servers.
2. Passwords should be needed for all users. Passwords should be long and difficult to guess. Passwords should never be shared with anyone else. For sensitive data, it may be advisable to use a two-factor authentication technique.
3. Encrypt any sensitive information. Data in transit and at rest should both be encrypted. This will prevent the information from falling into the wrong hands.
4. Ensure that all anti-virus software is up to date. Guarantee that all fixes are installed on the system to ensure that no known vulnerabilities exist.
5. To assure layers of security, install a host-based and network-based firewall, as well as a hardware firewall.
6. Ensure that all staff have received security awareness training.
7. **On-going IT risk mitigation steps for the seven domains of a typical IT infrastructure**

A policy prohibiting employees from establishing romantic relationships within the firm is one of the current risk mitigations utilized for the user domain. When a pair ends a relationship, they often don't want to see one other again, so seeing this person every day at work might turn sour at any point. One of the persons in the relationship, for example, may try to get the other in trouble by sending an email to the CEO from their personal email account. While dating, the pair exchanged passwords. This is why the firm insisted on enforcing the regulation. The operating system is up to date with the latest system on the market, which is the current on-going risk mitigation in use in the workstation domain. When a new patch is released by the manufacturer, the IT team will apply it to ensure that the system is free of known vulnerabilities. As of now, there are no ongoing risk mitigations for the LAN domain. Risk mitigation strategies for the LAN domain, WAN domain, and LAN to WAN domain are required by the firm. All data is backed up regularly as part of the existing risk mitigations for the system/application domain. Every week, a full backup is performed to guarantee that the data is not lost. On a daily basis, a partition backup is performed. All backups are kept off-site in case a natural disaster strikes and destroys the structure.

Only a single-factor authentication procedure is currently utilized for risk mitigation in the remote access domain. The user can access the system remotely, but they simply need a password to do so.

1. **Cost magnitude estimates for work effort and security solutions for the critical risks**
2. **Implementation plans for remediation of the critical risks**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task** | **Plan of Action** | **Day started** | **Date to be completed** | **Priority** |
| Unauthorized  Acces from public Internet | -Passwords that  are difficult to  guess  - Network-Based  Firewall  - Based on the  host  - Firewal  Passwords that  are difficult to  guess  - Network-Based  Firewall  - Based on the  host  - Firewal  Passwords that are difficult to guess  - Network-Based Firewall  - Based on the host  - Firewal | 1-4-15 | 5-4-15 | HIGH |
| Hacker penetrates your IT infrastructure and gains access to your internal network | -Network-Based Firewall -Complex Passwords  - Based on the host Firewall  - Double-check all of your equipment.  - Replace everything passwords  - Examine the event logs | 1-4-15 | 15-4-15 | HIGH |
| Unauthorized  access to  organizations  owned  worksation | -Change all passwords | 1-4-15 | 3-4-15 | HIGH |
| Fire in the datacenter | Offsite backup of all files and data | 1-4-15 | Continuously | HIGH |
| User inserts CDs and USB hard drives with personal photos, music,and videos on organization owned computers | - Disable the optical and USB drives. | 1-4-15 | 15-4-15 | HIGH |
| Need to prevent eavesdropping on WLAN due to customer privacy data access | -Set up firewalls  -Encrypt all information | 1-4-15 | 15-4-15 | HIGH |
| Denial of service attack on organization DMZ and email server | - Examine all anti-virus software  - Examine firewalls  - Double-check all of your equipment | 1-4-15 | 1-4-15 | HIGH |
| DoS/DDoS attack from the WAN/ Internet | -Examine all anti-virus software  - Examine firewalls  - Double-check all of your equipment | 1-4-15 | 1-4-15 | HIGH |

## **Develop a Risk Mitigation Plan Outline for an IT Infrastructure**

***Overview***

After completing your IT risk mitigation plan outline, answer the following Lab #6 – Assessment Worksheet questions. These questions are specific to the IT risk mitigation plan outline you crafted as part of Lab #6 – Develop a Risk Mitigation Plan Outline for an IT Infrastructure.

***Lab Assessment Questions & Answers***

1. **Why is it important to prioritize your IT infrastructure risks, threats, and vulnerabilities?**

It is important to prioritize because you must be aware of what the risks, threats, and vulnerabilities there are to your infrastructure. You need this so that you know where the most attention needs to be focused on.

1. **Based on your executive summary produced in Lab #4 – Perform a Qualitative Risk Assessment for an IT Infrastructure, what was the primary focus of your message to executive management?**

Setting up security measures through various means includes the following: \* Forcing users to update password every X number of days. \* Educating the users. \* Firewalls - Anti-malware.

1. **Given the scenario for your IT risk mitigation plan, what influence did your scenario have on prioritizing your identified risks, threats, and vulnerabilities?**

Common things such as user activity can be a very big risk, so your best bet is to consider all options as potential threats. You will have to rank some risk higher than the others

**4. What risk mitigation solutions do you recommend for handling the following risk element? User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers.**

A user inserts a CD or USB hard drive with personal photos, music, and videos on organization owned computers. A good antivirus program and have all devices scanned as soon as they are plugged in. Educate employees Disable optical drives/USB ports

1. **What is a security baseline definition?**

A "Security Baseline" defines a set of basic security objectives which must be met by any given service orsystem. The objectives are chosen to be pragmatic and complete, and do not impose technical means.

1. What questions do you have for executive management in order to finalize your IT risk mitigation plan?

* How did the executive team become acquainted with cutting-edge risk management techniques?
* Are you utilizing a recognized risk standard or framework to manage risk and uncertainty in general?
* How have you delegated risk management inside your organizations?

1. **What is the most important risk mitigation requirement you uncovered and want to communicate to executive management? In your opinion, why is this the most important risk mitigation requirement?**

Evaluating risk relationships and common causes is important since you can't reduce a risk if you don't know what it is.

1. **Based on your IT risk mitigation plan, what is the difference between short-term and long-term risk mitigation tasks and on-going duties?**

Short-term risks are those that can be rectified quickly and will (most likely) have no long-term consequences for the firm; long-term risks, on the other hand, are those that can result in fines if they entail compliance concerns. Ongoing chores are the everyday tasks that must be completed in order for the firm to operate safely.

1. **Which of the seven domains of a typical IT infrastructure is easy to implement risk mitigation solutions but difficult to monitor and track effectiveness?**

LAN-to-WAN

1. **Which of the seven domains of a typical IT infrastructure usually contains privacy data within systems, servers, and databases?**

Application

1. **Which of the seven domains of a typical IT infrastructure can access privacy data and also store it on local hard drives and disks?**

Workstation

1. **Why is the Remote Access Domain the most risk prone of all within a typical IT infrastructure?**

Because it enables people to access to the intranet from afar. Users can connect to network resources with ease. If the remote access server is a dial-in server, users can connect by dialing in. You can also utilize a virtual private network (VPN) (VPN). A VPN enables users to connect to a private network over a public network such as the internet. You must, however, reduce the danger of an attacker gaining unauthorized access to the same resources. Users who work from home computers or mobile devices such as laptops while on the job may drastically enhance their productivity and flexibility using remote access solutions.

1. **When considering the implementation of software updates, software patches, and software fixes, why must you test this upgrade or software patch before you implement this as a risk mitigation tactic?**

To ensure that there are no harmful elements, such as viruses, that might propagate to other systems

1. **Are risk mitigation policies, standards, procedures, and guidelines needed as part of your long-term risk mitigation plan? Why or why not?**

Yes, so no, everything is done in a certain order to ensure completion and accuracy.

1. **If an organization under a compliance law is not in compliance, how critical is it for your organization to mitigate this non-compliance risk element?**

It is critical for a company to understand which laws apply to them. Once these have been discovered, it is critical to guarantee that the company is compliant. Noncompliance might have serious ramifications. Some laws impose significant fines on organizations. Other laws may result in incarceration. Some can have a detrimental impact on an organization's capacity to do business. For example, HIPAA violations can result in fines of up to $25,000 per year. An internal compliance program can help to prevent these costly blunders.