Lab #6: Assessment Worksheet

Develop a Risk Mitigation Plan Outline for an IT Infrastructure

Course Name: Risk Management in Information Systems (IAA202)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 25/2/2023

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:

A. Executive summary

- "1" Critical - a risk, threat, or vulnerability that impacts compliance 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.
- "3" Minor - a risk, threat, or vulnerability that can impact user or employee productivity or availability of the IT infrastructure.

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

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	3
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	1
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 and 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	1
Workstation browser has software vulnerability	Workstation	3
Mobile employee needs secure browser	User	3

access to sales order entry system		
Service provider has a major network outage	WAN	2
Weak ingress/egress traffic filtering degrades performance	LAN-to-WAN	3
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	User	2
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	3
Need to prevent eavesdropping on WLAN due to customer privacy data access	LAN	1
DoS/DDoS attack from the WAN/Internet	WAN	1

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

- Unauthorized access from public Internet - Remote Access
- Hacker penetrates your IT infrastructure and gains access to your internal network - LAN-to-WAN
- Fire destroys primary data centre - System/Application
- Unauthorized access to organization-owned workstations - Workstation
- Denial of service attack on organization DMZ and e-mail server - LAN-to-WAN
- User downloads and clicks on an unknown - User
- Need to prevent eavesdropping on WLAN due to customer privacy data access - LAN
- DoS/DDoS attack from the WAN/Internet –WAN

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

- Unauthorized access from public Internet: strengthen firewall security and install IPS and IDS systems to the infrastructure
- Hacker penetrates your IT infrastructure and gains access to your internal network: identify and fix the vulnerabilities
- Fire destroys primary data centre: Deploy an upgrade or a patch as recommended by the vendor of the affected software
- Unauthorized access to organization-owned workstations: Reduce risk by implementing controls such as robust access control system, employee control and emergency response
- Denial of service attack on organization DMZ and e-mail server: Develop a remediation plan for action and coordination across the organization if vulnerabilities cannot be remediated within the recommended timeframes
- User downloads and clicks on an unknown: Restrict user access and set it up so that a user has to get authorization for downloads.
- Need to prevent eavesdropping on WLAN due to customer privacy data access: should use WPA2 encryption for your wireless router and access points.
- DoS/DDoS attack from the WAN/Internet: using a firewall to prevent attackers from detecting your IP address which can be used to launch an attack on your router.

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

- Discover: Identify vulnerabilities through testing and scanning
- Prioritize: Classify the vulnerabilities and assess the risk
- Remediate: Block, patch, remove components, or otherwise address the weaknesses
- Monitor: Continue monitoring for new vulnerabilities and weaknesses

F. On-going IT risk mitigation steps for the seven domains of a typical IT infrastructure

- User: Implement user awareness training, enforce strong password policies, restrict user privileges and access rights
- Workstation: Install antivirus software, enable firewall settings, apply security patches, encrypt hard drives
- LAN: Use secure protocols such as HTTPS and SSH, segment your network with VLANs or subnets, implement network access control (NAC) systems
- LAN-to-WAN: Use VPNs or proxies to encrypt traffic between networks, configure routers and switches with security features such as ACLs and port security
- WAN: Use dedicated lines or leased lines for sensitive data transmission, monitor network performance and traffic patterns for anomalies
- Remote access: Use multifactor authentication (MFA) for remote users, limit remote access to authorized devices only
- System/application: Perform regular backups and testing of critical systems and applications, implement secure coding practices and vulnerability scanning tools

G. Cost magnitude estimates for work effort and security solutions for the critical risks

- Define Estimate’s Purpose
- Develop Estimating Plan
- Define Project Scope
- Identify Project Resources
- Break Down Structure
- Obtain Data
- Develop Point Estimate
- Assess the Quality of the Estimate
- Analyze Risks
- Document Estimate and Present to Management

H. Implementation plans for remediation of the critical risks

- Acknowledge potential risks: Identify and assess the sources, causes, and impacts of possible risks
- Create a systematic risk management and classification: Analyze and prioritize the risks based on their likelihood and severity
- Create remediation strategies: Select and implement appropriate actions to reduce, avoid, transfer or accept each risk
- Address additional remediation efforts: Monitor and review the effectiveness of your actions and update them as needed

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

1. Why is it important to prioritize your IT infrastructure risks, threats, and vulnerabilities?
- **Answer**: It is important to prioritize your IT infrastructure risks, threats, and vulnerabilities because they can compromise your system's security, performance, and availability. By prioritizing your IT infrastructure risks, threats, and vulnerabilities, you can identify the most critical ones that need immediate attention and mitigation. You can also allocate your resources more efficiently and effectively to protect your system from potential harm.

2. 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?
- **Answer**: Setting up security measures through various means includes the following:
  - Forcing users to update password every 15-30 number of days.
  - Educating the users.
  - Firewalls - Anti-malware

3. Given the scenario for your IT risk mitigation plan, what influence did your scenario have on prioritizing your identified risks, threats, and vulnerabilities?
- **Answer**: Any changes to the scenario would alter the critical and minor risks. As the critical risks are identified, they can be prioritized above the minor, and then in ascending order of priority.

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

5. What is a security baseline definition?
- **Answer**: Deny the use of USB ports and control the installation of such devices.

6. What questions do you have for executive management in order to finalize your IT risk mitigation plan?
- **Answer**: A security baseline is a group of Microsoft-recommended configuration settings that explains their security implication. These settings are based on feedback from Microsoft security engineering teams, product groups, partners, and customers. Security baselines help you apply and enforce granular security settings that are recommended by the relevant security teams. You can also customize each baseline you deploy to enforce only those settings and values you require.

7. 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?
- **Answer**: The potential impact of major external risks on your business objectives and strategies

8. Based on your IT risk mitigation plan, what is the difference between short-term and long-term risk mitigation tasks and on-going duties?
- **Answer**: Short-term and long-term risk mitigation tasks are strategies to help lessen or halt potential risks to a project. Short-term tasks are those that can be fixed rapidly and will not have long-term effects on the company, such as replacing faulty equipment or hiring temporary staff. Long-term tasks are those that require more planning and resources and can have significant impacts on the company's future. On-going duties are the daily responsibilities that ensure the smooth operation of the project, such as monitoring performance, reporting progress or updating stakeholders.

9. Which of the seven domains of a typical IT infrastructure is easy to implement risk mitigation solutions but difficult to monitor and track effectiveness?
- **Answer**: Remote access domain

10. Which of the seven domains of a typical IT infrastructure usually contains privacy data within systems, servers, and databases?
- **Answer**: System/application domain

11. Which of the seven domains of a typical IT infrastructure can access privacy data and also store it on local hard drives and disks?
- **Answer**:Workstation domain

12. Why is the Remote Access Domain the most risk prone of all within a typical IT infrastructure?
- **Answer**: The Remote Access Domain is the most risk-prone of all within a typical IT infrastructure because it involves connecting to an organization's network from a remote location, such as a home or a public place.

13. 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?
- **Answer**: You must test software updates, patches, and fixes before you implement them as a risk mitigation tactic because they may have unintended consequences or conflicts with your existing systems or configurations. Testing will help you identify and resolve any issues before they affect your production environment or cause downtime, data loss, security breaches, or performance degradation. Testing will also help you verify that the updates, patches, and fixes are effective and address the vulnerabilities or bugs that they are intended to fix.

14. Are risk mitigation policies, standards, procedures, and guidelines needed as part of your long-term risk mitigation plan? Why or why not?
- **Answer**: Risk mitigation policies, standards, procedures and guidelines are needed as part of your long-term risk mitigation plan because they:

  - Help you define potential threats, assess their impacts and decide on steps to mitigate their effects.

- Provide a consistent and systematic approach to risk management across your organization.
- Enhance your accountability and transparency to stakeholders and regulators.
- Reduce the likelihood and severity of negative outcomes and losses.

15. 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?
- **Answer**: Compliance law refers to the obeyance of a particular law, rule or act in accordance with an agreement. Non-compliance risk is the possibility of facing penalties, reputational damage or access limitations for failing to follow the applicable laws and regulations.