Lab #6 Developing a Risk-Mitigation Plan Outline for an IT Infrastructure

Introduction

Identifying and assessing risks is challenging, but treating them is another matter entirely. Treating risks means making changes based on a risk assessment and probably a few hard decisions. When treating even the most straightforward of risks, practice due diligence by documenting what steps you are taking to mitigate the risk. If you don't document the change and the reasoning behind it, it's possible that your organization could reverse the mitigation and reintroduce the risk based on the notion of "but that's how we always did it before."

After you've addressed a risk, appoint someone to make certain that the risk treatment is being regularly applied. If a security incident arises even with the change in place, having a single person in charge will ensure that any corrective action aligns with the risk-mitigation plan. You're not appointing someone so you can blame that person if things go wrong; you are instead investing that individual with the autonomy to manage the incident effectively. The purpose of a risk-mitigation plan is to define and document procedures and processes to establish a baseline for ongoing mitigation of risks in the seven domains of an IT infrastructure.

In this lab, you will identify the scope for an IT risk-mitigation plan, you will align the plan's major parts with the seven domains of an IT infrastructure, you will define the risk-mitigation steps, you will define procedures and processes needed to maintain a security baseline for ongoing mitigation, and you will create an outline for an IT risk-mitigation plan.

Learning Objectives

Upon completing this lab, you will be able to:

- Identify the scope for an IT risk-mitigation plan focusing on the seven domains of a typical IT infrastructure.
- Align the major parts of an IT risk-mitigation plan in each of the seven domains of a typical IT infrastructure.
- Define the tactical risk-mitigation steps needed to remediate the identified risks, threats, and vulnerabilities commonly found in the seven domains of a typical IT infrastructure.
- Define procedures and processes needed to maintain a security baseline definition for ongoing risk mitigation in the seven domains of a typical IT infrastructure.
- Create an outline for an IT risk-mitigation plan encompassing the seven domains of a typical IT infrastructure.

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

1. Lab Report file;
2. Lab Assessments file.

Hands-On Steps

▶Note:
This is a paper-based lab. To successfully complete the deliverables for this lab, you will need access to Microsoft® Word or another compatible word processor. For some labs, you may also need access to a graphics line drawing application, such as Visio or PowerPoint. Refer to the Preface of this manual for information on creating the lab deliverable files.

1. On your local computer, **create** the **lab deliverable files**.

2. **Review** the **Lab Assessment Worksheet**. You will find answers to these questions as you proceed through the lab steps.

3. **Review** the seven domains of a typical IT infrastructure (see Figure 1).

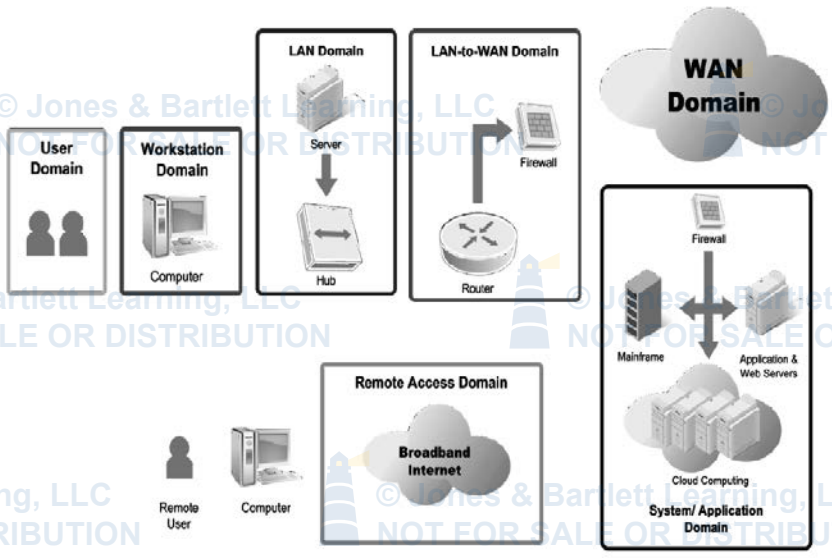

Figure 1 Seven domains of a typical IT infrastructure

4. Using the following table, **review** the results of your assessments in the Performing a Qualitative Risk Assessment for an IT Infrastructure lab in this lab manual. In addition, **review** the results of how you categorized and prioritized the risks for the IT infrastructure in that lab:

Risks, Threats, and Vulnerabilities	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		
Intraoffice employee romance gone bad		
Fire destroys primary data center		
Service provider service level agreement (SLA) is not achieved		
Workstation operating system (OS) has a known software vulnerability		
Unauthorized access to organization-owned workstations		
Loss of production data		
Denial of service attack on organization Demilitarized Zone (DMZ) and e-mail server		
Remote communications from home office		
Local Area Network (LAN) server OS has a known software vulnerability		
User downloads and clicks on an unknown e-mail attachment		
Workstation browser has a 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		
Virtual Private Network (VPN) tunneling between remote computer and ingress/egress router is needed		
Wireless Local Area Network (WLAN) access points are needed for LAN connectivity within a warehouse		
Need to prevent eavesdropping on WLAN due to customer privacy data access		
Denial of service (DoS)/distributed denial of service (DDoS) attack from the Wide Area Network (WAN)/Internet		

5. In your Lab Report file, **organize** the qualitative risk assessment data according to the following:

   - **Review** the executive summary from the Performing a Qualitative Risk Assessment for an IT Infrastructure lab in this lab manual.
   - **Organize** all of the critical "1" risks, threats, and vulnerabilities identified throughout the seven domains of a typical IT infrastructure.

Fighting Fear

In the real world, some managers will accept risk rather than make changes to mitigate it. If they offer up only vague reasons for sticking with the status quo, then their decision is likely based on fear of change. Don't let their fear stop you from treating the risk.

Here are two tips to fight a manager's fear:

- Prepare for your manager's "What if?" questions. Example of a manager's question: "What if we apply the firewall but it also stops network traffic we want, such as from our applications?" Your answer: "We've tested nearly all applications with the chosen firewall. And we're prepared to minimize unforeseen outages."
- Know, in concrete terms, what will happen if the risk is not treated. Example of a manager's question: "What is supposed to happen that hasn't happened already?" Your answer will come from the risk assessment you've performed, which will calculate the risk's likelihood and consequences.

6. On your local computer, **open** a new **Internet browser window**.

7. In the address box of your Internet browser, **type** the URL **http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-impact-assessment-and-prioritization** and **press Enter** to open the Web site.

8. **Read** the article titled "Risk Impact Assessment and Prioritization."

9. In your Lab Report file, **describe** the purpose of prioritizing the risks prior to creating a risk-mitigation plan.

10. In your Lab Report file, **describe** the elements of an IT risk-mitigation plan outline by covering the following major topics:

    - Executive summary
    - Prioritization of identified risks, threats, and vulnerabilities organized into the seven domains
    - Critical "1" risks, threats, and vulnerabilities identified throughout the IT infrastructure
    - Short-term remediation steps for critical "1" risks, threats, and vulnerabilities
    - Long-term remediation steps for major "2" and minor "3" risks, threats, and vulnerabilities
    - Ongoing IT risk-mitigation steps for the seven domains of a typical IT infrastructure
    - Cost magnitude estimates for work effort and security solutions

- Implementation plans for remediation

11. In your Lab Report file, **create** a detailed IT risk-mitigation plan outline by inserting appropriate subtopics and sub-bullets.

▶Note:
This completes the lab. **Close** the **Web browser**, if you have not already done so.

Evaluation Criteria and Rubrics

The following are the evaluation criteria for this lab that students must perform:

1. Identify the scope for an IT risk-mitigation plan focusing on the seven domains of a typical IT infrastructure. – **[20%]**
2. Align the major parts of an IT risk-mitigation plan in each of the seven domains of a typical IT infrastructure. – **[20%]**
3. Define the tactical risk-mitigation steps needed to remediate the identified risks, threats, and vulnerabilities commonly found in the seven domains of a typical IT infrastructure. – **[20%]**
4. Define procedures and processes needed to maintain a security baseline definition for ongoing risk mitigation in the seven domains of a typical IT infrastructure. – **[20%]**
5. Create an outline for an IT risk-mitigation plan encompassing the seven domains of a typical IT infrastructure. – **[20%]**