Lab #1 Identifying Threats and Vulnerabilities in an IT Infrastructure

Introduction

The task of identifying risks in an IT environment can become overwhelming. Once your mind starts asking "what if…?" about one IT area, you quickly begin to grasp how many vulnerabilities exist across the IT spectrum. It may seem impossible to systematically search for risks across the whole IT environment.

Thankfully, a solution is at hand that simplifies identifying threats and vulnerabilities in an IT infrastructure. That method is to divide the infrastructure into the seven domains: Wide Area Network (WAN), Local Area Network-to-Wide Area Network (LAN-to-WAN), Local Area Network (LAN), Workstation, User, System/Application, and Remote Access. Systematically tackling the seven individual domains of a typical IT infrastructure helps you organize the roles, responsibilities, and accountabilities for risk management and risk mitigation.

In this lab, you will identify known risks, threats, and vulnerabilities, and you will organize them. Finally, you will map these risks to the domain that was impacted from a risk management perspective.

Learning Objectives

Upon completing this lab, you will be able to:

- Identify common risks, threats, and vulnerabilities found throughout the seven domains of a typical IT infrastructure.
- Align risks, threats, and vulnerabilities to one of the seven domains of a typical IT infrastructure.
- Given a scenario, prioritize risks, threats, and vulnerabilities based on their risk impact to the organization from a risk-assessment perspective.
- Prioritize the identified critical, major, and minor risks, threats, and software vulnerabilities found throughout 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).

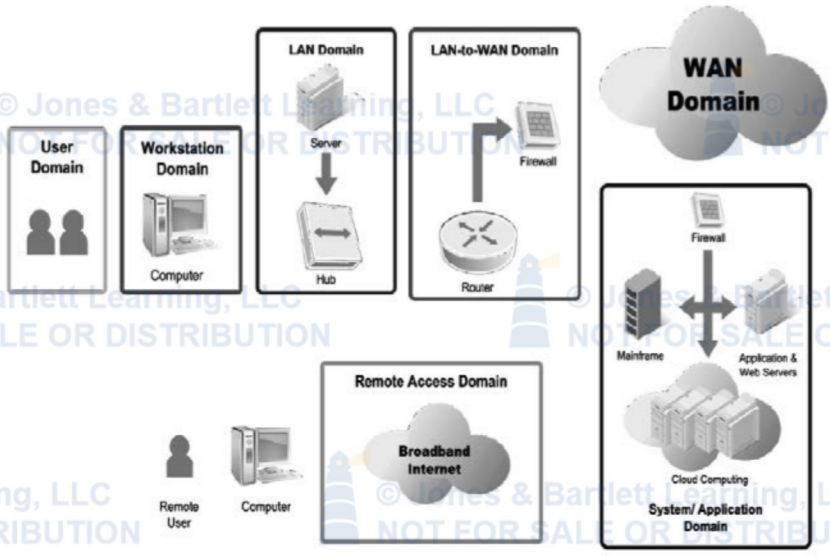

Figure 1 Seven domains of a typical IT infrastructure

4. In your Lab Report file, **describe** how risk can impact each of the seven domains of a typical IT infrastructure: User, Workstation, Local Area Network (LAN), Local Area Network-to-Wide Area Network (LAN-to-WAN), Wide Area Network (WAN), Remote Access, and System/Application domains.
5. **Review** the left-hand column of the following table of risks, threats, and vulnerabilities that were found in a health care IT infrastructure servicing patients with life-threatening conditions:

Risks, Threats, and Vulnerabilities	Primary Domain Impacted
Unauthorized access from public Internet	
Hacker penetrates IT infrastructure through modem bank	
Communication circuit outages	
Workstation operating system (OS) has a known software vulnerability	
Denial of service attack on organization's e-mail server	
Remote communications from home office	
Workstation browser has software vulnerability	
Weak ingress/egress traffic-filtering degrades performance	
Wireless Local Area Network (WLAN) access points are needed for LAN connectivity within a warehouse	
Need to prevent rogue users from unauthorized WLAN access	
Doctor destroys data in application, deletes all files, and gains access to internal network	
Fire destroys primary data center	
Intraoffice employee romance gone bad	
Loss of production data server	
Unauthorized access to organization-owned workstations	
LAN server OS has a known software vulnerability	
Nurse downloads an unknown e-mail attachment	
Service provider has a major network outage	
A technician inserts CDs and USB hard drives with personal photos, music, and videos on organization-owned computers	
Virtual Private Network (VPN) tunneling between the remote computer and ingress/egress router	

▶ Note:

Some risks will affect multiple IT domains. In fact, in real-world environments, risks and their direct consequences will most likely span across several domains. This is a big reason to implement controls in more than one domain to mitigate those risks. However, for the exercise in step 6 that follows, consider and select only the domain that would be most affected.

Subsequent next steps in the real world include selecting, implementing, and testing controls to minimize or eliminate those risks. Remember that a risk can be responded to in one of four ways: accept it, treat it (minimize it), avoid it, or transfer it (for example, outsource or insurance).

6. In your Lab Report file, **complete** the table from the previous step by identifying which of the seven domains of a typical IT infrastructure will be most impacted by each item in the table's left-hand column and **explain** why.

> **▶ 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 common risks, threats, and vulnerabilities found throughout the seven domains of a typical IT infrastructure. – **[25%]**
2. Align risks, threats, and vulnerabilities to one of the seven domains of a typical IT infrastructure. – **[25%]**
3. Given a scenario, prioritize risks, threats, and vulnerabilities based on their risk impact to the organization from a risk-assessment perspective. – **[25%]**
4. Prioritize the identified critical, major, and minor risks, threats, and software vulnerabilities found throughout the seven domains of a typical IT infrastructure. – **[25%]**