Lab #6 Risk Assessment for a Hospital Information System

Grade: 7%

Scenario

You are a cybersecurity consultant hired by MetroHealth Medical Center, a large urban hospital with 500+ employees, multiple departments, and highly sensitive data systems including patient records, billing systems, and connected medical devices.

The hospital relies on:

- A centralized Electronic Health Record (EHR) system
- On-premises servers for imaging and patient databases
- Hundreds of nurse/doctor workstations
- Medical IoT devices (infusion pumps, heart monitors)
- A Wi-Fi network that spans the entire facility
- A mobile app that allows patients to view results and schedule appointments
- Cloud backup systems for redundancy
- A legacy Windows 7 system used for MRI imaging

As part of your risk assessment process, you are tasked with conducting a complete risk register and quantitative risk analysis of this system.

Learning Objectives

- Analyze complex IT environments and inventory major assets
- Identify realistic threats and vulnerabilities in a critical infrastructure setting
- Build a risk register using the full NIST 800-30 framework

There are six parts to this lab. You can make assumptions as needed. Make sure to justify your assumption.

Part 1 (10 Points): Asset Inventory

Create a table listing 10 critical IT assets in the hospital environment. Think of what assets are in a hospital system.

For each asset, include:

- Asset Name
- Asset Description
- Asset Owner
- Estimated Asset Value ($)

Example:

Asset Name	Description	Owner	Estimated Value
EHR Server	Stores all patient records	IT Dept	$1,000,000

Part 2 (20 Points): Identify at Least 10 Risk Scenarios

Write 10 well-developed risk scenarios, each with the following:

- Risk ID
- Threat Event (e.g., ransomware, insider theft)
- Threat Source (e.g., hacker, disgruntled employee)
- Vulnerability (e.g., unpatched system, poor password policy)
- Impact Description (e.g., patient care interruption, data breach)

R1: A ransomware attack targets the hospital's file servers through a phishing email. The attacker encrypts critical medical imaging files. The vulnerability is the lack of email filtering and user training. This causes delayed diagnosis and patient care.

Part 3 (30 Points): Build a Full Risk Register

Using the NIST 800-30 Table I-5 format, build a full risk register for all 10 risks. You can use the simplified table from slides and in-class activity. **Use qualitative scale (High, Med, Low, etc).**

Part 4 (20 Points): Risk Heat Map

- Use your Excel sheet to create a risk heat map to visualize Impact vs. Likelihood of each risk.
- Refer to the YouTube video linked in the chapter slides.
- Each risk should be clearly labeled and placed in the appropriate zone.
- Use color coding (e.g., red for high risk, yellow for medium, green for low).

Part 5 (10 Points): Perform Quantitative Risk Analysis for 3 Risks

Select 3 of your identified risks and calculate (Assume values as needed):

a. Single Loss Expectancy (SLE) = Asset Value × Exposure Factor (%)
b. Annual Rate of Occurrence (ARO) = How many times the event might occur per year
c. Annualized Loss Expectancy (ALE) = SLE × ARO

Example:

Risk ID	Asset Value	Exposure Factor	SLE	ARO	ALE
R1	$500,000	60%	$300,000	0.5	$150,000

Part 6 (10 Points): Executive Summary (Short Paragraph)

Write a brief (4–6 sentence) executive summary explaining:

1. Which risk presents the highest risk score or ALE
2. Your top 1–2 recommendations for improvement

Submission:

Submit a single PDF to D2L.