Cybersecurity Risk Assessment & Asset Inventory

Portfolio Submission

Overview

This portfolio submission demonstrates foundational cybersecurity risk assessment and asset management skills. It includes:

1. A **risk register evaluation** for a commercial bank's funds based on likelihood and impact.

2. A **home network asset inventory** identifying devices, access characteristics, and sensitivity classifications.

Together, these exercises show practical application of **risk analysis, asset identification, and security prioritization** aligned with real-world environments.

Part 1: Commercial Bank Risk Register Assessment

Scenario Summary

I joined a cybersecurity team at a commercial bank conducting a risk assessment of its operational environment. The bank manages sensitive financial data, supports over 2,000 individual accounts and 200 commercial accounts, employs both on-premise and remote staff, and operates under strict financial regulations. The goal of this exercise was to evaluate risks to the bank's funds and help prioritize mitigation efforts.

Risk is calculated using the formula:

Risk = Likelihood × Impact

Likelihood is scored on a scale of **1–3**, where:

- **1** = Low likelihood

- **2** = Moderate likelihood
- **3** = High likelihood

Operating Environment & Risk Exposure (40–60 words)

Security events are possible due to a mix of human, technical, and environmental risks. Business email compromise and database exposure can result from weak authentication or misconfigured access controls. Theft and fraud remain concerns due to the bank's client-facing operations, while supply chain disruptions are possible because the bank is located in a coastal region.

Risk Likelihood Assessment

Risk	Likelihood (1–3)	Justification
Business Email Compromise	3	Common attack vector targeting employees through phishing and credential theft
Compromised User Database	2	Moderate risk due to many users and systems accessing sensitive data
Financial Records Leak	2	Possible if access controls or encryption fail
Theft	1	Low local crime rate, but still possible due to sensitive assets
Supply Chain Attack	1	Coastal location increases exposure, but events are infrequent

---

Part 2: Home Network Asset Inventory

Purpose

This exercise focuses on identifying network-connected devices in a home business environment to determine which assets contain sensitive information and require stronger

protection. Asset inventories help security professionals understand **attack surfaces** and prioritize safeguards.

Identified Assets

Three additional devices connected to the home network were identified and evaluated.

Asset Inventory Table

Asset	Network Access	Owner	Location	Notes	Sensitivity
Laptop Computer	Daily	Owner	Same room as router	Contains business documents and credentials; frequently used for work	Confidential
Smartphone	Constant	Owner	Throughout home	Stores email, MFA apps, and personal data; connects via Wi-Fi and cellular	Confidential
External Hard Drive	Occasional	Owner	Desk near desktop	Used for backups of sensitive files; only connected when needed	Restricted

---

Sensitivity Classification Rationale

- **Confidential**: Devices containing personal, financial, or authentication-related data that could cause significant harm if exposed.
- **Restricted**: Assets storing backups or critical business data that would severely impact operations if compromised.

Key Skills Demonstrated

- Risk identification and likelihood evaluation
- Understanding of operational and environmental risk factors
- Asset inventory creation and classification
- Application of confidentiality, integrity, and availability (CIA) principles
- Clear documentation suitable for audits and stakeholder review