Commercial Bank Risk Assessment Project

Project Overview

As a cybersecurity analyst at a commercial bank, I conducted a comprehensive risk assessment of the organization's operational environment. This project demonstrates my ability to identify, analyze, and prioritize security risks using industry-standard methodologies and the NIST Cybersecurity Framework (CSF).

Business Context

The assessment was performed for a commercial bank with the following characteristics:

- Geographic location: Coastal area with low crime rates
- Workforce: 100 on-premise employees, 20 remote employees
- Customer base: 2,000 individual accounts, 200 commercial accounts
- Marketing partnerships: One professional sports team, ten local businesses
- Regulatory environment: Subject to strict financial regulations including Federal Reserve requirements

Methodology

The risk assessment followed these key steps:

1. Environment analysis and risk identification
2. Likelihood assessment (Scale: 1-3)
3. Impact severity evaluation (Scale: 1-3)
4. Risk prioritization using the formula: Risk Score = Likelihood × Severity

Risk Assessment Results

1. Business Email Compromise

- Likelihood Score: 3 (High)
    - Rationale: Regular phishing attempts targeting financial institutions
- Severity Score: 3 (High)
    - Rationale: Potential for significant financial losses and data breaches

- Risk Score: 9

2. Compromised User Database

- Likelihood Score: 2 (Moderate)
    - Rationale: Enhanced security measures but distributed workforce
- Severity Score: 3 (High)
    - Rationale: Exposure of sensitive customer data, regulatory implications
- Risk Score: 6

3. Financial Records Leak

- Likelihood Score: 2 (Moderate)
    - Rationale: Multiple access points due to employee base
- Severity Score: 3 (High)
    - Rationale: Severe regulatory penalties, customer trust impact
- Risk Score: 6

4. Physical Theft

- Likelihood Score: 1 (Low)
    - Rationale: Low crime rate area, standard security measures
- Severity Score: 2 (Moderate)
    - Rationale: Limited to physical assets, insurance coverage
- Risk Score: 2

5. Supply Chain Attack

- Likelihood Score: 2 (Moderate)
    - Rationale: Coastal location, weather-related disruptions
- Severity Score: 2 (Moderate)
    - Rationale: Business continuity plans in place
- Risk Score: 4

Risk Matrix

Severity →
Likelihood ↓ | Low (1) | Moderate (2) | High (3)

High (3) | 3 | 6 | 9
Moderate (2) | 2 | 4 | 6
Low (1) | 1 | 2 | 3

Key Findings and Recommendations

1. Business email compromise represents the highest risk (Score: 9), requiring immediate attention and resources
2. Database security and financial record protection share second priority (Score: 6)
3. Supply chain resilience needs moderate attention (Score: 4)
4. Physical security measures are adequate for the current threat level (Score: 2)

Skills Demonstrated

- Risk assessment methodology application
- Threat analysis in financial environments
- Quantitative risk scoring
- Security control prioritization
- Compliance consideration in financial services
- Business impact analysis

Tools and Frameworks Used

- NIST Cybersecurity Framework
- Risk Assessment Matrix
- Risk Register Documentation
- Quantitative Risk Analysis