Risk Register - Bank Cybersecurity Assessment

Date: 2025-03-02

Prepared by: ZAYN AK. **Organization:** Commercial Bank Cybersecurity Team
Purpose: Identify and assess risks to the bank’s funds and prioritize mitigation strategies.

---

1 Risk Overview

The bank operates in a coastal area with low crime rates but faces risks related to digital threats. With 100 on-premise employees, 20 remote employees, and over 2,200 customer accounts, securing data and funds is crucial. Key risks include unauthorized access, data breaches, and financial fraud.

---

2 Risk Assessment Table

Risk	Description	Likelihood (1-3)	Severity (1-3)	Priority Score (L × S)
Business Email Compromise (BEC)	Attackers impersonate executives to deceive employees into sending funds.	3	3	9
Compromised User Database	Hackers gain access to employee/ customer credentials through phishing or weak passwords.	3	3	9
Financial Records Leak	Unauthorized access leads to sensitive financial	2	3	6

Risk	Description	Likelihood (1-3)	Severity (1-3)	Priority Score (L × S)
	data exposure.			
Theft	Physical theft of cash or hardware storing sensitive data.	1	3	3
Supply Chain Attack	Attackers target third-party vendors to infiltrate the bank's systems.	2	2	4

3 Risk Analysis and Mitigation Strategies

Business Email Compromise (BEC)

- **Likelihood:** High (3) – Employees may fall victim to phishing attempts.
- **Severity:** High (3) – Could lead to major financial losses.
- **Mitigation:** Implement email filtering, phishing awareness training, and strong sender authentication.

Compromised User Database

- **Likelihood:** High (3) – Phishing and weak passwords are common risks.
- **Severity:** High (3) – Data breaches could cause financial and reputational harm.
- **Mitigation:** Enforce strong password policies, multi-factor authentication (MFA), and regular security audits.

Financial Records Leak

- **Likelihood:** Medium (2) – Security flaws or insider threats could cause data exposure.
- **Severity:** High (3) – Regulatory fines and legal issues may arise.

- **Mitigation:** Encrypt sensitive financial data, restrict access using role-based control, and conduct regular audits.

Theft

- **Likelihood:** Low (1) – Physical security measures make it unlikely.
- **Severity:** High (3) – If it occurs, data loss could be catastrophic.
- **Mitigation:** Strengthen access control, install surveillance, and secure physical assets.

Supply Chain Attack

- **Likelihood:** Medium (2) – Vendors may not follow best security practices.
- **Severity:** Medium (2) – Attackers can infiltrate systems through suppliers.
- **Mitigation:** Conduct vendor security assessments, require compliance with security standards, and monitor third-party integrations.

---

4 Conclusion

This risk assessment highlights critical threats to the bank's operations. The most urgent concerns are **Business Email Compromise (BEC)** and **Compromised User Database**, both receiving the highest priority score (9). Immediate mitigation measures should focus on **email security, strong authentication practices, and employee security training** to reduce the likelihood of these threats.

By addressing these risks through proactive security measures, the bank can strengthen its defenses and protect sensitive financial data.

Prepared by: ZAYN AK **Date:** 2025-03-02