Evaluating Risks

Operational Environment

The bank’s location is in a coastal area with low crime rates. Many people and systems handle the bank's data—100 on-premises employees and 20 remote employees. The customer base of the bank includes 2,000 individual accounts and 200 commercial accounts. The bank's services are marketed by a professional sports team and ten local businesses in the community. There are strict financial regulations that require the bank to secure their data and funds, like having enough cash available each day to meet Federal Reserve requirements.

Notes:
There are multiple interfaces of potential vulnerabilities - numerous employees handling data on-premises and remotely, a wide customer base, and varied marketing strategies. With strict financial regulations, the bank cannot afford breaches. The coastal location also introduces natural disaster risks, affecting both digital and physical operations.

Asset	Risk(s)	Description	Likelihood	Severity	Priority
Funds	Business Email Compromise	An employee is tricked into sharing confidential information.	2 Given the large number of employees and the commonplace nature of email scams, this risk has a moderate chance of occurring.	3 A successful business email compromise can lead to significant financial and reputational damage.	6
	Compromised User Database	Customer data is poorly encrypted.	2 Poor encryption practices can easily be exploited if discovered by malicious actors.	3 Leaked customer data would severely damage the bank's reputation and could lead to heavy regulatory fines.	6
	Financial Records Leak	A database server of backed-up data is publicly accessible.	3 Assuming the database that’s publicly accessible has sensitive financial records information on it, the likelihood is high.	3 Leaked financial records would have serious implications for the bank's operations, reputation, and might attract regulatory penalties.	9
	Theft	The bank's safe is left unlocked.	1 Given the bank's location in a low crime area and assuming regular checks, the possibility is rare.	3 Direct financial loss and reputational damage would be immense.	3

	Supply Chain Disruption	Delivery delays due to natural disasters.	1 Even though the bank is in a coastal area, major disruptions like hurricanes are relatively rare.	2 While a disruption might not immediately compromise the bank's funds, it could hinder operations and financial obligations.	2

Risk Factors:
The bank's expansive operations put both its digital and physical assets at risk. Vulnerabilities span from email scams and database insecurities to public server exposures and potential natural disasters.

<u>Recommendations Using NIST CSF</u>

Identify:

- Asset Management – Ensure all databases and backup servers are inventoried and documented.
- Risk Assessment – Regularly reassess risks, especially those scored high in this assessment.
- Governance – Review current cybersecurity governance practices to ensure alignment with bank's risk strategy.

Protect:

- Access Control – Implement strict access controls, especially for sensitive data. Ensure databases are not publicly accessible.
- Training and Awareness – Conduct regular training sessions to prevent risks like business email compromise.
- Data Security – Encrypt sensitive customer data. Review and upgrade encryption methods to keep up with the latest standards.

Detect:

- Anomalies and Events – Monitor system logs for any anomalies or unauthorized access attempts.
- Security Continuous Monitoring – Ensure real-time monitoring of all data inflows and outflows.

Respond:

- Response Planning – Have a clear plan for incidents like data leaks or email compromises, ensuring rapid containment and mitigation.
- Communications – Ensure clear lines of communication internally and with affected parties during a breach.

Recover:

- Recovery Planning – In the case of a data breach, have a plan for data recovery and system restoration.
- Improvements – Post-incident, analyze the breach's cause, and take steps to prevent a recurrence.