Risk Assessment of Financial Institution

Operational environment:

The bank is located in a coastal area with low crime rates. Many people and systems handle the bank's data - 100 on premise 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.

Scenario

I'm a cybersecurity analyst at a commercial bank. The team is conducting a risk assessment of the bank's current operational environment. As part of the assessment, the team is tasked with creating a risk register to help them focus on securing the most vulnerable risks; risk register is a central record of potential risks to an organization's assets, information systems, and data.

My task is to evaluate a set of risks that the team has recorded in the risk register. For each risk, I need to first determine the likelihood of the occurrence. Then, I need to determine the severity of the risk towards the bank. Finally, I need to calculate a score that would determine the priority for the team to pay attention to.

Risk Register

The team has listed five primary risks to the bank's funds. Note that risks could come from various sources including malicious attackers, accidental human errors, and natural/environmental hazards such as a structural failure or power outage.

- Business email compromise
- Compromised user database
- Financial records leak
- Theft
- Supply chain attack

Risk Assessment

Asset	**Risk(s)**	**Description**	**Likelihood**	**Severity**	**Priority**
Funds	Business email compromise	*An employee is tricked into sharing confidential information.*	2	2	4
	Compromised user database	*Customer data is poorly encrypted.*	2	3	6
	Financial records leak	*A database server of backed up data is publicly accessible.*	3	3	9

	Theft	*The bank's safe is left unlocked.*	2	3	6
	Supply chain disruption	*Delivery delays due to natural disasters.*	1	2	2
Notes	**Risk notes:** *Risk of financial records leak: **Priority score of 9*** *With 2000 individual and 200 commercial accounts the bank holds, there are elevated risks of data leak. The bank holds its financial records in publicly accessible database server, and a leak of financial records might lead to a loss of profits, a loss of customers, and heavy regulatory penalty. In addition, dealing with many third parties could increase the attack surface potentially resulting in security incidents of sensitive financial information leak that are beyond the bank's control. This risk should be given the top priority for the team because it can greatly impact the bank's ability to operate.* *Risk of compromised user database: **Priority score of 6*** *The banks is holding 2200 customer accounts with poor data encryption, and this adds risks of potential data compromise which could result in regulatory fines and reputational damage. Further investigation of data encryption method would be needed to fully assess the risk.* *Risk of theft: **Priority score of 6*** *The risk of theft is very important as customers trust the bank to safeguard their assets; the consequences could severely jeopardize the business operations. There is an added risk of theft as the bank's safe is left unlocked. I assigned the likelihood as moderate because the bank is in an area with low crime rates.* *Risk of business email compromise: **Priority score of 4*** *With total 120 employees working for the bank, there are added risks of phishing and social engineering. We have learned that an employee had been tricked into sharing confidential information with an outsider; the security team should investigate the incident to assign the severity level more accurately.* *Risk of supply chain disruption: **Priority score of 2*** *This risk is regarded as unlikely due to the unpredictability of natural disasters. Being located in a coastal area, there is a low chance of supply chain disruptions caused by hurricanes. The risk could be more elevated in certain hurricane seasons.* **Likelihood score:** *I needed to estimate and score the likelihood of the risk causing a security event. The likelihood can be based on available evidence, prior experience, or expert judgement. A common way to estimate is to determine the potential frequency of the risk occurring.* *- Question: Could the risk occur once a day/month/year?*				

	All risks but ‘financial records leak’ one received low to moderate scores; the financial records leak has a high chance of occurring given the publicly accessible data server. **Severity score:** *I estimated the overall impact of the security event that could be caused by each risk. The impact could include damages in reputation or finances as well as a loss of data, customers, and assets. Evaluating the severity score helps the organization to determine the level of risk the bank could tolerate and how assets might be affected.* *- Question: How would the business be affected? What’s the financial harm to the business and its customers? Can important operations or services be impacted? Could there be violations to government regulation? What could be the reputation damage to the company’s standing?* *All risks received a severity score equal to or higher than 2 because they could lead to serious consequences such as difficulties in business continuity and potential fines and lawsuits. Furthermore, customers trust the bank to protect their information and assets; breaking this trust could jeopardize the bank’s* reputation. **Priority score:** *The goal of risk assessment is to help security teams prioritize their efforts and resources. Using the formula (Risk priority = likelihood * severity), I calculated priority score for each risk.* *The risk of financial records leak received the highest overall risk score of 9. This indicates that this risk is almost certain to happen and it would greatly affect the bank’s ability to operate. The high score indicates that the security team should prioritize remediating any issues related to this risk before resolving risks that scored lower.*

Definitions

Asset: The asset at risk of being harmed, damaged, or stolen.
Risk(s): A potential risk to the organization's information systems and data.
Description: A vulnerability that might lead to a security incident.
Likelihood: Score from 1-3 of the chances of a vulnerability being exploited. A 1 means there's a low likelihood (rare), a 2 means there's a moderate likelihood (likely), and a 3 means there's a high likelihood (certain).
Severity: Score from 1-3 of the potential damage the threat would cause to the business. A 1 means a low severity impact, a 2 is a moderate severity impact, and a 3 is a high severity impact.
Priority: How quickly a risk should be addressed to avoid the potential incident. Use the following formula to calculate the overall score: **Likelihood x Impact Severity = Risk Priority Score**