Risk register

Scenario:

Review the following scenario.

You've joined a new cybersecurity team at a commercial bank. The team is conducting a risk assessment of the bank's current operational environment. As part of the assessment, they are creating a risk register to help them focus on securing the most vulnerable risks.

A risk register is a central record of potential risks to an organization's assets, information systems, and data. Security teams commonly use risk registers when conducting a risk assessment.

Your supervisor asks you to evaluate a set of risks that the cybersecurity team has recorded in the risk register. For each risk, you will first determine how likely that risk is to occur. Then, you will determine how severely that risk may impact the bank. Finally, you will calculate a score for the severity of that risk. You will then compare scores across all risks so your team can determine how to prioritize their attention for each risk.

Operational environment:

The bank operates in a coastal area characterized by low crime rates. It encompasses a diverse ecosystem of data handlers, including 100 on-premise employees and 20 remote employees. The customer base comprises 2,000 individual accounts and 200 commercial accounts. Notably, the bank's services are actively marketed by a professional sports team and ten local businesses within the community. In line with stringent financial regulations, the bank is obligated to ensure data and fund security, such as maintaining sufficient cash reserves to meet Federal Reserve requirements on a daily basis.

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.*	1	3	3

	Supply chain disruption	*Delivery delays due to natural disasters.*	1	2	2
Notes	*Doing business with other companies might increase the risks to data since it presents other avenues for the information to be compromised. The risk of theft is important, but might not be a priority because the bank is in an area with low crime rates.*				

Asset: An asset refers to the valuable entity or resource that is susceptible to harm, damage, or theft.
Risk(s): Risks represent potential threats to the organization's information systems and data, which may lead to adverse consequences if not adequately addressed.
Description: A description outlines a vulnerability or weakness within the system that possesses the potential to culminate in a security incident.
Likelihood: The likelihood is assessed using a score ranging from 1 to 3, representing the chances of a vulnerability being exploited. A score of 1 signifies a low likelihood, while a score of 2 suggests a moderate likelihood, and a score of 3 indicates a high likelihood.
Severity: Severity is gauged using a score ranging from 1 to 3, signifying the potential damage that a threat could inflict upon the business. A score of 1 denotes a low severity impact, while a score of 2 signifies a moderate severity impact, and a score of 3 denotes a high severity impact.
Priority: Priority denotes the urgency with which a risk should be addressed to mitigate the likelihood of a potential incident. The overall risk score is calculated using the following formula: Likelihood x Impact Severity = Risk.

By aligning the scores for likelihood and severity, the team can effectively prioritize their attention and allocate resources to address the risks in a systematic manner.

Note: It is important to ensure that appropriate security measures are implemented to safeguard the bank's assets, information systems, and data, considering the unique operational environment and regulatory requirements.

Sample risk matrix

Severity

Likelihood

	Low 1	Moderate 2	Catastrophic 3
Certain 3	3	6	9
Likely 2	2	4	6
Rare 1	1	2	3