Risk register

Benjamin Taylor – Google Cybersecurity

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.

Asset	Risk(s)	Description	Likelihood	Severity	Priority
Funds	Business email compromise	*An employee is tricked into sharing confidential information.*	Certain	Catastrophic	9
	Compromised user database	*Customer data is poorly encrypted.*	Likely	Catastrophic	6
	Financial records leak	*A database server of backed-up data is publicly accessible.*	Certain	Catastrophic	9
	Theft	*The bank's safe is left unlocked.*	Rare	Catastrophic	3
	Supply chain disruption	*Delivery delays due to natural disasters.*	Likely	Moderate	4
Notes	*How are security events possible considering the risks the asset faces in its operating environment?* – Security events are possible due to human error, technical vulnerabilities, and even environmental factors. An example of a human risk could be falling for a phishing scam, whereas technical vulnerabilities could be forgetting to encrypt important information. Environmental factors (such as bad weather) could cause a disruption to the supply chain, leaving it out of human control.				

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, a 2 means there's a moderate likelihood, and a 3 means there's a high likelihood.
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**

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