Risk Register

Completed by: Hope Tan (github.com/hope-tan)

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.*	2	3	6
	Compromised user database	*Customer data is poorly encrypted.*	1	3	3
	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	While the bank's physical location has a low crime rate, the bank should still take efforts to secure its physical premises to prevent unauthorized access to servers and the money safe. Additionally, the presence of digital data means that cybercriminals can cause damage from a remote location. The bank must ensure digital security of all its assets for 3 reasons: financial loss, compliance, and reputational damage. 1. Financial Loss: Money makes banks frequent targets for financially-motivated cyber criminals, as they can steal or transfer money to their own accounts. 2. Compliance: If the bank does not apply rigorous security standards, it may get fined for noncompliance with standards like PCI DSS or GLBA. 3. Reputational Damage: Data leaks and financial losses from cyberattacks decrease the public's trust in an organization to securely guard their personal data and assets. This could lead to loss of business as these customers take their money elsewhere.				

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