Risk Assessment

Scoring risks based on likelihood and severity

Wendy Alayon
28/06/2024 **@syszern**

Risk assessment

Scenario

A new hire in a cybersecurity team at a commercial bank is conducting a risk assessment of the bank's current operational environment. As part of this assessment, a risk register is being created to prioritize securing the most vulnerable risks.

The supervisor requests an evaluation of risks recorded in the risk register by the cybersecurity team. Each risk will be assessed for likelihood of occurrence and potential impact on the bank. A severity score will be calculated for each risk, which will then be compared across all risks to prioritize attention.

Risk register

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	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

Asset	Risk(s)	Description	Likelihood	Severity	Priority
	Theft	*The bank's safe is left unlocked.*	1	3	3
	Supply chain disruption	*Delivery delays due to natural disasters.*	1	2	2
Notes	*Engaging in business with other companies could heighten data vulnerability by providing additional pathways for potential compromise. While the risk of theft remains significant, it might not be a top concern due to the bank operating in a region with low crime rates.*				

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***