## **RISK EVALUATION BY EVALUATING VULNERABILITIES THAT COMMONLY THREATEN BUSINESS OPERATIONS**

**SCENERIO**

You’ve joined a cybersecurity team at a commercial bank. the team is conducting a risk assesment of the bank’s cuurent operational environment, as part of the assesment 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 assets, information systems, and data. security teams commonly use risk registers when conducting a risk assesment.

Your supervisor ask you to evaluate a set of risks thatthe cybersecurity team has recorded in the risk register. for each risk, you will first determine how likely that risk to occur. Then, you will determine how severely that risk may impact for the bank. Finally, you will calculate a score for the securoty of that risk. you will compare scores all risks so your team can determine how to pririotize their attention for each risk.

**Step-by-Step Instructions**

1. Access the report
2. Understand the operating environment
3. Consider potential risks to assets: security events are possible when assests are at risk. the source of a risk can range from malicious attackers to accidental human errors. A risk source can even come from natural or environmental hazards, such as structural failure or power outage. the bank’s funds are one of its key assets. your team listed the five primary risks to the bank’s fund:

* Business email compromise
* Compromised user database
* Financial record leak
* theft
* Supply chain attack

consider these potential risks in relation to the bank’s operating environment. then, write 2-3 sentence (40-60 words) describing how security events are possible considering the risks facing the funds in this operating environment.

1. Score risks based on their likelihood
2. Score risks based on their severity

Risk can be calculated with this simple formula:

Livelihood × Impact/severity﹦ Risk

In order to calculate the score for security risk, you must first estimate and score the likelihood of the risk causing a security event. The livelihood of a risk can be based on available evidence, prior experience or expert judgement. A common way to estimate the likelihood of the risk is to determine the potential frequency of the risk occuring:

* could the risk happen once a day?
* could the risk happen once a month?
* could the risk happen once a year?

For example, the bank must have enough funds avalilable each day to meet its legal requirement. A potential risk that could prevent the bank from replenishing its funds is a supply chain disruption. being localated in a costal area, there’s a likelihood that the bank may experience supply chain disruptions caused by hurricanes. However, a hurricane might only impact the bak every few years, so you can score the likelihood as low.

In this instance, the team is scoring the livelihood of an events on a scale of 1-3:

* 1 represents an event with a low chance of occuring.
* 2 represents an event with a moderate chance of occuring.
* 3 represents a high chance of occring.

Review the Risks,Description, and notes of the risk register template. refer to the risk matrix and use it to estimate a likelihood score for each risk, Then , enter score (1-3) for each risk in the likelihood column of the register.

A severity score is an estimate of the overall impact that might occur as a result of an event. For example damage can occur to a company’s reputation or finances and there may be loss of data, customers or assets, evaluating the severity of a risk helps business determine the level of risk they can tolerate and how assets might be affected.

When evaluating the severity of a risk, consider the potential consequences of that risk occuring:

* How would the business be affected?
* what’s the financial harm to the business and its customer?
* Are there regulations that can be violated?
* What is the reputational damage to the company’s standing?

Use the top row risk matrix and consider potential impact of each risk. estimate a severity score for each risk. Then, enter a score (1-3) for each risk in the severity column of the register:

* 1 (low severity)
* 2 (moderate severity)
* 3 (high severity)

## **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 |
| Theft | *The bank's safe is left unlocked.* | 1 | 3 | 3 |
| Supply chain disruption | *Delivery delays due to natural disasters.* | 1 | 2 | 2 |
| Notes | *How are security events possible considering the risks the asset faces in its operating environment?* | | | | |

**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 |