## Risk register

### **Lab Scenario:**

In this lab I conducted a risk analysis layout structure to determine the potential risk for certain mains of a financial banking company that needed to meet government regulations to avoid legal arbitration conflict. The details shown below of its environment expose the potential issues the company may have to fix before it can be exploited by criminal means for government authority to audit against the business. The sections of the vulnerabilities I labeled show the rate of likelihood, severity and priority of the situational manners. This shows the complete overview of what I had to analyze.

### **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 | 3 |
| Compromised user database | *Customer data is poorly encrypted.* | 3 | 7 | 8 |
| Financial records leak | *A database server of backed up data is publicly accessible.* | 2 | 9 | 10 |
| Theft | *The bank's safe is left unlocked.* | 3 | 8 | 10 |
| Supply chain disruption | *Delivery delays due to natural disasters.* | 1 | 5 | 4 |
| Notes | *How are security events possible considering the risks the asset faces in its operating environment?*  *I’d say it’s possible due to the factors behind the severe ramifications of the event alone. The exposure of leaving anything behind for a threat to occur in these situations can easily harm people at a high level. The likelihood of any of these issues can result in a massive effect of the issue getting out of hand without noticing the vulnerabilities at the immediate reaction of it. The importance of noticing these issues should be looked at immediately to the level where there’s no means of a potential disaster or threat actor that wishes to harm against the targeted victim.* | | | | |

**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





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