## Risk register (fictive case)

### **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.* | 3 | 2 | 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.* | 1 | 3 | 3 |
| Theft | *The bank's safe is left unlocked.* | 2 | 3 | 6 |
| 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?*  ***Business email compromise:*** *It’s possible that a malicious actor falsely imitates himself as a customer of the bank, asking him sensitive information about the customer like birth of date or asking them to send personal information to the malicious actor on another email address.*  ***Compromised user database:*** *If the customer data is poorly encrypted, hackers can intercept these packets and easily decrypt and see it.*  ***Financial records leak:*** *If database records leak such as the financial info, this can impact in the bank getting a very bad reputation and losing its credibility and potentially customers.*  ***Theft:*** *If theft happens, money can be stolen which results in financial loss by unauthorzied means.*  ***Supply chain attack:*** *If we are connected with organizations in foreign countries that host our software, like USA, it can be accessed by people who hack those vendors.* | | | | |

**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 |