## 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 | *Doing business with other companies might increase the risks to data since it presents other avenues for the information to be compromised. The risk of theft is important, but might not be a priority because the bank is in an area 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. The following formula has been used to calculate the overall score: **Likelihood x Impact Severity = Risk**

## 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 |

### Likelihood

A range of likelihood scores were estimated based on factors that could lead to a security incident. Each risk was scored as a 1, 2, or 3 on a risk matrix, meaning the chances of occurring were rare, likely, or certain. A supply chain attack caused by natural disaster was scored with a 1, meaning it was regarded as unlikely due to the unpredictability of those events. On the other hand, compromised data events were scored a 2 because they are likely to occur given the possible causes.

### Severity

No risk received a severity score less than 2 because risks that involve data breaches such as business email compromise, can have serious consequences. Customers at a bank trust the businesses to protect their money and personal information. Also, the bank's operations could be terminated if they fail to comply with regulations.

### Priority

A financial records leak received the highest overall risk score of 9. This indicates that this risk is almost certain to happen and would greatly impact the bank's ability to operate. Such a high overall score signals the security team to prioritize remediating, or resolving any issues related to that risk before moving on to risks that scored lower.