Assigning Risk Scores to Identified Risks

A hand touching a screen with gears

Description automatically generated

Material & instructions developed by: Google Cybersecurity Professional Certificate Course

Completed by: Alexander Herman on 01/27/24

**Table of Contents:**

Activity Overview (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Scenario (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Risk Register/Risk Grades (Provided/My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**3**

Risk Grade Explanations (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**3-4**

**Activity Overview**



In this activity, you will practice performing a risk assessment by evaluating vulnerabilities that commonly threaten business operations. Then, you will decide how to prioritize your resources based on the risk scores you assign each vulnerability.

You might recall that the purpose of having a security plan is to be prepared for risks. Assessing potential risks is one of the first steps of the **NIST Cybersecurity Framework (CSF)**, a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. Risk assessments are how security teams determine whether their security operations are adequately positioned to prevent cyber-attacks and protect sensitive information.

**Scenario**



You've joined a new cybersecurity team at a commercial bank. The team is conducting a risk assessment of the bank's current operational environment. As part of the assessment, 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's assets, information systems, and data. Security teams commonly use risk registers when conducting a risk assessment.

Your supervisor asks you to evaluate a set of risks that the cybersecurity team has recorded in the risk register. For each risk, you will first determine how likely that risk is to occur. Then, you will determine how severely that risk may impact the bank. Finally, you will calculate a score for the severity of that risk. You will then compare scores across all risks so your team can determine how to prioritize their attention for each risk.

**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.

**Risk Register Risk Grades**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset** | **Risk(s)** | **Description** | **Likelihood** | **Severity** | **Priority** |
| Email Server & Accounts | Business email  compromise | An employee is tricked into  sharing confidential information. | 3 | 3 | 9 |
| Business Database & Information | Compromised  user database | Customer data is poorly encrypted. | 2 | 3 | 6 |
| Business Information | Financial records  leak | A database server of backed up  data is publicly accessible. | 3 | 3 | 9 |
| Physical Currency | Theft | The bank's safe is left unlocked. | 1 | 3 | 3 |
| Physical & Digital Assets | Supply chain  disruption | Delivery delays due to natural  disasters. | 2 | 2 | 4 |

**Risk Grade Explanations:**

**Business email compromise**: (Priority = **Urgent**)

* phishing attacks are a common occurrence
* poor data encryption practices
* backed up data available to public = stronger social engineering attack
* 120 possible employees to target
* “Many people and systems handle the bank's data” – too much access
* poor email security awareness
* highly marketed financial business

**Compromised user database**: (Priority = **Important**)

* poor boundary protections (publicly available database, too much access)
* remotely working employees connecting to company network
* poor email security awareness
* 120 possible employees to target
* backed up data available to public = stronger social engineering attack
* strong governing regulations
* highly marketed financial business

**Financial records leak**: (Priority = **Urgent**)

* poor boundary protections (publicly available database, too much access)
* poor email security awareness
* “Many people and systems handle the bank's data” – too much access
* poor data encryption practices
* 120 possible employees to target
* 2,000 private customers and 200 commercial accounts
* highly marketed financial business
* strong governing regulations

**Theft**: (Priority = **Review**)

* highly marketed financial business
* bad physical security practices
* poor boundary protections (publicly available database, too much access)
* backed up data available to public = stronger social engineering attack
* highly marketed financial business
* must meet Federal requirements for daily cash on-hand
* low crime rates

**Supply chain disruption**: (Priority = **Review**)

* backed up data available to public = not a secure storage that can be completely trusted
* 2,000 private customers and 200 commercial accounts
* highly marketed financial business
* located in a coastal region