Activity: The challenges of securing digital devices

Data owners and data custodians are both equally responsible for securing information. For example, as a data owner you might protect a social media account by setting a strong password. However, your information can still be compromised if data custodians, such as the employees of the social media company, use weak passwords to secure their accounts.

The devices you use in your daily life handle many types of information. Consider how you handle data based on your relationship to it.

As a data owner, how do you approach securing different types of information?

As a data custodian, how might it be challenging to protect the privacy of other people's information?

How do existing and emerging technologies factor into the challenges of safe data handling?

As a data owner, I approach securing different types of information by implementing strong passwords, encryption, and access control, modifying the sensitivity of the data.

As a data custodian, it might be challenging to protect the privacy of other people’s information because it requires maintaining strong security measures, ensuring compliance with data protection regulations, and safeguarding against potential threats.

Existing and emerging technologies factor into the challenges of safe data handling by introducing new vulnerabilities and attack vectors that custodians and owners must adapt to, necessitating ongoing cybersecurity efforts and innovation.

English

To pass this course item, you must receive 100%, or 1 out of 1 point, by completing the activity. You can learn more about graded and practice items in the course overview.

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.

Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Scenario

Review the following scenario. Then complete the step-by-step instructions.

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.

Step-By-Step Instructions

Follow the instructions and answer the question below to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

Step 1: Access the template

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	3	6
	Compromised user database	*Customer data is poorly encrypted.*	3	2	6
	Financial records leak	*A database server of backed up data is publicly accessible.*	2	2	4
	Theft	*The bank's safe is left unlocked.*	1	3	3

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

Step 2: Understand the operating environment

When conducting a risk assessment, it's important to consider the factors that could cause a security event. This often starts with understanding the operating environment.
In this scenario, your team has identified characteristics of the operating environment that could factor into the bank's risk profile:
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.

1 . Location: The bank is situated in a coastal area with low crime rate. This imply a lower likelihood of certain risks, such as theft, comapared to a high-crime urban area.
2 . Data Handling: Many people and system handle the bank’s data. There are 100 on-premises employees and 20 remote employees, which increases the potential for internal data breachs or leaks.
3 . Customer Base: The bank serves 2,000 individual accounts and 200 commercial accounts, meaning there is a significant amount of sensitive customer data to protect.

4 . Marketing: The bank’s services are marketed by a professional sports team and ten local businesses, which may attract attention and could potentially pose risks related to reputation or cuberattacks.
5 . Regulations: Strict financial regulations require the bank to secure their data and funds, emphasizing the impotance of risk management.

Step 3: Consider potential risks to assets:

Filled in on yellow highlight above table.

Step 4: Score risks based on their likelihood

Score risks based on their likelihood you can see that I’ve assigned likelihood scores to each risk based on the perceived chances of each vulnerability being exploited. The scores are between 1 and 3, with 1 representing low likelihood and 3 representing high likelihood.

Step 5: Score risks based on their severity

Score risks based on their severity “ Severity “ scores have also been assigned based on the potential damage each threat could cause to the bank. Scores range from 1 (low severity) to 3 (high severity).

Step 6: Calculate an overall risk score

To calculate the overall risk score, we have to multiply the Likelihood score by the Severity score for each risk. The results is the Priority score. I’ve already calculated and filled in the priority scores for each risk in step 3. Refering to the above table.
For example, for “Business Email Compromise,” the Priority score is 6 (Likelihood 2 x Severity 3). Another example, for “Compromised User database,” the Priority score is 6 (Likelihood 3 x Severity 2). Formula: The Priority score= Likelihood x Severity
Risk Factors
Business Email Compromise: Given the presence of many employees and systems handling the bank's data, there is a moderate likelihood (Likelihood Score 2) of an employee being tricked into sharing confidential information. The impact of this compromise could be moderate (Severity Score 2), resulting in a potential overall risk score of 4 (2 x 2).

Compromised User Database: With customer data being poorly encrypted, there is a high likelihood (Likelihood Score 3) of a breach. This has the potential for high severity (Severity Score 3) consequences. The overall risk score for this risk is 9 (3 x 3).
Financial Record leak: The publicly accessible backup data server presents a high likelihood (Likelihood Score 3) of a data leak. Such an event could have a catastrophic impact (Severity Score 3), leading to an overall risk score of 9 (3 x 3).
Theft: Leaving the bank's safe unlocked is a significant security risk. While it has a low likelihood of occurrence (Likelihood Score 1), the potential severity of this event is high (Severity Score 3), resulting in an overall risk score of 3 (1 x 3).
Supply Chain Distribution: Delivery delays due to natural disasters pose a moderate likelihood (Likelihood Score 2) of occurrence, with a moderate severity impact (Severity Score 2). This risk scores an overall risk score of 4 (2 x 2).
These risk scores can be used to prioritize the attention of the cybersecurity team, with higher overall risk scores indicating greater urgency for mitigation