Determine appropriate data handling practices

Activity Overview

In this activity, you will review the results of a data risk assessment. You will determine whether effective data handling processes are being implemented to protect information privacy.

Data is among the most valuable assets in the world today. Everything from intellectual property to guest WiFi networks should be protected with a combination of technical, operational, and managerial controls. Implementing the principle of least privilege is essential to protect information privacy.

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 work for an educational technology company that developed an application to help teachers automatically grade assignments. The application handles a wide range of data that it collects from academic institutions, instructors, parents, and students.

Your team was alerted to a data leak of internal business plans on social media. An investigation by the team discovered that an employee accidentally shared those confidential documents with a customer. An audit into the leak is underway to determine how similar incidents can be avoided.

A supervisor provided you with information regarding the leak. It appears that the principle of least privilege was not observed by employees at the company during a sales meeting. You have been asked to analyze the situation and find ways to prevent it from happening again.

First, you'll need to evaluate details about the incident. Then, you'll review the controls in place to prevent data leaks. Next, you'll identify ways to improve information privacy at the company. Finally, you'll justify why you think your recommendations will make data handling at the company more secure.

Step-by-step Instructions

Step 1: Access the template

To use the template for this course item, click the link and select *Use Template*.

Data leak worksheet

Incident summary: A sales manager shared access to a folder of internal-only documents with their team during a meeting. The folder contained files associated with a new product that has not been publicly announced. It also included customer analytics and promotional materials. After the meeting, the manager did not revoke access to the internal folder, but warned the team to wait for approval before sharing the promotional materials with others.

During a video call with a business partner, a member of the sales team forgot the warning from their manager. The sales representative intended to share a link to the promotional materials so that the business partner could circulate the materials to their customers. However, the sales representative accidentally shared a link to the internal folder instead. Later, the business partner posted the link on their company's social media page assuming that it was the promotional materials.

|  |  |
| --- | --- |
| Control | Least privilege |
| Issue(s) | *What factors contributed to the information leak?* |
| Review | *What does NIST SP 800-53: AC-6 address?* |
| Recommendation(s) | *How might the principle of least privilege be improved at the company?* |
| Justification | *How might these improvements address the issues?* |

Security plan snapshot

The NIST Cybersecurity Framework (CSF) uses a hierarchical, tree-like structure to organize information. From left to right, it describes a broad security function, then becomes more specific as it branches out to a category, subcategory, and individual security controls.

|  |  |  |  |
| --- | --- | --- | --- |
| Function | Category | Subcategory | Reference(s) |
| Protect | PR.DS: *Data security* | PR.DS-5: *Protections against data leaks.* | NIST SP 800-53: AC-6 |

In this example, the implemented controls that are used by the manufacturer to protect against data leaks are defined in NIST SP 800-53—a set of guidelines for securing the privacy of information systems.

Note: References are commonly hyperlinked to the guidelines or regulations they relate to. This makes it easy to learn more about how a particular control should be implemented. It's common to find multiple links to different sources in the references columns.

NIST SP 800-53: AC-6

NIST developed SP 800-53 to provide businesses with a customizable information privacy plan. It's a comprehensive resource that describes a wide range of control categories. Each control provides a few key pieces of information:

Control: A definition of the security control.

Discussion: A description of how the control should be implemented.

Control enhancements: A list of suggestions to improve the effectiveness of the control.

|  |  |
| --- | --- |
| AC-6 | Least Privilege |
| Control:  Only the minimal access and authorization required to complete a task or function should be provided to users. |
| Discussion:  Processes, user accounts, and roles should be enforced as necessary to achieve least privilege. The intention is to prevent a user from operating at privilege levels higher than what is necessary to accomplish business objectives. |
| Control enhancements:  Restrict access to sensitive resources based on user role.  Automatically revoke access to information after a period of time.  Keep activity logs of provisioned user accounts.  Regularly audit user privileges. |

Note: In the category of access controls, SP 800-53 lists least privilege sixth, i.e. AC-6.

Step 2: Analyze the situation

The principle of least privilege is a fundamental security control that helps maintain information privacy. However, least privilege starts to lose its effectiveness when too many users are given access to information. Data leaks commonly happen as information gets passed between people without oversight.

To start your analysis, review the following incident summary provided by your supervisor:

A customer success representative received access to a folder of internal documents from a manager. It contained files associated with a new product offering, including customer analytics and marketing materials. The manager forgot to unshare the folder. Later, the representative copied a link to the marketing materials to share with a customer during a sales call. Instead, the representative shared a link to the entire folder. During the sales call, the customer received the link to internal documents and posted it to their social media page.

After reviewing the summary, write **20-60 words (2-3 sentences)** in the **Issue(s)** row of the Data leak worksheet describing the factors that led to the data leak.

The data leak incident resulted from a lack of adherence to the principle of least privilege. The manager initially shared access to a folder of internal documents with a customer success representative, which contained sensitive materials, including unreleased product details. This unauthorized access was not revoked, and a subsequent mistake by the representative in sharing the link led to the documents being posted on social media.

Step 3: Review current data privacy controls

NIST SP 800-53: AC-6, also known as "Least Privilege," is a security control that emphasizes providing users with only the minimum access and authorization necessary to complete their tasks. It suggests enforcing processes, user accounts, and roles as needed to prevent users from operating at privilege levels higher than necessary to achieve business objectives. The control also includes enhancements such as restricting access based on user roles, automatically revoking access after a period, and maintaining activity logs of provisioned user accounts.

Step 4: Identify control enhancements

To improve the principle of least privilege, the company should consider the following enhancements:

. Implement role-based access controls to restrict access to sensitive resources based on user roles.

. Set up automated access revocation mechanisms for sensitive information after a predetermined period to reduce the risk of prolonged exposure.

. Conduct regular audits of user privileges to ensure compliance and identify any potential security gaps.

Step 5: Justify your recommendations

These recommendations for enhancing the principle of least privilege will address the issues by reducing the likelihood of unauthorized access and sharing of sensitive information. Role-based access controls and automated access revocation will ensure that only authorized personnel have access, and regular audits will help in detecting and rectifying any deviations from the least privilege principle, thus improving data handling security at the company.

Top of Form

Regenerate