Justin Goncalves

8/13/24

InfoSec Data Handling Activity (NIST CSF Activity)

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 scenario below. 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 an external business partner. 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.

Follow the instructions and fill in the sections to complete the activity.

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?* The information leak occurred because the principle of least privilege was not enforced. The sales manager allowed ongoing access to the internal folder without restricting access after the meeting. The sales team member had more access than was necessary for their task, leading to the accidental sharing of the internal folder. Additionally, there was a lack of automated mechanisms to revoke access or reminders to remove access after the task was completed.
Review	*What does NIST SP 800-53: AC-6 address?* NIST SP 800-53: AC-6 addresses the principle of least privilege, ensuring that users are granted only the minimal access and authorization required to complete their tasks or functions. The control emphasizes the need for processes, user accounts, and roles to be enforced as necessary to maintain least privilege, thereby preventing users from operating at privilege levels higher than needed to accomplish business objectives. The control also includes enhancements such as restricting access to sensitive resources based on user roles, automatically revoking access after a specified period, keeping activity logs of user accounts, and regularly auditing user privileges to ensure compliance with the principle of least privilege.

Recommendation(s)	*How might the principle of least privilege be improved at the company?* To improve the principle of least privilege at the company, it is recommended to implement automated access controls that revoke access to sensitive information after a certain period or upon task completion. Enforcing stricter role-based access controls will ensure that employees only have access to information relevant to their specific duties. Additionally, the company should establish a process for regularly auditing user privileges to identify and correct any discrepancies in access levels. Keeping activity logs for provisioned user accounts will also help monitor and enforce the appropriate levels of access.
Justification	*How might these improvements address the issues?* Implementing automated access revocation and stricter role-based access controls would ensure that employees have access only to the information necessary for their tasks, reducing the risk of accidental information leaks. Regular audits of user privileges would help identify and rectify any over-provisioned access, thereby maintaining compliance with the principle of least privilege. By keeping detailed activity logs, the company can monitor access to sensitive resources and ensure that access controls are consistently enforced. These improvements will enhance the security of the company's data handling processes, reducing the likelihood of similar incidents occurring in the future.