Data leak analysis

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 principle of least privilege was not adhered to and lead to the data leak of sensitive information. The manager did not revoke access from an internal folder which the sales team still had access to. The sales rep then shared the internal folder with a business partner who shared the entire folder to their social media.*
Review	*What does NIST SP 800-53: AC-6 address? It addresses the principle of least privilege, why and how it should be implemented. It focuses on three main points, the definition of the control, a description on how you can implement it and a list on how to improve the enhancements of the control.*

Recommendation(s)	*How might the principle of least privilege be improved at the company?* *One improvement that can be made at the company is having access to data revoked after a specified period, especially after the data is no longer in active use by the employee. Another enhancement that can be utilized is restricting access to sensitive data based on user role. The sales rep had access to marketing materials, but there were other materials that they shouldn't have had access to. Utilizing these two enhancements will help to improve the likelihood of data only being accessed by authorized users.*
Justification	*How might these improvements address the issues?* *Implementing the recommendations mentioned should help to strengthen security posture in the arena of Principle of Least Privilege. Restricting access to sensitive data will lessen the chance of accidental sharing since the party involved will understand their responsibility of keeping said data safe. Also revoking access to data when not in use can help to prevent accidental sharing as employees will not have access to said data when its not in use.*

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.