Data Leak Incident Report

Incident Summary

A sales manager shared access to a folder containing internal-only documents, including pre-release product information, customer analytics, and promotional materials, with their team during a meeting. The manager neglected to revoke access afterward and only verbally warned the team against sharing the materials without approval. During a subsequent video call, a sales representative inadvertently shared a link to the entire folder with a business partner, who then mistakenly posted it on social media, believing it to be the approved promotional materials.

Security Control: Least Privilege

Issue(s):

Several factors contributed to the data leak:

- **Overly Broad Access:** The sales team was granted access to the entire folder, exceeding the principle of least privilege, which dictates that users should only have access to the information necessary for their specific roles.
- **Lack of Automated Controls:** The reliance on a verbal warning, without any automated controls to prevent unauthorized sharing, increased the risk of human error and accidental disclosure.
- **Insufficient Review Process:** The absence of a formal review process for sharing materials with external partners created an opportunity for miscommunication and inadvertent disclosure of sensitive information.

Review: NIST SP 800-53: AC-6

NIST SP 800-53: AC-6 addresses the importance of access controls to protect the confidentiality, integrity, and availability of information systems and data. It emphasizes the need to limit access to authorized users, processes, and devices, and to grant access only to the types and amounts of information necessary to perform their duties.

Recommendation(s):

To improve the implementation of least privilege at the company, the following recommendations are proposed:

- **Granular Access Controls:** Implement a system of granular access controls that allows for fine-grained permissions on folders and files. This would enable the sales team to access only the specific promotional materials needed for their interactions with business partners, while restricting access to other sensitive documents.

- **Automated Access Revocation:** Utilize automated tools to revoke access to sensitive information after a specified period or when a project is completed. This would prevent lingering access that could lead to accidental data leaks.
- **Formal Review and Approval Process:** Establish a formal review and approval process for sharing materials with external partners. This process should include verification of the recipient's identity, the sensitivity of the information, and the purpose of sharing.

Justification:

These recommendations directly address the identified issues by:

- **Reducing the risk of oversharing:** Granular access controls ensure that employees can only access the specific information they need, minimizing the chance of accidentally sharing confidential data.
- **Preventing lingering access:** Automated access revocation ensures that permissions are promptly removed when they are no longer needed, reducing the risk of unauthorized access due to forgotten or neglected permissions.
- **Mitigating human error:** A formal review and approval process adds a layer of oversight and verification, reducing the likelihood of miscommunication or accidental disclosure of sensitive information.

By implementing these control enhancements, the company can significantly strengthen its data security posture and reduce the risk of future data leaks.