Data leak worksheet

By Jovworie Tanshi

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?* *Several factors contributed to the information leak:* 1. ***Excessive Access:*** *The sales manager granted broad access to the internal folder without restricting it to only the necessary files or individuals.* 2. ***Failure to Revoke Access:*** *After the meeting, the manager did not revoke access to the folder, leaving it accessible to team members.* 3. ***Miscommunication:*** *The sales team member was not adequately reminded or informed about the sensitivity of the folder's contents and the importance of sharing only the specific promotional materials.*

---

	4. ***Insufficient Training:*** *Lack of thorough training on data sharing protocols and the principle of least privilege for employees.* 5. ***Inadequate Monitoring:*** *There was no system in place to monitor or control the sharing of sensitive information in real-time.*
Review	*What does NIST SP 800-53: AC-6 address?* *NIST SP 800-53: AC-6 (Access Control) addresses the principle of least privilege, which involves:* 1. ***Access Authorization:*** *Ensuring that users are granted only the minimum access necessary to perform their job functions.* 2. ***Role-Based Access Control (RBAC):*** *Assigning permissions based on roles to ensure that users can only access information relevant to their duties.* 3. ***Separation of Duties:*** *Implementing controls to prevent conflicts of interest by dividing tasks and privileges among multiple users.* 4. ***Review and Adjustment:*** *Regularly reviewing and adjusting access controls to align with changes in roles, responsibilities, and requirements.* 5. ***Monitoring and Reporting:*** *Implementing mechanisms to monitor access and detect unauthorized or excessive access.*
Recommendation(s)	*How might the principle of least privilege be improved at the company?* *To improve the principle of least privilege at the company, the following recommendations can be made:* 1. ***Access Control Policies:*** *Implement strict access control policies that limit access to sensitive information based on job roles and responsibilities.*

	2. ***Automatic Revocation:*** *Use automated systems to revoke access to shared folders and documents after a predefined period or when no longer needed.* 3. ***Granular Permissions:*** *Set granular permissions to ensure that employees only have access to the specific files they need.* 4. ***Regular Audits:*** *Conduct regular audits of access permissions to ensure compliance with the principle of least privilege.* 5. ***Employee Training:*** *Provide regular training sessions on the importance of least privilege and secure data handling practices.* 6. ***Access Monitoring Tools:*** *Deploy tools to monitor and report on access patterns and detect any unauthorized or unusual access attempts.*
Justification	*How might these improvements address the issues?* ***Least Privilege: How might these improvements address the issues?*** 1. ***Access Control Policies:*** *By implementing strict policies, the company can ensure that only authorized personnel have access to sensitive information, reducing the risk of accidental leaks.* 2. ***Automatic Revocation:*** *Automatic revocation of access reduces the risk of outdated or unnecessary permissions lingering, which can be exploited or mistakenly used.* 3. ***Granular Permissions:*** *Granular permissions ensure that employees have access only to the information they need, minimizing exposure to sensitive data.* 4. ***Regular Audits:*** *Regular audits help identify and rectify any deviations from access control policies, maintaining adherence to the principle of least privilege.* 5. ***Employee Training:*** *Regular training raises awareness among employees about the importance of secure data handling and*

	reinforces the need to follow access control protocols. 6. ***Access Monitoring Tools:*** *Monitoring tools provide visibility into access patterns, allowing the company to detect and respond to unauthorized access attempts promptly, thereby preventing potential leaks.*