### **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?*  Factors contributing to the leak include a lack of access revocation after the meeting, the representative's oversight in sharing the incorrect link, and inadequate enforcement of the principle of least privilege regarding sensitive internal documents. |
| **Review** | *What does NIST SP 800-53: AC-6 address?* NIST SP 800-53: AC-6 addresses the enforcement of the least privilege principle, aiming to limit access and authorization to users based solely on what is required for them to perform their tasks. This minimizes the risk of unauthorized access or actions beyond a user's necessary scope. |
| **Recommendation(s)** | *How might the principle of least privilege be improved at the company?* To enhance the principle of least privilege, the company should implement role-based access control (RBAC) to restrict access to sensitive information based on user roles. Additionally, access to sensitive resources should be automatically revoked after a specified period or immediately after the necessity for such access has passed. Regular audits of user privileges and maintaining activity logs for provisioned user accounts can help track and manage access rights effectively. |
| **Justification** | *How might these improvements address the issues?* These improvements directly address the issues by ensuring that access to sensitive information is tightly controlled and monitored. Role-based access control ensures that employees have access only to the information necessary for their roles, reducing the risk of accidental or unauthorized sharing. Automatic revocation of access limits the window of opportunity for sensitive information to be leaked. Regular audits and activity logging provide oversight and accountability, enabling swift action to rectify any improper access rights and prevent potential data leaks. This structured approach to managing access privileges aligns with best practices for information security and privacy, bolstering the company's defenses against similar incidents in the future. |

### **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.

**Summarizing NIST SP 800-53: AC-6:**

NIST SP 800-53: AC-6 focuses on enforcing the principle of least privilege, ensuring that users are granted only the access necessary to perform their duties. This control is designed to limit the potential for unauthorized actions or access, reducing the risk of data breaches and leaks by preventing users from operating with more privileges than required for their tasks.

**Control Enhancement Recommendations:**

1. **Implement Role-Based Access Control (RBAC):** This system can dynamically adjust the access levels of employees based on their current roles and responsibilities, ensuring they have access only to the information necessary for their specific tasks at any given time.
2. **Automated Access Revocation:** Develop and integrate a system that automatically revokes access to sensitive documents or data after a specified period or immediately following the completion of a task that required such access. This system should be complemented by real-time monitoring to enforce access policies proactively.

**Justifying the Recommendations:**

Implementing RBAC addresses the core issue by ensuring that access to sensitive information is strictly need-based, significantly reducing the risk of accidental sharing of sensitive information. Automated access revocation further strengthens security by ensuring that temporary access does not become a permanent vulnerability. Together, these measures directly address the lapses highlighted by the incident, fostering a more secure and disciplined data handling environment that adheres closely to the principles of least privilege.