### **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)** | *The data leak occurred because access to the data was not restricted to the manager and the sales team. This allowed everyone with the link access to the shared folder. Access also wasn’t limited to specific promotional materials in the folder. The business partner should not have been given access to share the promotional information on their social media page.* | | |
| **Review** | *The NIST SP 800-53 : AC-6 addresses issues related to protections against data leaks by implementing the least privilege principle. This is a security control that ensures that users are only granted minimum permissions and authorisation to perform job duties and functions at a particular point in time. Those permissions must also be audited regularly to ensure the user still needsthem. They must be revoked after a while and only reinstated on need basis. It also involves keeping accurate logs of user actions.* | | |
| **Recommendation(s)** | *How might the principle of least privilege be improved at the company?*   * Restrict access to sensitive resources based on user role. * Automatically revoke access to information after a period of time. * Regularly audit user privileges. | | |
| **Justification** | *How might these improvements address the issues?*  *I believe that restricting access to sensitive resources based on role would have ensured that the link shared with the employees had an expiry date and time set which would have revoked the permissions they had. The link would definitely had expired at the time it was shared with the business partner. Moving forward, the company must ensure that links to shared folders or internal files are restricted to authorised users. Passwords and links with expiry dates must be used as an additional measure to prevent unauthorized users from accessing internal files. Also, security teams and managers must regularly audit access to files to help limit the exposure of sensitive or confidential information.* | | |

### **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.799\*/–\*\*\*----

### **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.