### **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?*  Customer success representative received access to a folder of internal documents from a manager. It contained files associated with a new product offering, including customer analytics and marketing materials. The manager forgot to unshare the folder. Later, the representative copied a link to the marketing materials to share with a business partner during a sales call. Instead, the representative shared a link to the entire folder. During the sales call, the business partner received the link to internal documents and posted it to their social media page.  *The manager should have revoked rights to everyone until it was clear that they could have access to the files. There should be more security and data protection for the data that got leaks.* |
| **Review** | *What does NIST SP 800-53: AC-6 address?*  *It address control enhancements such as authorize access to security functions, non-privileged access for nonsecurity functions, network access to privileged commands, separate processing domains, privileged accounts, review of user privileges*  *NIST SP 800-53: AC-6 addresses how an organization can protect their data privacy by implementing least privilege. It also suggests control enhancements to improve the effectiveness of least privilege.* |
| **Recommendation(s)** | *How might the principle of least privilege be improved at the company?*  *Increase security, protect data, and in the long run provide protection for the integrity of the business to it’s customers, business partners and employees.*   * *Restrict access to sensitive resources based on user role.* * *Regularly audit user privileges.* |
| **Justification** | *How might these improvements address the issues?*  *More control the data that is being shared.*  *Data leaks can be prevented if shared links to internal files are restricted to employees only. Also, requiring managers and security teams to regularly audit access to team files would help limit the exposure of sensitive information.* |

### **Security plan snapshot**

The NIST Cybersecurity Framework (CSF) uses a hierarchical. It is a 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. For more information on this guideline – see https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

### **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.