

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)	<i>Access to the internal folder was not limited to the sales team and the manager. The business partner should not have been permitted to share the promotional information on social media.</i>
Review	<i>NIST SP 800-53: AC-6 addresses how an organization can protect its data privacy by implementing least privilege. It also suggests control enhancements to improve the effectiveness of least privilege.</i>
Recommendation(s)	<ul style="list-style-type: none">● <i>Restrict access to sensitive resources based on user role.</i>● <i>Regularly audit user privileges.</i>
Justification	<i>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.</i>

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: <i>Data security</i>	PR.DS-5: <i>Protections against data leaks.</i>	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.