Issue(s):

The data leak occurred due to improper access management. The sales manager granted access to an internal folder without promptly revoking it after the meeting. A sales representative, unaware of the restricted nature of the documents, mistakenly shared the internal folder link instead of the intended promotional materials. The business partner then publicly posted the link.

Review (NIST SP 800-53: AC-6):

NIST SP 800-53 AC-6 defines the principle of least privilege, ensuring that users receive only the minimum access necessary to perform their tasks. This control prevents unauthorized actions by restricting access based on user roles and responsibilities. Control enhancements include time-based access restrictions and regular audits to minimize risks.

Recommendation(s):

1. **Implement automatic access revocation** – Configure access permissions to expire automatically after a predefined period or after a meeting concludes.

2. **Regularly audit user access logs** – Conduct periodic audits to ensure that access permissions align with business needs and that unnecessary access is revoked.

Justification:

Implementing automatic access revocation would prevent users from retaining access to sensitive folders beyond the necessary timeframe, reducing accidental leaks. Regular audits would help identify and remove excess permissions, ensuring that only authorized personnel maintain access to internal documents. These measures collectively strengthen information security and minimize human errors leading to data leaks.

Would you like me to refine this further or format it in a structured document? 🚀