Data Risk Assessment

Determining Appropriate Data Handling Practices

Wendy Alayon
01/07/2024 **@syszern**

Data Risk Assessment

Scenario

An educational technology company has developed an application for automated assignment grading, handling data from academic institutions, instructors, parents, and students. The company's team discovered a data leak of internal business plans on social media. An investigation revealed that an employee accidentally shared confidential documents with an external business partner. An audit is now underway to prevent similar incidents.

Information provided by a supervisor indicates that employees did not follow the principle of least privilege during a sales meeting. The task is to analyze the situation and propose preventive measures.

Firstly, the incident details will be evaluated to understand how confidential documents were shared during the sales meeting. Secondly, existing controls for preventing data leaks will be reviewed. This includes assessing access controls, data sharing policies, and employee training on data handling practices. Next, strategies to enhance information privacy within the company will be identified. Possible improvements may involve stricter access controls based on job roles, enhanced encryption protocols for sensitive documents, and reinforced data sharing policies through regular training.

Finally, the justification for these recommendations will focus on how they can strengthen data handling security. For instance, stricter access controls will limit sensitive information access to authorized personnel only. Enhanced encryption and reinforced policies will ensure data remains protected and accessible only to those who require it.

Wendy Alayon: **@syszern** Date: 01/07/2024

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)	*Access to the internal folder was not restricted solely to the sales team and manager, resulting in the unintended permission for the business partner to share promotional information on social media.*
Review	*NIST SP 800-53: AC-6 outlines methods for organizations to safeguard data privacy through the implementation of least privilege. Additionally, it recommends control enhancements to bolster the efficacy of least privilege measures.*
Recommendation(s)	• *Limit access to sensitive resources according to user roles.* • *Conduct regular audits of user privileges.*
Justification	*To prevent data leaks, restrict shared links to internal files exclusively to employees. Additionally, implementing regular audits of access to team files by managers and security teams would help minimize the exposure of sensitive 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.

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.