ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 3, pp: (18-20), Month: July - September 2021, Available at: www.researchpublish.com

BEST PRACTICES FOR A SUCCESSFUL DLP IMPLEMENTATION

Abdullah Tariq Al-Essa[1]

[1,2]Affiliation None

[1,2]Saudi Aramco, Dhahran, Saudi Arabia

Abstract: **A large amount of confidential data daily flows in and out of organizations to employees, customers, and partners. Unauthorized disclosure of this data creates a significant risk to the company, their customers, and their business partners, with the potential of negatively impacting their reputation, competitive advantage, and business relationships. The Data Loss Prevention (DLP) solution has been introduced to address this concern. The selection of a good DLP solution is important but technology selection is only one component of DLP. In this article, we will cover best practices that will combine technology, process, people to help you in implementing DLP in your organization successfully.**

Keywords: **Data Loss Prevention, Data Leakage Prevention, DLP, DLP Best Practices, DLP Strategy, DLP Guide.**

I. INTRODUCTION

More companies are looking for the protection of an organization's data from both outside threats as well as individuals within an organization that may compromise the data. Accordingly, many organizations use various investigative entities to identify and review data transfers that may violate one or more security policies.

Data loss prevention (DLP) is the practice of detecting and preventing confidential data from being "leaked" out of an organization's boundaries for unauthorized use.

Before diving into the technology and available vendor solutions, you should first build a good understanding of what your business requirements for DLP will be. Why you might need DLP, how you plan on using it, and the business processes around creating policies and managing incidents. The first step in any DLP implementation project is to determine which data would cause the biggest problem were it stolen. While it may seem obvious, data loss prevention should start with the most valuable or sensitive data that is most likely to be targeted by attackers

II. DETAILED DESCRIPTION

When initiating a DLP implementation project, there are several activities that must occur. Below is a framework and general guidelines that your DLP implementation should follow:

1. Project Sponsorship:

- Executive-level sponsorship is required to support DLP implementation.

2. Business Owners involvement:

- Involve key stakeholders (IT, HR, Finance, Legal and Internal Audit, etc.).
- Keep business leaders, stakeholders, and users informed of your plans and timelines.

3. Establish Goals:

- DLP implementation requires careful planning, including the development of clear and achievable goals, and the establishment of proper expectations among executives and business unit leaders.

4. Roles & Responsibilities:

- Build a responsibility assignment matrix (RACI), which details who is responsible, who is accountable, who needs to be consulted, and who is informed for each activity related to DLP implementation and support.

5. Identify Business Requirements:

- Before diving into the technology and available vendor solutions, you should first build a good understanding of what your business requirements for DLP will be.
- Understand your data and how it is used.
- Prioritize your data, Identify Sensitive data.
- Identify types of data to protect.
- Identifying Data Owners.

6. Define Security Requirements:

- After identifying your business requirements, next sketch out a set of security requirements to support them.

7. Conduct your own Research:

- Consult with research analysts such as Gartner, Forrester and gain a basic to intermediate understanding of the industry, the vendors and solutions available, and their particular strengths and weaknesses.

8. Review Architecture Options:

- Depending on what sensitive data you wish to protect, where it resides, and how it is accessed, the DLP solution that is a best fit for your business may include any one.
- Software-based DLP solutions
- Hardware-based DLP solutions

9. DLP Deployment Strategy:

- Use a phased approach. Deploy to highest risk areas of your business early on.
- Start slow. Begin by enabling monitoring only.

10. Data Classification:

- It's data classification first, and DLP second.
- Increase the accuracy and effectiveness of DLP.
- Create a document classification matrix. Identify where the existing data resides and how this data is classified. Classify the document according to risk.

11. DLP Governance Policy:

- Create Policy to establish governance around DLP.

12. Incident Management Process:

- Define the Incident Response Process.
- Trained Incident Response Team with clear defined roles, responsibilities, and procedures to drive consistency and organizational buy-in.

13. Have robust Awareness Program

- Awareness is a key to DLP implementation success.
- Begin user education to obtain employee buy-in.
- Users must understand the risk of data loss and the repercussions to their organization.
- Highlight Do’s and Don'ts.

III. CONCLUSION

DLP is an integral part of a mature security program. It's a powerful tool for protecting sensitive data which provides comprehensive data-centric security. The most critical element of successful DLP implementation is to understand that it is not a product that provides a quick fix. It is a process, and implementing it is just the beginning.

REFERENCES

[1] "Data Loss Prevention (DLP) Best Practices", https://www.mcafee.com/enterprise/en-us/security-awareness/data-protection/dlp-best-practices.html

[2] "The CISO's Guide to Data Loss Prevention: DLP Strategy Tips, Quick Wins, and Myths to Avoid", July 27, 2017, By Mike Pittenger, https://digitalguardian.com/blog/cisos-guide-data-loss-prevention-dlp-strategy-tips-quick-wins-and-myths-avoid

[3] "Understanding and Selecting a Data Loss Prevention Solution", SANS Institute and Securosis LLC sponsored by Websense, https://securosis.com/assets/library/publications/DLP-Whitepaper.pdf

[4] "What is Data Loss Prevention (DLP)? A definition of Data Loss Prevention", October 1st, 2020, By Juliana De Groot, https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

[5] "Maximizing the value of data protection program", June 2014, Ernst & Young, www.ey.com

[6] "EY_Data_Loss_Prevention - Insights on governance risk and compliance", October 2011, Ernst & Young, https://www.coursehero.com/file/16255515/EY-Data-Loss-Prevention/