7 Data Loss Prevention Best Practices & Strategies

By Michael Swanagan, CISSP

Published: 2024-02-24 · Archived: 2026-04-06 01:21:33 UTC

On average it takes organizations 191 days to identify data breaches.

If an organization lacks diligence in protecting the sensitive data it owns or is entrusted with, they are at risk of exposing sensitive data to those who are not authorized to observe or possess it.

The 7 best practices for data loss prevention include:

1. Identifying the crown jewels.
2. Researching multiple vendors.
3. Defining incident response and remediation.
4. Crawling, walking, and running.
5. Perform a proof of concept exercise.
6. Identifying the DLP stakeholders and support team.
7. Informing stakeholders of the state of the DLP program.

The strategy often used to counter and reduce the risk of data loss is referred to as Data Loss Prevention (DLP).

In this article, we will define DLP, describe how it works, briefly cover the top DLP software, and explain the best time to implement a DLP strategy.

By the end, you will have a deeper understanding of data loss prevention best practices and why DLP strategies are important to a successful cybersecurity program.

Free Security Policy Templates

Get a step ahead of your cybersecurity goals with our comprehensive templates.

Data Loss Prevention is defined as a strategy that detects potential data breaches or data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while *in use* (endpoint actions), *in-motion* (network traffic), and *at rest* (data storage).

Data Loss Prevention is also synonymous with the term Data Leakage Prevention. These terms are often used interchangeably, however, Data Loss Prevention is the common term used by DLP solution providers today.

Sensitive data is information that must be protected against unauthorized access to safeguard the privacy or security of an individual or organization.

It can exist within entries on a spreadsheet containing employee names and Social Security numbers.

Sensitive data may be the contents of a document describing the secret formula for a brand of soda, or it could be a database that contains the full names, addresses, and driver license numbers for a state's DMV.

One of the core functions of a DLP strategy and solution is to prevent exposing sensitive data to unauthorized parties.

Organizations today are faced with the challenge of selecting the best security solutions.

This includes implementing a SIEM and IDS/IPS to protect their corporate data.

This is because the unintentional leakage or loss of sensitive data due to a malicious actor, an inside job, or an unknowing employee, can lead to significant financial loss and reputational damage to any organization.

Data Loss Prevention Best Practices

1. Identify The Crown Jewels

Know thy business. Identify the proverbial ‘crown jewels’ of your company. This could be Intellectual Property such as a recipe, source code, or formula.

Engage Executive and Senior Leadership to direct the DLP program by providing input on what is critical to the organization.

This approach is referred to as the ‘top-down’ approach.

Input from technical leaders can be shared during the maturation of the DLP program to enhance value and creativity.

2. Research Multiple Vendors

Define your expectations for DLP in your organizations. Consult with peers in your industry and find out who they are using for DLP and gauge their satisfaction with support, incident workflow, and overall confidence level.

Gartner can also be used as a reference to determine how the DLP vendor has performed over time.

3. Define Incident Response And Remediation

Enterprise DLP is not simply a tool, it is a program. The downfall of many DLP installations is poor planning for incident triage.

It is not unusual for an organization to go through the strategy process, purchase the software, and fail to plan for DLP incident management.

Ensure there is an incident response plan and team in place before going live with the implementation.

4. Crawl, Walk, and Run

I recall working on my first deployment of Vontu/Symantec DLP. One of their sales engineers mentioned the phrase, do not boil the ocean right out of the gate.

He was advising us to go for small wins, instead of turning on every single policy checkbox available.

Doing so would overwhelm the system and inundate the system with massive amounts of incidents, therefore, defeating the purpose of the investment. Same principle applies a decade later.

Start with a small subset of policies and demonstrate value to leadership, then gradually build the system over time as your understanding of the product matures.

5. Perform A Proof Of Concept Exercise

The goal here is to replicate the functionality and test the feature sets.

This can also be compared to as a pilot. This is the time to kick the tires and ensure the product meets your compliance needs and observe deficiencies in your triage process.

6. Identify The DLP Stakeholders And Support Team

I t is not surprising to hear many organizations have DLP in the environment and barely utilize the features or have support teams to manage incidents.

Create an internal DLP Committee, comprised of Senior Leaders, Business Unit Managers, Legal, and InfoSec Management.

If internal resources are not available to support DLP Operations, consider partnering with a Managed Service Provider that specializes in DLP.

7. Regularly Inform Stakeholders Of The State Of The DLP Program

Ensure stakeholders are informed of the state of the program.

Consider creating a DLP committee comprised of Executive Leadership members and key Business Unit leaders.

Monthly or quarterly meetings will provide input and will help to continuously drive the program and ensure the quality of the investment is operating optimally.

A DLP strategy can commence once executive leadership is on board with the solution. This usually takes place after a vulnerability assessment or cost-benefit analysis has been performed.

The DLP strategy will provide direction on how to implement the solution and outline what, where, and how to protect the data.

I'll list a few real-world scenarios to bring the strategy process into focus.

Scenario A

A fictional company named MediHealthRecords processes medical insurance claims for a regulated Health Care organization.

They are aware that HIPAA and Medical claim data reside on file servers, but they are not sure where the data is located.

Solution: Implement A DLP At Rest Solution

Here the best choice would be to implement a DLP at Rest solution. The strategy would include a discovery scan of unstructured data, which will crawl the selected storage and locate data matching the pattern of HIPAA and Medical keywords, as set forth in the scan policy.

When a pattern match occurs, a notification alert will be recorded in the DLP database and viewable on the management console by the DLP Analyst.

Scenario B

The Human Resources manager has learned that a few members of the HR department have been emailing sensitive files to their personal Gmail accounts to work on backlogged HR requests over the weekend.

Solution: Implement DLP For Network And Endpoints

A couple of options can be employed. A network security policy can be created to prevent file uploads to Gmail.

The component utilized to enforce this would be data in motion or DLP for the network.

DLP for Endpoint can also detect HTTP/HTTPS, which can be done with advanced application configuration. File upload data can detect the content as it leaves the endpoint to the Internet.

Scenario C

The Sales team is complaining that they cannot store their PowerPoint presentations on USB thumb drives. There isn't any sensitive data saved, only presentation.

Solution: Implement DLP For Endpoints

The best strategy that fits this scenario is to provide an exception for the Sales team members.

DLP for the Endpoint in most cases allows the ability to whitelist users via a policy based on Active Directory membership.

Scenario D

The CEO would like to know when the secret formula document has moved from its original location or emailed within network.

Solution: Create A DLP Policy

When researching a DLP vendor, ensure that they can demonstrate any scenario involving the protection of your Intellectual Property.

Create a policy that detects the exact match of the document or monitor for specific keywords as it resides in storage or email.

As stated, the examples listed above are real world scenarios that organization's face every day in the corporate world.

By developing a strategy, an organization can assess which DLP component is applicable to their environment.

It would not be a wise investment to purchase an expensive Enterprise DLP solution that offers an entire suite of DLP features if your organization doesn't manage unstructured data on-premise or in the cloud.

The cost of implementing a DLP platform can be expensive.

Be sure the capital investment is based on sound cost-benefit analysis, risk assessment, and vendor analysis.
