This article focuses on common pitfalls when implementing a DLP solution to secure your organizational information assets. The article also lists out our practical insights; lessons learnt and recommended process to achieve an effective and efficient DLP implementation.
## Document Tracker

<table>
<thead>
<tr>
<th>Author</th>
<th>Version</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manasdeep</td>
<td>August 2012</td>
<td>Document Created</td>
</tr>
</tbody>
</table>
NOTICE

This document contains information which is the intellectual property of Network Intelligence. This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of Network Intelligence.

Nothing in this document constitutes a guaranty, warranty, or license, expressed or implied. Network Intelligence disclaims all liability for all such guaranties, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non infringement of intellectual property or other rights of any third party or of Network Intelligence; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of Network Intelligence.

Network Intelligence retains the right to make changes to this document at any time without notice. Network Intelligence makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Copyright
Copyright. Network Intelligence (India) Pvt. Ltd. All rights reserved. NII Consulting, AuditPro, Firesec, NX27K is a registered trademark of Network Intelligence India Pvt. Ltd.

Trademarks
Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

NII CONTACT DETAILS

Network Intelligence India Pvt. Ltd.
204 Ecospace, Old Nagardas Road, Near Andheri Subway, Andheri (E),
Mumbai 400 069, India
Tel: +91-22-2839-2628
    +91-22-4005-2628
Fax: +91-22-2837-5454
Email: info@niiconsulting.com
Contents

1. **Introduction** 5
   **What is DLP?** [1] 5

2. **Data Loss vs. Data Leakage** 5
   a. Types of DLP systems: 5

3. **Generic Data Leakage Prevention** 6
   a. Deploy Security Mechanisms 6
   b. Advanced security measures 6

4. **DLP Solutions** 7
   a. Mechanisms for classifying sensitive information: 7
   b. Popular DLP Solution Vendors: 7

5. **Categories of DLP** [1] 7
   a. Network DLP (aka Data in Motion) 7
   b. Storage DLP (aka Data at Rest) 7
   c. Endpoint DLP (aka Data in Use) 7

6. **Data Identification** [1] 8

7. **Preparing for DLP Implementation** [2] 8

8. **DLP Implementation Challenges** 8
   a. Other implementation challenges: 8

9. **References** 9
1. INTRODUCTION

Data Leakage is an important concern for the business organizations in this increasingly networked world these days. Unauthorized disclosure may have serious consequences for an organization in both long term and short term. Risks include losing clients and stakeholder confidence, tarnishing of brand image, landing in unwanted lawsuits, and overall losing goodwill and market share in the industry. To prevent from all these unwanted and unpleasant activities from happening, an organized effort is needed to control the information flow inside and outside the organization. Here is our attempt to demystify the jargon surrounding the DLP procedures which will help you to choose and apply the best suitable option for your own business.

What is DLP? [1]

Data Leakage Prevention is the category of solutions which help an organization to apply controls for preventing the unwanted accidental or malicious leakage of sensitive information to unauthorized entities in or outside the organization. Here sensitive information may refer to organization’s internal process documents, strategic business plans, intellectual property, financial statements, security policies, network diagrams, blueprints etc.

2. DATA LOSS VS. DATA LEAKAGE

Data Loss pertains to actual "loss" of information with no trace present in original site while data leakage pertains to the disclosure of information with originating site left unmodified.

a. Types of DLP systems:
   - Information Leak Detection and Prevention (IDLP)
   - Information Leak Prevention (ILP)
   - Content Monitoring and Filtering (CMF)
   - Information Protection and Control (IPC),
   - Extrusion Prevention System (EPS)
3. Generic Data Leakage Prevention

a. Deploy Security Mechanisms
To protect against inside and outside attacks we can deploy common security mechanisms, such as firewalls, intrusion detection systems (IDSs), and antivirus software. A better design is always to place these security mechanisms at appropriate places in the corporate network so that it becomes increasingly "hard" for the attacker to breach the corporate network. A "design in depth" strategy can be helpful to protect the most valuable and business critical assets of the organization. Within the organization, using thin-client architecture (with no sensitive data stored on client machine) can also reduce the data leakage to a great extent.

b. Advanced security measures
We can install behaviour and pattern based monitoring tools to detect and stop the malicious activities before they happen. Care has to be taken that very less false positive alerts are generated and specific log trails with timestamps are recorded all the time on the monitoring server. These security mechanisms rely on reasoning algorithm to learn and subsequently detect abnormal data access, suspicious mail exchange etc.

A good practice would be to set them in conjunction with honeypots for detecting malicious intent of the individual by gathering as much information about his activities to rule out any possibility of "false positives". This with combination of log trails can effectively single out the adversary and can help in formation of a strong case in legal proceedings if needed.

c. Access control and encryption
Device control, access control, and encryption are the basic means by which sensitive information can be protected from malicious outsider and insider attacks. Good practices must include proper log maintenance on every access attempt, and "strong" encryption done for "business critical" data. Encryption keys must be stored in secure separate places.
4. DLP SOLUTIONS

Designated DLP solutions detect and prevent unauthorized attempts to copy or send sensitive data, intentionally or unintentionally, by authorized personnel who have access to the sensitive information.

a. Mechanisms for classifying sensitive information:
   - Exact data matching,
   - Data fingerprinting,
   - Statistical methods,
   - Rule and regular expression matching,
   - Lexicons,
   - Conceptual definitions, and
   - Keywords

b. Popular DLP Solution Vendors:
   - Websense
   - McAfee
   - RSA
   - Symantec
   - Trend Micro
   - MyDLP (Open-source)

5. CATEGORIES OF DLP[1]

a. Network DLP (aka Data in Motion)
   A software or hardware solution that is installed at the end points near network perimeter. It analyzes network traffic to detect sensitive data that is being sent in violation of information security policies.

b. Storage DLP (aka Data at Rest)
   This usually involves a mechanism (agent or agent-less) to prevent unauthorized access to the data stored on your hard drive and/or USB sticks. Data at Rest must be regularly checked with data retention policies of the organization and compliance procedures as it might have increased probability to be leaked out. Phased-out data must be securely disposed such that data forensic techniques can’t recover back the deleted data.

c. Endpoint DLP (aka Data in Use)
   Such systems run on end-user workstations or servers in the organization. They are used to control information flow between groups or types of users. They prevent conflict-of-interest between 2 or more group of users within the organization also. They control email and IM communications before being stored in the corporate archive. These systems have the advantage that they can provide application controls to block attempted transmissions of confidential information from physical devices with spontaneous user feedback. Disadvantage is that they need to be installed on every workstation in the network, and can’t be used on mobile devices.
6. Data Identification[1]
Here, DLP techniques are used to identify sensitive data (in motion, at rest, or in use). Care has to be taken to ensure the accuracy of the DLP technology is high enough to ensure lower rates of false-positive reporting. Heavy testing must be done to ensure that data reported can be well relied upon.

They are of 2 methods:
- **Precise**: Methods which can pinpoint and report almost zero false positives
- **Imprecise**: Comprise of keywords, lexicons, regular expressions, Meta tags, Bayesian analysis, statistical analysis etc. All have greater chances of false positive reporting.

7. Preparing for DLP Implementation[2]
So, you are all geared up and ready for DLP implementation. But before doing that you must ensure to do your homework with either your IT team with steering committee or seek professional help for doing the following:
- Identify all organization's assets. Mark their critical value and its impact to business.
- Evaluate the risk of the critical and sensitive data both in qualitative and quantitative terms.
- Evaluate possible data leakage avenues.
- Decide how this data should be protected and how those avenues can be plugged.
- Agree upon a cost effective DLP solution as per your requirement and team's analysis

8. DLP Implementation Challenges
User resistance for change is the most difficult obstacle which has to be handled with greatest care. Training workshops and seminars must be held on regular basis to infuse confidence in them for adopting DLP procedures. The effectiveness of DLP solution must be closely monitored to iron out any issues if they arise during implementation. Recommended review duration is 3-6 months.

Likewise, over-optimism also needs to be checked upon as people tend to get carried away and get over dependent on the DLP technology. Policy and procedure framework must be properly documented and accordingly implemented.

a. Other implementation challenges:
- Under-estimation of the time and effort involved
- Lack of trained resources
- Perception that ownership resides with IT
- Underestimation of the expense (TCO) involved
- False positives
- Ignoring the legal & regulatory framework
9. REFERENCES