Data Loss Prevention (DLP) is the process and methodology to detect and prevent the unauthorized transmission or disclosure of sensitive information. At the heart of DLP is a combination of people, processes, and technology. Together, these elements work to help ensure data is utilized in its intended manner.

Implementing a comprehensive DLP program is essential for reducing the risk of exposure of sensitive information. Organizations cannot risk the harmful implications due to loss of data or to suffer the penalties from a regulatory requirement violation. But in today’s business environment, the increased volume of data makes it challenging to efficiently manage new or existing data. Nevertheless, it is a problem that all organizations need to address.

Although some of the DLP processes and procedures may appear to be redundant to existing security safeguards, creating a separate program can actually strengthen existing security controls and initiate new methods for detecting data leakage. As part of Foundstone’s solution, consultants will conduct an assessment addressing the following eight elements:

1. Data Governance
2. Risk Assessment
3. Regulatory and Privacy Requirements
4. Data Classification
5. Policies, Standards, Procedures
6. Data Discovery
7. Remediation Processes
8. Training and Awareness

**Data Governance**

Data Governance (DG) encompasses the overall management of the confidentiality, integrity and availability of data within an enterprise. The detailed components of DG can be difficult to define because it is a new concept and it is still evolving. From a security standpoint, DG is the act of protecting data and monitoring the flow of where the data travels. Although this may sound overly simplified, this can be a challenging task within a large organization.

Foundstone DG service consists of the following:

- Develop a DG structure
- Define DG roles and responsibilities

**Risk Assessment**

Conducting a Risk Assessment (RA) is a good second step in any DLP program. The main purpose for a RA is to identify all types of data within your network and to identify threats and vulnerabilities related to this data.

Foundstone’s DLP Risk Assessment service consists of the following:

- Risk identification and analysis
- Strategy development
- Strategy implementation

**Regulatory and Privacy Requirements**

A key step in a DLP program is to identify regulatory and privacy requirements. These may include, but are not limited to:

- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability & Accountability Act (HIPAA)
- Payment Card Industry Data Security Standards (PCI DSS)
- Sarbanes-Oxley Act

Having a strong understanding of what requirements apply to your organization and what types of security controls are required need to be identified.

Foundstone’s Regulatory and Privacy service consists of the following:

- Regulatory and privacy requirement identification
- Requirement analysis
- Requirements and data mapping

**Benefits**

- **Prevent Data Leakage** - Prevent accidental or malicious loss of data by insiders or hackers, even when data is disguised.
- **Reduce Cost of Investigation and Reputation** - A DLP program can help reduce costs in investigating data loss and it can help reduce the expenses in rebuild losses due to reputation damage.
- **Facilitate Early Risk Detection and Mitigation** - Implementing a DLP program will help identify data leakage and will help ensure information is in its proper place.
- **Increase comfort level with senior management** - Implementing DLP controls will help assure senior management that proper security safeguards have been implemented, allowing them to concentrate on other critical business issues.

**Related Foundstone Services**

- Data Loss Prevention Assessment
- Risk Assessment
- Policy and Procedure Development
Data Classification
Data Classification is the process of classifying information data according to its value and sensitivity to the organization. It provides the proper prioritization of an organization’s assets and resources, which will result in the appropriate level of controls being applied to each system accordingly.

Foundstone’s Data Classification service consists of the following:

- Develop a standard or policy for data classification
- Identify data-type by departments
- Identify administrator/custodian/users for each data-type
- Identify systems maintaining, processing, or storing each data-type
- Specify the criteria of how the data will be classified and labeled

The data classification program will add additional controls to limit the access and movement of sensitive data, thus reducing the amount of data that is leaked within the organization.

Policies, Standards, Procedures
Sound policies, standards, and procedures are fundamental to an effective DLP strategy. They ensure that the organization’s data is protected at a level appropriate to its value. It is not only critical to create sound policies, standards and procedures, but it’s equally important to ensure that they are updated on a regular basis.

Foundstone’s DLP Policies, Standards, and Procedures service consists of the following:

- Policies, standards, and procedures collection
- Policies, standards, and procedures gap analysis
- Policies, standards, and procedures document development

Data Discovery
Regardless of the amount of security controls implemented, the chances of intellectual property leaking out are highly likely. This is why a data discovery assessment needs to be conducted on a periodic basis. A data discovery assessment highly depends on a tool, with the capability of either monitoring the organization’s networks, or with the capability to scan data files on systems, or both.

Foundstone’s Data Discovery service consists of the following:

- Query definition development
- Network discovery capture (data-in-transit)
- System data discovery capture (data-at-rest)
- Data analysis

Data discovery is one of the key elements of a DLP program. Obtaining a strong tool and knowledgeable staff can limit most organizations from implementing a solid DLP program.

Remediation Processes
A major challenge with DLP programs is determining which data is valid leaked data and which data is a false positive detection. In today’s business environment, the amount of data traveling through the network and stored on disk drive can be overwhelming. Nevertheless, the challenge needs to be managed and processes need to be in place beforehand. Should a violation be discovered, proper methodologies can be implemented and the cause of the breach accurately determined.

Foundstone Remediation Process service consists of the following:

- System data cleanup
- Event investigations
- Security control implementation

Training and Awareness
It is important for an effective DLP solution to interact with the organization’s employees so that they have a strong understanding why certain activities are inappropriate and could be harmful for the organization.

Foundstone Training and Awareness service consists of the following:

- DLP Training and Awareness for All Employees
- DLP Training and Awareness for Security Practitioners
- DLP Training and Awareness for Executive Staff

The Foundstone Difference
All Foundstone projects are managed using Foundstone’s proven Security Engagement Process (SEP) for project management. This process ensures continual communication with your organization to ensure the success of all Foundstone consulting engagements.