Data Loss Prevention Program

Safeguarding Intellectual Property

Author:

Powell Hamilton
Senior Managing Consultant
Foundstone Professional Services
Data Loss Prevention Program: Safeguarding Intellectual Property

One of the major challenges for today’s IT security professional is having a strong awareness of the type of data and value of the data that they are responsible for protecting. No matter how robust their technology is, or how vigorous the monitoring systems are, data and/or Intellectual Property (IP) can find a way to leak out (i.e., data leakage) onto less secure systems and devices for which they are not intended.

What is Data Leakage?

The concept of data leakage is simple. Data leakage is the separation of IP from its intended place of storage. Most of the time, the data’s originally intended place of storage has stronger security controls than the place the IP ends up.

Data leakage can occur in many ways. The most common method is for an employee to violate corporate policy and copy the IP to a less secure system or their personal computer or removable device. Other methods include human error, technology mishaps, system misconfiguration, disgruntled employee, or, possibly, a system breach from a hacker.

Although data leakage can occur in many ways, the end result can be devastating to an organization and/or to the owner of the information.

Common Sources of Data Leakage

There are many reasons why data leakage occurs. Some leakage may be intentional and others may be from human error or a system misconfiguration. The following outlines some common examples of data leakage:

- **An employee needs to create a report.** The employee extracts the data from a secure system and conducts the analysis on a less secure system, such as their desktop or notebook device. After the analysis has been complete, the employee does not properly dispose the information.

- **A disgruntled employee with privileged access to sensitive information acts maliciously and steals information.** The information is copied to a non-secure system or device (such as a memory stick).

- **A new or upgraded application is being implemented on a test system.** Personal Identifiable Information (PII) is used to ensure the system is working properly. After the tests are completed, the PII is not removed or disposed.

- **Processes for conducting secure backups are not established.** The backup tapes are stored in a non-secure environment and a curious intruder removes the tape to examine the content.

- **Outdated hardware is donated to a local school.** Before the system is delivered, the hard drive is not properly cleaned and sensitive information is not removed.
• A home-grown application is developed to interface to the public. The application developer lacks secure coding experience and writes the program with leakage errors. These types of applications can provide a malicious hacker with unauthorized access to sensitive data.

• Improper configuration settings or inadequate security controls for shared drives can increase risk of exposure. Incorrect setting of permissions of the file and directory structure could allow anyone to access the information. The organization has a loosely guarded policy towards its propriety information, whereby data becomes easily accessible to everyone.

Although it is common for data leakage incidents to occur internally, it is also common for data to leak due to hackers, social engineering, phishing attacks and even dumpster diving. These attacks can spread sensitive information from system to system.

What is Data Loss Prevention?

Data Loss Prevention (DLP) is the process and methodologies to detect and prevent the unauthorized transmission or disclosure of sensitive information. DLP depends on a combination of people, processes, and technology as its strategic control foundation. These control elements work together to help ensure data is utilized in its intended manner.

Components of a Data Loss Prevention Program

The potential legal liability and damage to brand-reputation from exposure of sensitive data has encouraged security leaders to implement a DLP program. A DLP program can be constructed in many ways. The following diagram illustrates a unique model:
Most DLP solutions solely rely on technology. Although technology is an important aspect, it also takes people and process to build a holistic DLP program.

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 label 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.

A sound DG program includes a governing body or a committee to define policies and procedures and a plan to implement those procedures. In a large organization, this group needs to consist of individuals who have a strong understanding of the organization’s industry, business objectives, internal processes, and the corporate culture.

This group is not responsible for managing data directly, but is responsible for creating the rules (policies) and the methods (procedures) for storing, accessing, and handling data. Along with creating policies and procedures, the group needs to define the responsibilities of the owners and/or custodians of the data and outline the accountability for the data, specifically how the data is processed, stored, archived, and transmitted internally and externally.
**Risk Assessment**

Conducting a risk assessment is a good first step in any DLP program. The main purpose for a Risk Assessment is to identify all types of data within your network and to identify threats and vulnerabilities related to this data. Non-Public Data (financial, business, HR, legal, and regulatory data), Personally Identifiable Information (social security numbers, credit card information, personal health data), and Intellectual Property (patents, trademarks, design plans) are examples of data that need to be identified. Once this information has been identified, a flow analysis needs to be conducted to identify all systems and devices the data either resides on or flows through. For example, the HR department may utilize employee information. This information is stored on a centralized server utilizing a second server with a proprietary database. To access this information, the HR employee connects their intranet web browser to the server (i.e., three-tier architecture). In this simple scenario, the devices transferring and storing data are the employee’s desktop workstation, network components connecting to the server, the server itself, and a separate server maintaining the proprietary database. Each of these systems needs to be evaluated to determine threats and vulnerabilities that may put the data at risk.

This exercise needs to be conducted for all types of data being utilized within the organization. A comprehensive DLP solution ultimately has to protect all potential risk points in your organization.

**Regulatory and Privacy Requirements**

One key step in a DLP program is to identify regulatory requirements. Having a strong understanding of what regulatory requirements apply to your organization and what types of security controls are required, need to be identified. Most organizations do not have a strong understanding of their requirements, or their interpretations of those requirements are different from the regulators. Thus, most organizations are operating in a non-compliance mode.

Identifying regulatory requirements supports the prioritization security resources-to-system containing, processing, and/or transmitting the sensitive information. This also helps to focus the scope of security controls.

Identifying privacy requirements is essential for an organization to ensure that the goals and promises of privacy and confidentiality are supported by its practices, thereby protecting confidential information from abuse and the organization from liability and public relations problems. Although there are some federal and state regulatory requirements, most organizations maintain privacy policies and procedures to satisfy the comfort levels of their customers.

A successful DLP program needs to conduct a privacy assessment to ensure that data is protected based on the organization’s policies. If policies are not being followed or are not enforced, sensitive information is bound to leak out.
**Data Classification**

Data Classification is the process of classifying information data according to its value and sensitivity to the organization. Data classification provides the proper prioritization of an organization’s assets and resources, which will result in the appropriate level of controls be applied to each system accordingly.

Data should be categorized in terms of criticality within an organization’s environment (i.e., public, confidential, secret, and private, etc.). Business requirements should drive the classification process and should be directly related to data classes.

Once data requirements have been established and intellectual property has been identified, classification categories can be assigned. A typical data classification program should include 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
- Create an enterprise awareness program

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

**Policies, Standards, Procedures**

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

Within the realm of DLP, *policies* are the starting point before a company can establish standards and procedures, which allow an organization’s DLP solution to operate more securely and efficiently. *Standards* are mandatory activities, actions, rules, and regulations designed to provide the DLP policies with the support, structure, and specific direction required to be meaningful and effective. *Procedures* spell out the specifics of how the DLP policies and the supportive standards will actually be implemented in an operating environment.

**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...
Data Loss Prevention Program: Safeguarding Intellectual Property

Networks, or with the capability to scan data files on systems, or both. Although this task is dependent on a discovery tool, there are several commercial and non-commercial products available.

Data discovery is one of the key elements of a DLP program. Access to a strong discovery 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 drives is almost overwhelming. Nevertheless, the challenge needs to be managed and processes need to be in place beforehand. Should a violation be discovered, proper methodology can be implemented and the cause of the breach accurately determined.

After a violation has occurred, an investigation needs to be launched to determine if a corporate policy has been violated. To accomplish this objective without disrupting the work environment, processes and procedures need to be in place to effectively remediate the issue. A strong resolution process needs to be automated, efficient, and timely to manage and resolve the issue before the organization is harmed.

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. Not all violations are conducted with a harmful intent. An employee may want to work at home and email sensitive data to their personal, less secure public account. Although the intent is good, the action is not. Ongoing education will help reinforce correct behavior and provide the employee with guidance on how to correctly handle sensitive data.

When organizations educate and highlight the dangers of data loss, violations are reduced dramatically. Over time, as the employees become more familiar with corporate policy, the overall security awareness practices increase throughout the organization.

The Benefits of a Data Loss Prevention Program

The following illustrates some of the benefits for creating a Data Loss Prevention Program:

- **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.** Reducing costs in investigating data loss can also reduce the cost of rebuilding damage to an organization’s reputation.
Data Loss Prevention Program: Safeguarding Intellectual Property

• **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.

**Conclusion**

Implementing a comprehensive DLP program is essential for today’s working environment. Organizations cannot risk the harmful implications due to loss of data or to suffer the penalties from a regulatory requirement violation. In today’s business environment, the increased volume of data is such that it is a challenge to efficiently manage new or existing data. Nevertheless, it is a problem that all organizations need to address.

**About Foundstone Professional Services**

*Foundstone® Professional Services, a division of McAfee. Inc., offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, Foundstone identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company’s professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military.*