ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Loss of Data Control Scenarios and Best Data Loss Prevention (DLP) Practices

Prashanth Kodurupati

Information Technology, Managed File Transfer Engineer, PragmaEdge LLC, Alpharetta, USA

ABSTRACT

Humans (employees in an organizational context) still remain the weakest link in cybersecurity and data loss. Employees can become a data vulnerability for an organization in a number of ways, i.e., copying data on physical media that can be lost or maliciously used, using the internet to intentionally send sensitive data to the wrong entities, unintentionally letting malware in or sending company data to malicious individuals/entities, and a number of other scenarios. Good Data Loss Prevention (DLP) practices like strict device use policies and access control can mitigate (if not eliminate) these security vulnerabilities.

***Corresponding author**

Prashanth Kodurupati, Information Technology, Managed File Transfer Engineer, PragmaEdge LLC, Alpharetta, USA.

Received: July 14, 2022; **Accepted:** July 20, 2022; **Published:** July 27, 2022

Keywords: DLP, Data Control

Introduction

Humans are responsible for the bulk of data leaks and breaches from company servers, with technical vulnerabilities making up only a small fraction of the total data leak incidents. The financial losses from these data breaches and penalties can easily rise to millions of dollars, and reputation and business damages can be significantly more protracted and adverse in nature. Data controls are in place in most organizations to eliminate or at least drastically reduce the possibility of employees intentionally or unintentionally copying and leaking sensitive data outside the company fold, and data loss prevention (DLP) techniques and practices can serve as the most significant line defense in this regard.

Literature Review

Data loss and leaks have been a focal point of academic research since the early days of computers, though both the problem and its solutions have experienced a significant expansion in scope thanks to the internet. Numerous dimensions for data loss in transit and at rest, as well as the impact it can have on a business, have been identified in the literature, including but not limited to litigation, loss of customer confidence, and loss of competitive advantage [1]. Employees, i.e., the human element, have been identified as one of the most significant sources of data loss/leaks and can be enhanced in case of disgruntled employees when it's intentional, but it can also be unintentional [2]. Data Loss Prevention (DLP) emerged as a group of practices, techniques, and technologies with the sole aim of reducing or eliminating data loss from organizations, but it's also extended to keeping track of all data leaks, which may aid in recovery or at least, litigation against intentional data leaks [3]. DLP solutions, systems, and frameworks focus on both intentional and unintentional data leaks as well as on different dimensions of data leaks, including organizational parameters (both digital and physical) and end-points that connect to the company data points [4]. In addition to tangible protective measures and safety layers, employee education is also critical to preventing organizational data loss [5].

Problem Statement: Unauthorized Access and Data Loss

Different businesses have different data vulnerabilities and attack surfaces (for intentional data loss). The stakeholders associated with these vulnerabilities may be both internal (employees) and external. However, for these problem statements, we will focus solely on internal data vulnerabilities, i.e., employee-related ones.

Physical Media

Employees of a business may be allowed to connect their work computers and devices with other physical media, like a hard drive, USB flash drive, or their personal phones. The permissions may vary among positions, and the types of files employees have access to, but in most cases, businesses either do not strictly control these permissions or have to grant them for smooth operations. This opens the organization up to both intentional and unintentional data loss scenarios. An example of an intentional data loss would be an employee who is about to be fired for copying critical customer information to poach or sell to a competitor. Unintentional data loss would be an employee losing his or her flash drive with the quarterly financials somewhere, and the drive falls into the wrong hands.

Online Connectivity

Nowadays, the internet is the lifeblood of most organizations, and there are very few cases where sensitive data is kept in air-gapped drives/systems. Most devices are connected to the internet, albeit with different levels of control. Some organizations have strict controls over what data can be sent out of the company servers and what can be accepted, while other work computers have virtually no restrictions. This allows employees to transfer data from work computers to home computers and devices, keep a copy of the work documents in their personal drives, use online tools (personal) to work on company data and keep copies of the work there, and several other scenarios where employees may have access to sensitive and potentially dangerous company data. Online connectivity can also lead to unintentional data leaks and losses. For example, an outgoing email with sensitive information where you copy the wrong individuals (like clients on vendor emails or vendors on client emails). These vulnerabilities and data loss problems may lead to getting significantly enhanced with the culture of Bring Your Own Device (BYOD) to work, especially if it's not regulated through the right cybersecurity approach.

Security Vulnerabilities

Then, there are security vulnerabilities in each system in both online and offline conditions. Employees who are allowed to receive emails from vendors and other outsider elements may become a phishing target or a social-engineering attack target. Similarly, employees handing over their work devices or personal devices with work data for repairs to unknown and unvetted vendors may become the source of data loss.

Academic Review of Key Challenges and Proposed Solutions

Research	Challenge	Solution
Karen Leung (2009)	Employees are allowed to copy company files and data on personally owned physical media.	Strict control over which employees can connect physical media to company devices and employee education.
Larry G. Wlosinski (2018)	Several data vulnerabilities stem from online connectivity and data transmission.	Comprehensive DLP planning and implementation.
Lior Arbel (2015)	Unauthorized access - Many employees have access to a wide range of data, most of which is irrelevant to their day-to-day operations, but the access makes them vulnerable to security.	Strict access control is based on the role of the employee, their position in the department, or any projects they might be working on.
David F. Perri and Erinmichelle D. Perri (2018)	Employees can be targeted for intentional data leaks and inducing data losses from an organization.	Employee education.
Gabriel Lopez et. al. (2015)	Comprehension of the full attack surface and data vulnerabilities of an organization and choosing the appropriate DLP solutions and framework.	Comprehensive DLP evaluation framework to identify the perfect match for organizational needs.

Proposed and Implemented Solutions: Best Data Loss Prevention (DLP) Practices

All the proposed and implemented solutions pertain to the best DLP development and integration practices.

Strict Control Over Physical Media Connectivity

Organizations should implement comprehensive controls over which external physical devices can be connected to company hardware and company devices and company servers and who is authorized to make these connections and copy the files to and from company systems. There are several ways to do that. One is a blanket ban on physical media connectivity on company devices, and employees have to ask for access when they need to copy something from company devices. But there are other uses as well. Like device whitelisting, where some devices are able to connect to company systems (like mouse, keyboard, etc.) while others are not (USB flash drive, external hard drive, etc.).

Access Control

Access control prevents who can do what with the data they have access to and who has access to certain data segments. For example, general employees do not have access to the company's financial data, while financial department employees may not have access to the client data a department and its employees are working with. Separating access by operational domains is a good DLP practice and ensures that employees only have access to data necessary to their work, reducing the points of vulnerabilities.

Organizations can also control what employees can do with the data. For example, a simple control setting may prevent employees from copying company data to their personal accounts or, better yet, prevent employees from opening personal or unauthorized online accounts on company computers (like cloud drives). Similarly, the sensitive files can be kept and transferred in an encrypted form, so even if they are copied outside an organization's IT ecosystem, they would not be considered a data loss because no data could be salvaged from them in their encrypted state. One prerequisite to establishing healthy access control is classifying both data and employees based on sensitivity and access levels.

Real-Time Tracking of Unauthorized Data Transfers

Even with a wide range of DLP systems in place, it's not possible to plug all the holes from which organizational data can leak. Also, in some cases, permissions have to be granted to employees who may not have access to certain files, not just to access them but to copy them to an external media or upload them online. In these scenarios, tracking both authorized and unauthorized data transfers can be critical.

Firstly, it helps FTP and the organization as a whole gain visibility to all the data transfers taking place within the organizational fold, so even if a loss does happen, it's easier to track the culprit, which may help mitigate the situation to an extent. Secondly, it can alert the individuals responsible for company data and transfers whenever an unauthorized transfer is taking place or if it's requested. They can then reach out to the individual or their managers or supervisors to determine whether the attempt was made with their permission. If not, it might be considered a malicious act (if done intentionally) or a vulnerability.

Employee Education

Employee education essentially complements all the other DLP measures and can go a long way in preventing employees from unintentionally losing their data or falling victim to cyber-attacks. This is especially useful for employees who may have access to sensitive data or have a higher level of access when it comes to handling company data, including sending it to outside stakeholders.

Use Cases

Employee-Related Data Vulnerability Dimension	Commonly Implemented DLP Solutions	Use Case
Physical Media Connectivity	Strict Control (Blanket Ban) Device Whitelisting	* Organizations with highly sensitive data (e.g., healthcare, finance) * Environments with minimal need for external device usage
	Data Encryption	* Employees who need to transfer data occasionally (e.g., presentations)
Online Connectivity	Access Control Data Encryption Secure File Transfer Applications	* Limiting access to sensitive data based on job roles * Preventing unauthorized data uploads to personal cloud storage * Securely transferring large files to external collaborators
	Web Filtering Email Monitoring (with caution)	* Blocking access to malicious websites * Identifying accidental data leaks in outgoing emails (avoid privacy concerns)
Security Awareness	Employee Training Phishing Simulations	* Educating employees on cybersecurity best practices * Identifying and mitigating susceptibility to phishing attacks
BYOD (Bring Your Own Device)	Device Management Mobile Data Encryption	* Enforcing security policies on personal devices accessing company data * Protecting sensitive data on lost or stolen mobile devices
Insider Threats	User Activity Monitoring (with caution) Data Loss Prevention Rules	* Identifying suspicious user behavior that might indicate data exfiltration attempts * Blocking unauthorized data transfers based on predefined rules

Conclusion

Data Loss Prevention (DLP) is a broad umbrella covering a wide range of practices, tools, and methods, and it has significant overlap with cybersecurity practices and frameworks. The best DLP outcomes can be achieved by identifying the organizational data vulnerabilities and choosing the DLP solutions, techniques, and policies that are ideally positioned to mitigate those vulnerabilities. Like cybersecurity, DLP is also an evolving domain, and remaining apprised of top-of-the-line DLP solutions, techniques, and tools can give your organization a security edge.

References

1. Wlosinski LG (2018) Data Loss Prevention-Next Steps. ISACA Journal https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2018/volume-1/data-loss-prevention-next-steps_joa_eng_0218#:~:text=Another%20step%20necessary%20to%20protecting,be%20viewed%20as%20organizational%20vulnerabilities.
2. Datardina PM (2009) Information Leakage & Data Loss Prevention. Acc 626 IT Assurance & Governance.
3. Arbel L (2015) Data loss prevention: the business case. Computer Fraud & Security 13-16.
4. Lopez G, Richardson N, Carvajal J (2015) Methodology for Data Loss Prevention Technology Evaluation for Protecting Sensitive Information. Revista Politécnica 36.
5. Perri David F, Perri Erinmichelle D (2018) Acknowledging the “M” in MIS: Managing a Data Breach Crisis. Journal of the Academy of Business Education 19: 9-32.