

WHITE PAPER: DATA LOSS PREVENTION KEY REQUIREMENTS

# Data Loss Prevention Requirements Roadmap

APRIL 2009

Gijo Mathew

CA SECURITY MANAGEMENT

---

# Table of Contents

---

## Executive Summary

---

|   |   |
|---|---|
| SECTION 1   | 2 |
| <b>Why is Data Loss Prevention One of the Hottest Areas of IT Security?</b> |   |
| SECTION 2   | 2 |
| <b>The Eight Key Considerations for Effective Data Loss Prevention</b>      |   |
| SECTION 3: CONCLUSIONS  | 7 |
| SECTION 4: ABOUT THE AUTHOR   | 7 |

# Executive Summary

## Challenge

---

The creation and sharing of digital information within the typical enterprise continues to accelerate. Being able to effectively and efficiently exchange this information to and from any location or person is a prerequisite for every successful company today. However, the very same technologies (i.e. email, Web, IM, etc.) that allow this advanced level of connectivity and collaboration between employees, customers, and partners also generates an enormous security risk for the enterprises that use them. A single “insider” breach of sensitive data, whether inadvertent, intentional or downright malicious, can expose the company to far reaching financial, public relations, legal, and brand reputation costs.

## Opportunity

---

There is an opportunity to raise awareness about the value and proper use of sensitive information. You can reduce risk by learning where valuable information is located throughout the organization, how and where it is being moved, and the level of risk it represents. In addition to preventing information security breaches of Personally Identifiable Information (PII), Intellectual Property (IP), and other Non-Public Information (NPI), your DLP solution should also mitigate all risks created by unsafe or noncompliant behavior conducted electronically.

## Benefits

---

A comprehensive solution will help an organization find, classify, and control the use of sensitive data throughout the company while providing the benefits such as:

- Identifying and analyzing data at all control points including at the endpoint, at rest, at the message server, and on the network.
- Reducing the risk of high-profile losses of Personally Identifiable Information and Protected Health Information (PHI).
- Preventing the inadvertent or malicious disclosure of sensitive information.
- Addressing government and industry information protection regulations.
- Prevent violations of general corporate security and behavioral policies.

## SECTION 1

# Why is Data Loss Prevention One of the Hottest Areas of IT Security?

Information is one of a business's most important assets. Businesses want to be able to access information from anywhere, on any device, and collaborate with almost anyone. The desire for information to be 'free' presents many security and risk management challenges. Organizations have moved from securing the IT infrastructure to securing information. To do this, they must understand where critical data is used and where it is stored. Compounding this challenge is continuous pressure from corporate and regulatory compliance requirements, customer and employee privacy concerns, and the rising cost of a data loss incident.

To mitigate the risks from control-free message, Web, and file activity, organizations need to learn where their valuable information is located, how and where it is being used, and the level of risk it represents. Most importantly, they need to ensure that it doesn't fall into the wrong hands, both inside and outside the organization.

With so many DLP solutions on the market, all making similar claims about their ability to mitigate data loss, it is difficult to know which road to take to proactively reduce your company's risk and protect confidential and sensitive data. Using straightforward language, a lot of common sense, and some out-of-the-box thinking, this roadmap will help you understand the eight essential requirements for a data loss prevention solution that actually prevents information breaches from occurring rather than simply reporting on them. We have compiled the most important requirements from some of the world's most data security-conscious organizations to bring this insightful guide to you.

## SECTION 2

# The Eight Key Considerations for Effective Data Loss Prevention

## 1. Identify and Prioritize Your Most Vulnerable Risk Points

Unwanted internal and external disclosure of Non-Public Information (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) can occur at many different points throughout your network. This is why a comprehensive DLP solution ultimately has to protect all potential risk points in your organization.

While end-to-end protection of all vulnerable sites is the ultimate goal for a DLP solution, in reality, it makes far more tactical and financial sense to begin by protecting the data — as well as the mechanisms used to move this data — that represents the most danger to your enterprise. As the most frequently accessed and used electronic application in all companies, email is, without question, the most susceptible data loss risk point for most enterprises. With literally every employee in a typical organization sending and receiving more than 100 messages every day, it's an obvious vessel for sensitive and confidential information to go where it shouldn't. Adding to this security threat is the fact that email can originate from several different locations, many with gaping security holes, including desktops, mobile devices, public computers, Web-based corporate email, and disconnected laptops.

### Risky Behavior

- Forrester estimates that about 80% of all data leaks occur because of accidents. *Source: The Forrester Wave™: Data Leak Prevention, Q2 2008, Forrester Research, June 6, 2008*
- Insider abuse of network access or email edged out virus incidents as the most prevalent security problem. *Source: CSI/FBI Survey*
- New state, federal, and industry regulations are placing additional burdens on IT staffs when it comes to ensuring the protection of private and confidential information.

Not far behind email in propagating enterprise risk are removable storage devices — USB keys, iPods, CD/DVD burners, and disconnected laptops — that can hold hundreds of megabytes of data. Control-free Web activity also represents a Pandora’s Box of data loss opportunities, particularly due to popular social networking and file-sharing tools such as instant and third-party messaging, Webmail, internet forums, blogs, and wikis.

Additional enterprise vulnerabilities that need to be addressed include scanning file systems, repositories, document management systems, mail archives for sensitive and confidential data, as well as communication protocols such as FTP, general SMTP, and HTTP.

**TAKEAWAY #1** Only after the principal risk points of corporate email, removable storage devices, and Web activity have been sufficiently addressed at all important breach points — including the network boundary, endpoint (desktop PCs, laptops, etc.), and infrastructure servers used for messaging applications — should you move on to monitor and protect other vulnerable points.

## 2. Comprehensive Accuracy Is Essential

While simple, content-based analysis uses lexicon\_matching to detect data loss violations, for every identified authentic breach, hundreds of compliant events are flagged. When your review queue is filled with “false positives,” the only alternatives are to manually inspect hundreds of incidents (most of them legitimate actions), evaluate breaches post event, or relax policy. All of these options — resulting from simple detection — significantly increase the probability of data loss by missing true violations and introducing potentially serious operational inefficiencies by flagging too many events.

The only way to confidently respond to potential violations is to use an analysis technique that is identity and business aware — one that can identify true violations while allowing legitimate business activity to take place. This level of comprehensive accuracy is only possible by going beyond matching simple key words and phrases to examine content\_around\_content and context, while considering enterprise hierarchy and the identity of end users involved. Context, in particular, plays a crucial role in distinguishing a potential data breach from a genuine action. For example, a content\_based approach to detecting three\_digit credit scores would likely flag a file or message containing the number “225” as a potential violation. But since valid three\_digit credit scores only fall between 300 and 850, this information should not immediately qualify as a potential data loss breach. Likewise, if the number “703” is detected between parentheses, it is more than likely a telephone area code in Virginia than a credit score.

In addition to standard scoring for positive “hits”, accurate analysis also involves weighting and scoring offsets to determine whether a file or message should be flagged. For example, a subjective threshold might define a privacy violation when 50 nine\_digit numbers are found in any one document or message. But what if there are only 48 of those numbers — should that item be given a pass? Most likely, it should not.

Taking into consideration the identities involved — such as the author of a document, the sender/recipient of an email, and their role within the organization — is another key analysis technique that helps determine if a given action represents a true data loss risk.

**TAKEAWAY #2** If the DLP solution your company chooses cannot perform comprehensive and accurate content analysis, you won't be able to find and resolve true violations among a mass of false positives. As a result, this ineffective detection system will prevent you from proactively blocking potential data loss violations with confidence, since so many of those flagged actions will be legitimate business activities.

### **3. Insist on Proven, Pre-Built Policies**

An extensive catalog of effective policies — one that employs comprehensive and accurate analysis to provide the right response for any given event — is the foundation of any DLP solution. While it is critical to be able to quickly and easily create and deploy policies, it is just as important that the policies you employ effectively capture your company's best practices and business rules.

Your DLP solution should draw on a complete set of customizable, pre-built, and tested policies that can address an array of security and compliance issues or target a particular area of risk with pinpoint precision. Most must be 100% ready for immediate deployment across all critical risk points, including e-mail, Web, and Instant Messaging. Some may require customer-specific configuration to ensure optimum operation in a particular environment. With either approach, the time and effort required to design, prioritize, develop, and deploy your DLP policies will be dramatically reduced.

An ideal policy catalog should feature packaged, proven methodologies and blueprints that provide options to appropriately respond to violations based on who was involved, what occurred, and what was detected.

**TAKEAWAY #3** No matter how easy it may be to configure a policy, a DLP solution with overly simplified or functionally limited policy capabilities will not deliver meaningful data loss protection. You should insist on a comprehensive set of proven, pre-built policies to provide full breadth of coverage, while enabling quick deployment.

### **4. Protect More Than Just Confidential and Sensitive Data**

In addition to preventing information security breaches of PII, IP, and NPI, your DLP solution should also mitigate all risks created by unsafe or noncompliant behavior conducted electronically. This broad range of activity can include unsuitable and offensive employee behavior, communication not in compliance with various regulatory and jurisdictional requirements, behavior that could compromise legal activity and strategy, uncontrolled financial transactions, and inappropriate handling of customer complaints.

You should also ensure that the solution can address broader regulatory and corporate compliance needs: from HIPAA, SOX, GLBA, and PCI requirements to industry-specific codes specified by the SEC, NASD, NYSE, and FSA.

**TAKEAWAY #4** An effective Data Loss Prevention solution can and should be used to resolve a wide range of information risk issues beyond guarding sensitive and confidential information. Most companies start by addressing DLP-related concerns first, and then expand protection to other areas, such as information misuse.

## 5. Respond Appropriately to Each Incident

Once an event has been determined to be a violation, your DLP solution should respond in real time with the appropriate action such as blocking, quarantining, warning, encrypting, or informing, and then provide suitable steps for immediate remediation. Each response should be gauged specifically to the type and severity of the violation — in particular, by considering who is involved. For example, an infraction caused by the company CEO may need to be handled differently than one by a sales rep or a member of the research team.

Other appropriate responses include redirecting a message or a user to an informative webpage on company security policy, providing procedural support to complete the task at hand, classifying the relevant message or file, updating an incident dashboard, and silently capturing problematic activity. In addition, you should be able to move, copy, delete, or tag all files at rest.

To ensure that breaches are addressed wherever they occur, responses must originate at all potential risk points, including desktop, message server, network boundary, files repositories, and upon import and analysis of historical events.

**TAKEAWAY #5** Instead of a one-size-fits-all approach that only allows passive, post-incident review or indiscriminate blocking of all suspected violations, your DLP solution should provide the flexibility to take the right action for each policy violation.

## 6. Optimize Your Incident Response Process

Half of the battle in data loss prevention is detecting real information leaks while minimizing false positive detections. The other half is efficiently and decisively resolving suspected breaches as close to the incident as possible. To accomplish this objective without impeding business workflow, you need a complete, automated, fully customizable remediation application that helps supervisors and administrators review, audit, escalate, annotate, report, and resolve problematic activity.

An optimized remediation process should always feature native visibility controls that securely determine which manager can review a specific violation. To facilitate the proper course of action, a Web-based remediation application must provide configurable one-click review buttons for easy evaluation of events in their entirety. This includes automating the creation of the audit trail and recording how, when, and by whom each incident was handled in the system. The reviewer must be able to view all relevant information — including the full message, complete files, and attachments in their original formats — as well as be able to search automatically or in an ad hoc manner, and to easily find related incidents to aid investigations.

There should be no need to employ third-party case management tools or to process obscure system activity logs. If appropriate, the originator of problematic content must be able to be notified of incident status or required action via automated, secure messages sent from the review application.

**TAKEAWAY #6** Your DLP solution should not only find all genuine policy violation incidents, but also provide quick and efficient remediation of them.

## 7. End-User Education and Self Remediation

An effective Data Loss Prevention solution must interact with employees so that they understand why a given activity is inappropriate and learn how to self-correct and avoid potential future breaches.

Ongoing education reinforces correct behavior and provides users with full knowledge of the repercussions of violating various company policies. Appropriate interaction with employees at the right time ensures that security and other policies will be top-of-mind for employees — maximizing their data loss awareness. Moreover, this solution dimension can seamlessly complement your company's existing training and awareness efforts for use of electronic communication, human resources, ethics, e-policies, and many other areas of employee education.

When companies do a better job educating employees on the dangers of data loss at the “moment of truth” (i.e. the click of the “send” button), violations will be drastically reduced over time, along with similarly diminished enterprise risk, IT burden, financial costs, and lost time.

**TAKEAWAY #7** While most data loss events aren't intentional, continuing education creates a deterrent effect among people plotting malicious actions, as they will be aware that their actions are being observed. Also, employees who inadvertently violate policy will appreciate learning how to rectify their actions.

## 8. Implement a Flexible Architecture

A DLP solution based on a set of modular, distributed, data\_analyzing components allows companies to immediately and cost effectively address their most pressing requirements while being able to add new controls as their needs change. This type of platform architecture enables the system administrator to determine which combination of control points provides necessary coverage for your company. In some cases, only desktop or laptop controls may be desired, while in others, network control points will be necessary. In certain situations, server\_based controls combined with desktop and network controls may achieve an enterprise's data loss prevention objectives.

A modular approach will ensure speedy deployment, eliminate single points of failure, and easily scale to protect 500 or 500,000 employees. Endpoint or client components should be able to ensure protection even when disconnected from a central server or from the corporate network. When the user re-connects to the corporate network, new policies must be automatically downloaded and captured incidents seamlessly uploaded.

The platform should provide automated policy distribution so that the right policy is quickly and securely deployed to the right place imperceptibly to the user, ensuring higher adoption rates. All capabilities must be supported regardless of the number of policies used or the number of control points (50,000 desktops or five network egress points).

In addition, the DLP solution must work in a variety of locations (desktops, network, messaging servers and data repositories) in any sequence, with supplementary modules added later with little effort. As new data types, channels, and protocols emerge, the solution should be able to adapt to these evolving requirements.

**TAKEAWAY #8** Compared to a rigid or unproven solution, one with a modular, distributed architecture — providing superior flexibility, scalability, performance, and fault tolerance — is the best way to cover both current and future information risk needs.

### SECTION 3

## Conclusions

### **CA DLP (Data Loss Prevention) delivers all eight vital requirements.**

CA DLP protects the enterprise from a wide range of data loss and misuse by detecting and responding appropriately to the true violations that can cause extensive financial, legal, public relations, and brand damage. Industry-leading detection methods and analysis avoids creating massive queues of false-positives, enabling organizations to concentrate compliance and data loss review efforts on genuine breaches and pursue immediate corrective action.

CA DLP monitors and detects violations across many control points, including email, IM, Web, mobile mail, FTP, file repositories, and endpoint activity. Once an infraction is detected, it takes appropriate actions such as blocking, warning, quarantining, or alerting a supervisor.

Equally important, the intelligent review process provides an array of capabilities that allows administrators to focus exclusively on security violations relevant to their specific area of oversight. Integrated workflow facilitates advanced searching, escalation, and other case management activities — all of which automatically builds an extensive audit trail. Finally, ongoing education helps employees understand, self-correct, and prevent future data loss risks.

The CA DLP product helps organizations protect and control sensitive data wherever it is stored or used, significantly minimizing the risks associated with uncontrolled information. It addresses a broad set of risks while minimizing the operational burdens associated with the detection and remediation of these risks. Data loss prevention is part of a holistic Identity and Access Management strategy. A complete solution allows organizations to manage identities, control access, and protect how people use the data they have access to. This approach helps organizations streamline IT security environments and enables them to be more secure, agile, and compliant with regulations and privacy mandates. By implementing complete, automated, and integrated solutions, organizations striving towards lean and efficient IT systems realize a faster time to value and a reduction in costs, manual review, and security risks.

---

To learn more about CA DLP and its ability to help you to unify and simplify IT management for better business results, visit [www.ca.com/dlp](http://www.ca.com/dlp).

#### SECTION 4

## About the Author

### **Gijo Mathew — Vice President, CA**

Gijo Mathew leverages ten years of software development and security experience to interpret customer needs, drive security awareness and implement business centric strategies within enterprise organizations. For CA, he ensures that solutions reflect customer needs, market requirements and industry standards. His expertise extends into many areas of security including Data Loss Prevention, Security Information Management, and Identity Management. Gijo is a Certified Information Systems Security Professional and uses his experience to help organizations master the art of security by balancing business needs and risks.

CA (NASDAQ: CA), one of the world's leading independent, enterprise management software companies, unifies and simplifies complex information technology (IT) management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure IT.

MP335110409