Realtime publishers

"Leading the Conversation"

The Essentials Series:
Email-Centric Data Loss Prevention

# Executive Perspectives on Data Loss Prevention

*sponsored by*

proofpoint

by Dan Sullivan

## *Copyright Statement*

# Executive Perspectives on Data Loss Prevention

The range of business assets has expanded well beyond traditional tangible objects, like real estate and manufacturing equipment, to include intangibles such as intellectual property and business information. Management practices that have been traditionally used with tangible assets are now being applied to intangible assets as well. Risk management techniques are particularly important because information assets are subject to a wide array of threats, and even the best designed information management system harbors vulnerabilities. For example, confidential information can be exposed when a laptop is stolen, an attacker gains access to a database by exploiting a vulnerability in a Web application, or an employee mistakenly emails a confidential document to someone outside the company. These are just some examples of the risk of data loss. Data loss prevention (DLP) is a risk management practice that is designed to protect private and confidential information while supporting and enabling business operations.

This series examines the practice of DLP from three perspectives: an executive's view, an employee's perspective, and a technical standpoint. In this first article in the series, we consider issues important to executive management:

- Business drivers for DLP adoption
- Multiple dimensions of DLP
- Key benefits of deploying DLP technologies

This series will focus on email-based data loss. As many of the challenges and issues of DLP are found in email management and email is a virtually universal technology used in business, this area of DLP provides a representative and broadly relevant model for understanding DLP in general.

## Business Drivers for DLP Adoption

Besides the obvious need to protect the confidentiality, integrity, and availability of information assets in general, executive management must address compliance requirements while enabling and promoting more efficient operations.

### *Compliance*

Compliance with government and industry information management regulations has become one of life's certainties, along with death and taxes. Regulations range from broad privacy protections designed to protect consumers to targeted, industry-specific standards.

Government regulations vary by jurisdiction, especially with regard to privacy protection. For example, at least 44 states, the District of Columbia, and Puerto Rico have data breach laws (see the National Conference of State Legislators for a full list). Although many states follow similar guidelines to those established in California's privacy law, there is still significant variation in state legislation. For example, Texas and Kansas laws have no right of private civil action but California and Illinois laws do. Compliance with privacy legislation also extends beyond U.S. boarders. Companies doing business in Canada are subject to both national and provincial privacy laws and the European Union has long established privacy directives as well.

Other well-know regulations are industry specific:

- The Health Insurance Portability and Accountability Act (HIPAA), a federal government regulation that defines required policies and procedures to secure protected healthcare information
- The Payment Card Industry Data Security Standard (PCI DSS), an industry established standard that defines minimal protections for credit card transaction and cardholder information
- The Gramm-Leach-Bliley Act (GLBA), a federal government regulation that specifies consumer protections in the banking and financial services industry

A common theme across information protection regulations is the need to preserve the confidentiality of particular categories of information. Rather than devise individual policies to comply with the nuances of every possible regulation that applies to a business, it is often more prudent to ensure that a single comprehensive governance, risk management, and compliance strategy meets all requirements. DLP is a fundamental component of such a strategy and within that DLP framework, there should be significant efforts to prevent email-based data loss.

### *Business Innovation*

DLP is not just about cost avoidance, though. With sufficient controls in place to preserve the confidentiality, integrity, and availability of information assets, businesses are in a position to leverage technology to enable more efficient operations. Consider a few examples.

- In healthcare, doctor-patient communications typically occur in person or over the telephone; electronic communications, especially email, are not generally considered secure enough. If email were available to physicians, they could more efficiently share information, respond to questions, relieve office personnel, and more easily collaborate with colleagues on patient cases.
- In the retail sector, reliable and secure communications could enable better data collection about customer buying habits, which in turn support more personalized marketing efforts.
- Financial services are information intensive yet as any mortgage holder can attest, the business processes in this industry remain unusually paper intensive. Innovation and streamlining is dependent in part on ensuring secure communication channels that include DLP controls.

There are both negative and positive incentives to adopt DLP processes and technology. The range of government and industry regulations demand such measures but business opportunities for new services or more efficient operations are also compelling reasons to formalize DLP controls. Taking that step to more structured management of DLP requires the attention of multiple branches of executive management.

## Multiple Dimensions of DLP Risk Management

We have seen that there are multiple business drivers for adopting a formal DLP framework; similarly, there are multiple dimensions to the management of such a framework. These include human resources, financial controls, and information security management as well as non-IT business units. Although each of these areas has their own domain-specific issues, they should all be considered part of a single risk management practice.

Risk management entails inventorying assets, determining their relative values, assessing the threats to those assets and any inherent vulnerabilities, and ultimately formulating a plan to mitigate risks to them. This is obviously a complex task. Many parts of the organization will contribute to the development of a risk management plan as well as its implementation. In the following sections, we will examine a few specific contributions as well as one more generalized example from different functional areas of a business.

### *Human Resources and DLP*

DLP begins with people. If we start with the reasonable assumption that employees, contractors, and business partners see their success aligned with the success of the business, one has a significant set of allies in the effort to prevent data leaks. It follows that most employees would not intentionally leak intellectual property, allow a breach of customer credit card data, or email confidential documents in an unsecure manner. The problem from a human resources perspective is making sure they do know and that they do comply.

Before human resources executives can develop strategies for educating employees, well-defined policies must be in place. Email and data classification policies, for example, should address:

- Acceptable uses of email applications;
- Types of information that may be shared via email, which in turn depend upon
- Data categorization schemes defining public, private, and confidential information;
- And restrictions where information may be sent, for example, no company confidential information may be sent to personal email accounts.

It is also imperative that email policies be kept up to date. Many of the principles behind email policies may also apply to the use of social networking sites, for example, and should be stated explicitly.

Another aspect of human resources' role in DLP is ensuring that employees are aware of policies and sufficiently trained. Policies are virtually useless if they sit on a shelf and are not implemented and enforced. Human resources personnel will likely have to work with their IT colleagues to develop metrics for measuring compliance with policies. For example, IT may provide an email content filtering system to scan and quarantine messages that contain confidential information sent outside the company. This application can provide useful information about where these messages originate, the employee involved, the content that triggered the quarantine, and so on. This type of information, in aggregate form, can help identify weaknesses in compliance and employee understanding of policies.

### *Financial Management and DLP*

Financial management's role in DLP management is two-fold: articulate the costs of risks associated with data losses and define what is required to remain in compliance with respect to DLP.

A business needs quantified measures of the cost of data leaks to understand how to allocate resources to mitigate the risk of data loss. Most likely one will never come up with a precise figure. For example, if customer credit card information is disclosed, those customers will have rights as defined by various privacy laws in the various states with jurisdiction. Depending on the distribution of customers in the different jurisdictions and the projected size of the breach, the associated costs could range from low to high. Although this is clearly a challenge and there may be no estimate that is 100% satisfactory, there are costs associated with choosing to not manage data loss as well.

Another contribution from financial management is support for governance and compliance. Financial managers are well versed in policy definition, audit controls, and oversight. The same skills that worked well managing financial resources have analogs with regard to managing information resources.

### *IT and Security Management's Role in DLP*

IT management, and security professionals in particular, will likely work closely with human resources on employee training and with financial management on policies and audits, but they are also responsible for devising, implementing, and managing technical controls. The fundamental responsibility for IT within the DLP framework is to ensure that security measures are properly aligned with business strategy. If one becomes too narrowly concerned with mitigating all possible risks without tempering those concerns with the practical needs of the business, one risks impeding the normal flow of business.

Consider an overly rigid content filtering policy for email: any email message containing private or confidential information must be quarantined and reviewed before it is sent to its recipient. This is clearly unworkable and would likely quarantine a large percentage of executive communications. A better approach is to log the sender, the recipient, the category of information sent, and other information about the message. Knowledge of this kind of monitoring will dissuade some from disclosing information and the log will be a valuable source for monitoring for questionable patterns and for mining forensic data, if needed.

For IT management, the goals are too keep security measures aligned with business strategy without hindering operations. This in turn requires a well-designed DLP framework—*ad hoc* responses are less likely to be effective and are more likely to disrupt other business operations.

### *Other Business Units and DLP*

Human resources, financial management, and IT management bear responsibilities that cross organizational lines, but individual departments have a role in DLP within their own organizational units. Consider, for example, DLP in a marketing department. Questions such as the following arise:

- Is confidential information about marketing and product plans leaking to competitors?
- If so, how would one know?
- Are employees sending sensitive information to their personal email accounts in violation of policy?
- Could marketing information leak through social networks and collaboration tools like blogs, wikis, and third-party sites?

Departments that do not have a direct responsibility for DLP planning still have a role with regard to ensuring employees understand and follow policies. They must provide IT with functional requirements about their business operations and support data classification efforts to ensure that confidential information is properly identified and controlled. DLP is a complex challenge that requires the coordinated efforts of multiple departments in a business, but the benefits are equally widespread.

## Key Benefits of Deploying DLP Controls

DLP controls protect information, support compliance efforts, and enable operational efficiencies. With well-planned and managed DLP controls, businesses can

- Raise the cost and ability threshold of attackers attempting to steal information. One cannot guarantee that a determined attacker will never discover a particular piece of information, but one can try to make the cost of acquiring that information greater than the value of the information itself.
- Reduce the chance of accidental and unintentional leaks of confidential and private information.
- Support various compliance efforts, ranging from government-legislated privacy protections to ensuring the integrity of business operations as required by industry regulations.
- Support operational efficiency by establishing preventive rather than reactive controls on protected information assets. With secure communication channels in place, businesses can be more innovative with how email is used knowing that the risk of data loss is mitigated and if there were a problem, the DLP systems would help detect the incident sooner rather than later.

Businesses need to attend to the problem of data loss in order to remain in compliance with government and industry regulations, but also to sustain efficient business operations. No single department is responsible for planning and implementing DLP efforts; the responsibilities, as well as the benefits, of data loss protection, span the enterprise.