Realtime publishers
"Leading the Conversation"

The Essentials Series:
Email-Centric Data Loss Prevention

Benefits of Using Data Loss Prevention Technology

sponsored by
proofpoint

by Dan Sullivan

Benefits of Using Data Loss Prevention Technology 1
Need for Automated DLP 1
Benefits of Automated, Email-Centric DLP 3
The Cost of DLP 4
DLP and Business Operations 5

Copyright Statement

Benefits of Using Data Loss Prevention Technology

Data loss prevention (DLP) has emerged as an important element of risk management and compliance, and governments around the world have established laws and regulations to protect the privacy of their citizens. Some governing bodies, such as the European Union, have adopted a broad set of privacy regulations that apply to all member states; the United States has chosen a different path to regulation with individual states crafting consumer privacy protection measures while the federal government has established regulations in specialized areas, such as healthcare and banking. From a business perspective, DLP is both required by regulation and in a business' own self interest.

This, the third and final article in the series, examines the benefits of using automated DLP technology to meet business and compliance requirements. In particular, this article examines:

- The need for automated DLP
- The benefits of such technologies
- The costs incurred when automated DLP solutions are not used
- DLP and business operations

Together, the articles in this series highlight key aspects of an effective DLP strategy: comprehensive executive management, effective engagement of employees, and the appropriate use of DLP technology.

Need for Automated DLP

In theory, DLP does not require automated tools. Organizations can, and do, manually monitor employee emails. Proofpoint's *Outbound Email and Data Loss Prevention in Today's Enterprise, 2008*, an international survey of large enterprise responses to and concerns about outbound messaging security conducted by Forrester Consulting, found that manual methods are commonly used:

- 41% of US companies with 20,000 or more employees employ staff to read or otherwise analyze outbound email; 35% of European companies of the same size employ staff for this function
- Considering companies of all sizes, 29% of US companies, 20% of European companies, and 27% of Australian companies employ staff to read or otherwise monitor employee email.
- 22% of US companies and 11% of European companies with 20,000 or more employees employ staff whose primary or exclusive job function is to read or otherwise monitor outbound email content
- Considering companies of all sizes, 15% of US companies, 5% of European, and 17% of Australian companies said they employ staff whose primary function is reading or otherwise monitoring employee email.

Human resources are expensive and cost conscious companies do not employ staff without justification. If substantial percentages of surveyed companies are employing staff to read and analyze staff email, there must be some compelling reasons. Those reasons are also found in the Proofpoint survey.

In the 12 months prior to the survey, 44% US companies investigated email leaks of confidential or proprietary information and 40% investigated suspected violations of privacy or data protection regulations; in Europe the rates were 30% and 32%, respectively, and in Australia, the rates were 23% and 27%, respectively. Violations of policies and regulations adversely impacted 23% of US respondents, 30% of European respondents, and 23% of Australian respondents. In addition to these findings, the Proofpoint survey found even higher levels of concern about potential data leaks from mobile devices. 56% of US respondents are concerned or very concerned about such leaks from email used with mobile devices; the same is true of 40% of European companies and 43% for Australian companies. These survey results paint a picture of concern justified by findings of negative consequences of data leaks.

Given that roughly one-quarter of respondents have suffered negative impacts of data leaks, it is prudent for businesses to consider the potential risks of such events in their own operations. If one further calculates the expected costs of data breaches in terms of loss of intellectual property, fines for lack of compliance, and the cost of negative publicity and brand damage, an investment in dedicated staff to monitor email can seem reasonable and justified; however, is it enough?

Surveys such as the one discussed here are useful for understanding the scope of email-based data loss across a range of industries and geographic regions. This information can inform policies and support risk analysis calculation, but more company-specific details are needed to for day-to-day management decisions. For instance, managers need metrics on scope of policy violations and potential leaks to craft targeted employee training programs and identify the most frequent types of regulation violations. Even in cases in which manual email review is used to block leaks, there may not be sufficient data collected to meet management needs. This is just one of several reasons automated DLP tools are used to complement other information control measures.

Benefits of Automated, Email-Centric DLP

The benefits of automated email-centric DLP tools can be described in terms of

- Effectiveness
- Efficiency
- Consistency
- Targeted application

Some combination of these attributes can be found with manual operations, but maximizing benefits for all these can be costly and/or adversely impact business operations.

In terms of effectiveness, automated solutions can more cost-effectively scale to the volume of email traffic in today's enterprises than manual approaches. A properly scaled automated solution could scan all outgoing traffic rather than just sample a subset of all traffic.

Efficiency is also a consideration because email is an essential business communications medium. Automated DLP tools can scan and send messages with minimal delay when compared with the potential delay if human review is required. (Human review of messages already sent is useful for detecting, but not preventing, data loss.) With automated solutions, routine business operations as well as more innovative uses of email can continue without unwarranted slow-downs.

Consistent application of policies is another benefit of automated tools. This is especially important with respect to compliance. If a regulation specifies per-incident fines for violations, even a single email leaking protected information could become an expense for a business. Similarly, a significant loss of proprietary information can occur in few emails. From a management perspective, the consistency of automated DLP solutions means that the data collected by these tools is comprehensive; management does not have to settle for monitoring email it thinks might potentially leak data; it can evaluate all of it.

Policy rules and responses can be readily crafted to the particular requirements of an enterprise and shared between businesses. A company that manages protected healthcare information can customize policies to align with HIPAA requirements. A retailer maintaining compliance with Payment Card Industry (PCI) data protection standards can establish policies to scan for credit card information in outbound email. Many companies are subject to broad US state and European Union privacy laws regarding personal and financial information; over time, best practices may become encoded in policies and shared among system users. Both automated and manual controls can reduce the risk of data loss, but both incur costs.

The Cost of DLP

There are the obvious costs of DLP measures: the cost of software and hardware for automated tools; the cost of installing, configuring, and maintaining the system; the cost of creating policies and training employees on those policies; and the cost of monitoring and auditing DLP measures. These are far from the only costs. Perhaps less obvious, but also important, are the costs of not employing DLP measures.

To start an evaluation of email-centric DLP tools, one needs to consider the level of control that is needed over outbound emails. The next step is assessing options for implementing that level of control, such as with existing email management tools, using manual review of emails, or the adoption of a DLP application. The ideal solution will balance effectiveness, efficiency, consistency, and customizability with cost. Even ideal solutions, though, may not seem justifiable unless one also considers the cost of not deploying a DLP system. Not addressing the problem of email-based data loss can leave an organization vulnerable to a costly trio of problems:

- Lack of compliance
- Stunted business process innovation
- Loss of intellectual property

Businesses face an array of regulatory requirements and a sound DLP program can help meet multiple needs in this area. Privacy regulations are largely designed to prevent the disclosure of personal information without the person's permission and to create incentives for businesses to protect that information. DLP, along with data classification efforts, access controls, monitoring, and auditing, is a basic security practice that enables compliance with a variety of regulations. Another beneficiary of DLP management is business innovation.

It is easy to construe a tool or practice designed for compliance as a drag on business innovation. Compliance can be seen as just a set of things you cannot do. However, it can also be the means for getting the tools you need to enable new business processes. Consider healthcare professionals who might want to communicate with patients via email. Doctors and patients might agree but if a compliance officer does not agree, it will not happen, at least not to the degree possible. Assuming a regulation does not specifically bar the use of email, a compliance officer might agree to its use if conditions are met to sufficiently reduce the chances of data loss. The same logic applies in other industries, such as banking, retail, manufacturing, distribution, and other areas with significant exchange of financial and other confidential data.

Privacy regulations are designed to ensure businesses protect other people's information. There is no need for such regulation when it comes to businesses protecting their own valuable information—self-interest is sufficient. Without an automated DLP system, though, how can a business efficiently and effectively monitor all the email messages and attachments that pass through its servers every day? Even if the chance that a message contains proprietary information is small, the sheer volume of messages sent in businesses means that the overall likelihood of a breach is much higher. When considering the cost of DLP solutions, it is important to include both the upfront costs of acquiring a system and the potential costs of not deploying such as system.

DLP and Business Operations

Throughout, this series has described the breadth and depth of data loss risks that many businesses confront. Fortunately, one does not have to address all these risks at once. Automated DLP systems provide the means to incrementally improve a business' security position, especially when combined with a four-step process.

The first step is to identify and address the most common problems. This could be carelessness on the part of employees sending confidential material to personal email accounts, customer service representatives responding to inquiries with email messages containing credit card data, or a comparable problem. Addressing these early, easy-to-identify problems should include employee training to raise awareness of the issue. As noted in the second article in this series, an effective DLP strategy leverages technical controls and employee understanding of DLP issues.

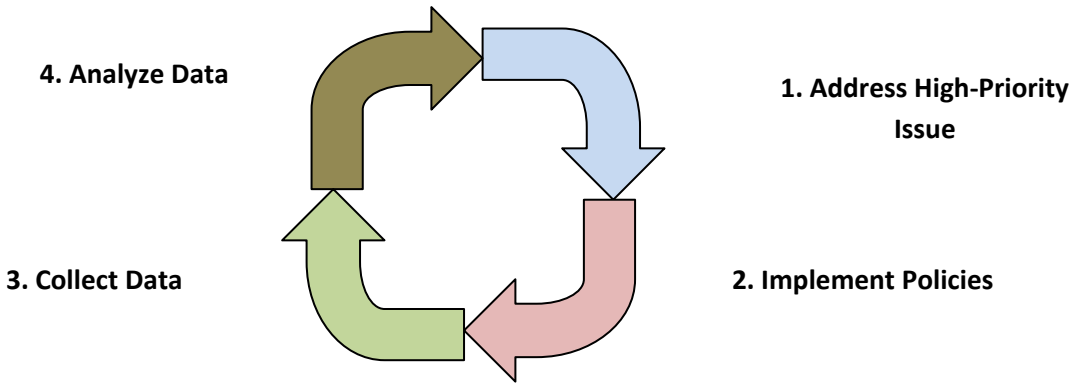

Figure 1: A four-stage process for incremental improvement of DLP.

The second step is to implement application-enforceable policies in a DLP system. These policies direct the DLP system to block outgoing email, quarantine messages, and collect data about suspect email messages.

Closely linked with the second step is the third part of the process: collect data on policy violations. The goal here is not necessarily to block a particular message (that is addressed by step 2 processes) but to aggregate information over multiple violations to identify patterns of interest. These could include higher than expected violations from one particular department or branch; an unusual spike in violations of a particular rule in the policy; or even an attempt to email a particularly sensitive piece of information.

The fourth step in the process is to analyze the data collected in step three to identify the next set of high-priority violations. The aggregate data from the DLP system may be useful to C-level executives as well with regards to refining DLP strategy and ensuring that risks are properly managed. Employees can receive feedback when messages are blocked, including details of policy rules that are violated, reinforcing training.

Effective, comprehensive, and cost-efficient DLP is a product of sound management, employee participation, and the judicious use of automated controls.