BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Data Security

Risks and Rewards of Using Data Loss Prevention Technology in Information Security Programs

By Margaret P. Eisenhauer

Peggy Eisenhauer is founder of Privacy & Information Management Services–Margaret P. Eisenhauer, P.C., a privacy, security and information management law firm. Eisenhauer helps companies develop, implement, and assess privacy and fair information practices, including policies governing the collection, use and disclosure of consumer, professional and employee information. She has extensive experience with U.S. and international privacy and security laws and is a Fellow of the Ponemon Institute, a Certified Information Privacy Professional (CIPP) and a member of the International Association of Privacy Professionals CIPP Advisory Board. Eisenhauer can be reached at peggy@privacystudio.com or (404) 914-1163. The information in this article has been prepared for informational purposes only and is not legal advice. The need for legal services and the selection of an attorney should not be based solely upon these materials.

Companies spend substantial time and money developing and implementing information security policies and procedures. As part of this process, information security teams often employ data loss prevention (DLP) technology to help assure compliance with the policies and procedures.

While DLP tools can be used at any stage of information security program maturity, the greatest benefit comes when the tools are used within the context of a defined security program. In this model, companies classify document types and data elements based on sensitivity or regulatory requirements (*e.g.*, those regulated under the Health Insurance Portability and Accountability Act or Gramm-Leach-Bliley Act), and specify rules to appropriately manage the risks associated with the data processing. For example, a rule might restrict access to systems containing sensitive personal information (such as Social Security numbers) or prohibit the transmission of sensitive information via unencrypted e-mail. DLP tools then verify compliance with these established rules, identify compliance gaps and, in some cases, enforce those rules automatically.

For companies that do not have a formal information security program, DLP tools can be used to help locate sensitive data within the enterprise and enforce legal requirements, such as Payment Card Industry Data Se-

 ISSN 1538-3423

curity Rules [PCI] rules or Social Security number transmission restrictions.

This paper explores the types of DLP products that exist and the issues that corporate lawyers should consider when evaluating these products.

Types of DLP Tools

Data loss prevention providers offer an array of DLP products. These products can locate and inventory specific data types across corporate systems, monitor data traffic internally and externally, assess and enforce compliance with pre-established rules, and provide reports on various events. The tools provide compliance support for both data-at-rest within corporate systems and data-in-transit across systems/applications and with external recipients.

Assessment tools can scan systems and applications and determine where different data types reside, so that an inventory of systems/applications with sensitive data can be created. The tools enable companies to catalogue instances of specific document types, file types and data elements (such as PCI data, Social Security numbers or protected health information). The assessment can also determine how data flows among systems, applications, and users.

Monitoring tools can confirm that the company's application of its rules for handling sensitive personal information is consistent across all the system assets that contain sensitive personal information. For example, the tools can verify that role-based access controls and data transmission rules are consistently applied.

The tools can help enforce policies by reporting policy violations. For example, the tools may monitor data-in-transit and alert users and/or company security personnel to inappropriate conduct, such as attempts to download sensitive information or to transmit sensitive information via unencrypted e-mail. The reports may contain detailed information on network user activities, allowing managers to detect both inadvertent and malicious policy violations. Alternatively, the reports can contain summary information about network activity, without user information. While less detailed, these reports still permit managers to identify procedural and training gaps.

Some DLP products can enforce security rules. DLP products can block the downloading of sensitive information to portable devices, USB [universal serial bus] drives or other insecure media. They can scan, intercept and encrypt e-mails with sensitive data elements prior to transmission over the Internet.

Finally, DLP tools can be used for other corporate purposes, such as protecting intellectual property and enforcing acceptable use policies and worker productivity rules.

DLP Rewards & Risks

The benefits of using DLP tools to support security program compliance efforts are clear. These tools support data inventory development and data flow mapping. By demonstrating that sensitive information assets are known and rules applied properly, they provide an unparalleled level of confidence in your compliance posture. They can also provide real-time alerts to business process and employee training issues and prevent inappropriate data transmissions and security incidents.

While the benefits of DLP tools are great, there are risks that must be considered as well. Critically, companies that engage in compliance monitoring must be prepared to respond to the gaps revealed. Prior to deploying monitoring, companies should consider what gaps may be revealed and how those gaps would be closed. Companies should confirm that the reports being generated by the monitoring tools will be both appropriate and appropriately handled. Corporate counsel should also consider how these reports fit within the corporate document retention program.

Companies that are not prepared to resolve compliance issues may wish to deploy basic loss prevention technology, such as automatic encryption of sensitive data, as a stopgap measure during the policy and procedure development process.

Companies must also ensure that their DLP implementation is appropriately respectful of worker privacy interests, including compliance with any applicable international data protection laws. Employees should be informed about the use of DLP tools and the ways that reports will be used within the company. Some states require notice of electronic monitoring, and it is a good practice even if not legally-required. In addition to showing respect for the workers, this transparency serves to reinforce the importance of the underlying data handling rules.

From a worker privacy standpoint, DLP tools raise more serious concerns when used for productivity analysis (such as determining if employees are spending time on non-business Web sites) than for privacy/security compliance. However, companies should confirm that the proposed DLP implementation and reporting plan are consistent with privacy promises made to workers. Additionally, if the company has workers outside of the United States, the DLP implementation may raise international data protection law concerns. Corporate counsel should understand the scope of the DLP program to determine if any non-U.S. workers or customers will be impacted.

International Considerations

Many companies have information systems that span national boundaries. These companies may utilize centralized information systems or process all company e-mails on a U.S.-based server. These companies must carefully consider data protection law implications to their DLP initiatives.

European data protection laws generally limit the ability of companies to monitor worker communications, such as e-mails. European Union laws also often protect employee activities, such as Web-surfing. Any DLP initiative that encompasses EU worker data (even if stored in the United States) should reflect the requirements of the applicable laws as well as any works council agreements.

Data protection laws also require companies to assure an appropriate level of security for personal information they process. DLP technology can help companies meet these security requirements in appropriate ways. For example, use of technology that automatically encrypts sensitive personal information can help a company meet its security goals without offending worker privacy interests, if the encryption is done without creating reports that identify non-compliant users.

Thoughtful implementation of DLP tools can help companies achieve security goals while balancing

  PVLR ISSN 1538-3423

worker privacy interests and meeting data protection law obligations. However, if your DLP tools will be used to monitor international worker communications, you should consult your local counsel regarding the best approach for your company.

Questions to Consider when Selecting DLP Products

When considering a DLP product suite, corporate counsel should ask the following types of questions:

■ *What are our goals?*

If you are in the policy creation phase, you may want tools that identify the systems and applications that house sensitive data. If you have policies/procedures in place, you may want to assess compliance with those policies/procedures and detect gaps. Or, you may want to use DLP tools to achieve specific compliance objectives, such as blocking certain types of data transmissions or automatically encrypting communications with sensitive data. When considering DLP products, select the tools that will enable you to achieve your specific corporate goals and manage the scope of the implementation to maximize the benefits while managing risks.

■ *How do we classify data within our organization?*

DLP tools work best when the company has clearly defined data classification standards. Unfortunately, many companies classify data on an *ad hoc* basis, given the application. If your organization has not created a comprehensive data classification scheme, it may be difficult to determine what data elements to monitor across your enterprise. You may want to create a master data classification policy prior to your DLP implementation.

■ *What policies/procedures currently exist?*

If your goal is to assess your compliance posture, you should tailor your use of monitoring tools so that you are assessing against your current compliance structure. For example, if you prohibit transmission of unencrypted Social Security numbers or PCI data, you can use monitoring tools to determine compliance with these rules. But note that it generally does not make sense to audit in a vacuum. If you have not established internal rules (and trained your users on those rules), you have nothing to assess against. Formally establish, document and communicate your data handling expectations before you begin auditing.

■ *What are our risks? Are we prepared to address gaps detected by our DLP tools?*

Before undertaking any assessment initiative, you should have confidence that the management team will appropriately respond to the results. You should also confirm that your incident response program is sufficient to provide guidance in the event of ''worst case scenario'' findings. You may want to formalize the reporting infrastructure, so that the results can be considered and prioritized by the right individuals. You may also want to consider if the results can be protected under any type of self-assessment privilege in those jurisdictions where you do business. You also want to ensure that employee privacy interests and data protection obligations are respected.

■ *How do the data loss tools support our existing enterprise risk management efforts?*

Finally, it is appropriate to consider how your implementation of data loss products can support broader enterprise risk management (ERM) initiatives. For example, DLP tools may be used to protect intellectual property as well as personal data. You can evaluate the ability of your DLP tools to achieve other ERM goals at initial deployment or over later implementation phases, once your initial compliance objectives are met.

Final Thoughts

DLP products should play an important role in every information security compliance program, but use of these tools requires careful consideration of the risks and benefits. Once the company's internal needs have been identified, the company can select the DLP product suite that best meets its operational needs.