

EXPLORING

Data Loss Prevention Systems for Legal Holds and E-Discovery



Many organizations use data loss prevention (DLP) systems to monitor and guard against unauthorized use and transmission of proprietary and/or confidential electronic information, as well as against communications violating their code of conduct policy (e.g., insider trading or sexual harassment). However, they may not know that their DLP systems store in-

requently store copies of communications, including web browsing conduct, that may be relevant in certain regulatory and litigation contexts, this results in the risk that such systems will be overlooked as a potential source of electronically stored information (ESI) that should be considered for legal holds and e-discovery purposes. In fact, DLP systems may need to be included in an organization's targeted ESI data map for purposes of *Federal*

What, if any, DLP systems are being used?

An organization should identify who is responsible for its DLP systems. Typically, only a few personnel have access to these systems (e.g., information security group). Ask this group what DLP system, if any, the organization is using. Different DLP systems may take different approaches to achieving the end goal – detecting and preventing the unau-

Data loss prevention (DLP) systems police electronic communications to prevent intellectual property and a variety of other sensitive information from falling into the wrong hands. They also pose a challenge to records and information management, legal, and IT professionals, who must work together to ensure that the information DLP systems capture is addressed properly to meet the organization's legal holds and discovery requirements.

M. James Daley, Laura Clark Fey, and Diana Fasching

formation that may be relevant to actual or reasonably anticipated litigation, government investigations, or audits. And, this is a situation where what they don't know can hurt them.

DLP systems are designed to monitor and classify electronic information while it is:

- In motion (as users send e-mails or instant messages)
- In use (as users create or modify documents on their c:\drive)
- At rest (as users store documents on network file shares)

DLP systems generally work in a way that is invisible to users. They are primarily familiar to information technology and information security personnel and those responsible for addressing violations. Thus, others who need to know – such as inside counsel and records and information management professionals – may not even be aware such systems exist.

Because DLP systems may sepa-

Rules of Civil Procedure Rule 26 meet and confer disclosures.

Following are key questions an organization should ask to gain a more thorough understanding of whether its DLP system contains information that may be subject to legal holds and/or discovery obligations.

1. What, if any, DLP systems are being used?
2. What communications are being monitored and for what purpose?
3. What information is being saved within the DLP system?
4. How long is such information saved?
5. When implementing legal holds, is information being saved by the DLP system being taken into consideration?

Answering these questions will better position an organization to evaluate what steps it can take to ensure compliance with legal hold and discovery obligations.

thorized use and transmission of information. For example, some DLP systems store only unauthorized communications, while others store every communication they monitor.

Additionally, some organizations may use more than one DLP system because it has concluded (or is testing its assumptions) that two DLP systems working in conjunction better help achieve its data loss prevention goals.

What communications are being monitored and for what purpose?

DLP systems generally include a wide selection of out-of-the-box, pre-defined policies an organization can selectively turn on to monitor communications for content, such as personally identifiable information and payment card industry data. DLP systems are generally capable of monitoring any information transmitted over a network using corpo-

rate e-mail, webmail, instant messaging, file transfer protocol, web-based tools, or any generic transmission control/Internet protocols. But, few organizations monitor every communication. For example, an organization may monitor e-mail sent to or received from people outside of the organization, but it may not monitor e-mails sent internally.

When an organization enables a security policy, which is a set of rules it has chosen to follow, the DLP system monitors and, depending on how it is configured, may even enforce compliance with it. For example, rather than allowing an employee to send an e-mail with confidential information outside of the organization, the DLP system

may intercept and stop the transmission of the e-mail and notify the sender that the e-mail containing confidential information was not sent.

In addition to enabling out-of-the-box, pre-defined policies, DLP solutions generally allow organizations to create custom policies. For example, if an organization wants to monitor e-mails for reference to a highly confidential product or service in development, it could create a custom policy to detect e-mails sent outside of the organization that contain the product or service's name.

Understanding the policies an organization has enabled provides insight into the type of information that may be stored in its DLP system, which is invaluable to understanding whether the system may contain information subject to legal holds.

For example, if an organization is monitoring communications for mergers and acquisitions, its DLP system may contain information that

is subject to legal holds if it is facing actual or anticipated litigation related to recent mergers or acquisitions. Whether or not the DLP system contains information subject to legal holds depends on the specific configuration of the organization's business and DLP system. Consider asking the following:

- Does the organization monitor e-mail that employees (including anyone authorized to use its e-mail



Understanding the policies an organization has enabled provides insight into the type of information that may be stored in its DLP system

systems, such as contractors and temporary workers) send or receive when both the sender and recipient(s) are using its e-mail system?

- Does the organization monitor e-mail that employees send to or receive from people outside of the organization?
- Does the organization monitor e-mail that its employees send or receive using web-based e-mail systems (e.g., Google Mail, Yahoo! Mail, or Microsoft's Hotmail)?
- Does the organization monitor instant messaging communications? If so, does it include instant messages sent employee-to-employee and/or instant messages sent to or received from people outside of the organization?

- Does the organization monitor websites that employees visit?
- Is the organization monitoring any other communications?

Working with information security personnel to refine the content it monitors will help an organization find a balance between protecting itself and monitoring – as well as potentially storing – more information than it can manage effectively.

General security policies, such as monitoring for webmail usage, may be overbroad for an organization's needs and result in a large amount of information unnecessarily being stored in the DLP system. There may be opportunities to disable or tailor security policies to appropriately balance data loss prevention and litigation risk goals while ensuring the organization appropriately retains any information under legal holds.

Because the security policies an organization enables may change over time, there should be an ongoing conversation with information security personnel concerning the type of communications the organization is monitoring and how changes to the enabled policies are tracked over time.

What information is being saved within the DLP system?

As mentioned earlier, an organization may have a DLP system that captures all monitored communications or only those monitored communications that trigger a security policy violation. It's helpful to understand how and where the monitored communications and policy violations are stored.

Some DLP systems have multiple databases, such as a capture database (where all monitored communications are stored), an incident database (where policy violations are stored), and a case database (where cases containing multiple policy violations are stored), all of which could

contain information that might be subject to legal holds.

It is also important to understand whether DLP systems routinely automatically purge stored information and, if so, how often or under what conditions (i.e., when information exceeds a certain age or volume).

Is the DLP system backed up? Some organizations back up only the DLP system itself, but others also back up the communications the DLP system is capturing and storing. If the latter is the case, it's important to know how long the communications backups are saved before being recycled.

If an organization operates in or does business with other countries, it should con-

sider international data privacy issues with respect to the communications captured and stored by its DLP system. For example, if a customer in France sends the customer service department an e-mail inquiry, and a copy of that e-mail is captured and stored in the DLP system, French data privacy regulations must be followed.

For more information, review the Sedona Conference® Cross-Border Discovery Framework available at www.thesedonaconference.org/dltForm?did=WG6_Cross_Border and Article 29 Data Protection Working Party's Working Document 1/2009 on Pretrial Discovery for Cross Border Civil Litigation (Working Paper 158) available at http://ec.europa.eu/justicehome/sj/privacy/docs/wpdocs/2009/wp158_en.pdf.

How long is such information saved?

An organization needs to know how long it is saving communications that it monitors and/or communications that provide evidence of policy violations.

For example, if a disgruntled employee sends an e-mail containing confidential business information from work to a personal e-mail account and immediately deletes it from his or her sent items mailbox, it may not exist in the organization's primary or backup e-mail system because backup systems generally run at night. However, depending on the specifics of how the organization's DLP system is configured and working, the e-mail may reside



Unnecessarily storing communications captured by current and/or predecessor DLP systems longer than needed creates the possibility that they are discoverable

there. It could be beneficial to have that evidence.

Unnecessarily storing communications captured by current and/or predecessor DLP systems longer than needed creates the possibility that they are discoverable and could become subject to legal holds – even if they are deleted from primary business systems.

In addition, certain laws in the United States (e.g., the Fair and Accurate Credit Transactions Act and the Health Insurance Portability and Accountability Act) and elsewhere (e.g., EU Data Protection Directive) require mandatory deletion of stale financial, medical, and other personally sensitive information when it is no longer needed for its particular purpose.

When implementing legal holds, is information being saved by the DLP system being taken into consideration?

A final important question to ask is whether the organization is properly taking the information saved by its DLP system into account when considering its legal holds and discovery processes. DLP systems generally are not designed for ease of conducting e-discovery. Search and targeted preservation capabilities are often limited. It is vital to understand what the organization's capabilities – or lack thereof – are in regards to searching, preserving, collecting, and producing information from its DLP system.

Communicating Effectively

An organization should know whether and to what extent it uses a DLP system and how this may impact legal holds and discovery obligations. Start the conversation today among information security, legal, and records and information management personnel. Answering the above questions will provide the requisite knowledge to determine when information in the organization's DLP system may be discoverable and will address whether and to what extent, if any, the organization needs to preserve, review, and produce that information.

Opening the lines of communication will make everyone involved better informed and help them work toward the end result: striking the delicate balance between retaining information for data loss prevention and investigation purposes and minimizing the associated risks and costs this poses from a discovery perspective. **END**

M. James Daley can be contacted at jdaley@daleylegal.com, Laura Clark Fey can be contacted at lfey@daleylegal.com, and Diana Fasching can be contacted at dfasching@daleylegal.com. See their bios on page 50.