



Leveraging Technology to Enable Automatic Legal Holds

Storing all business records
poses litigation risks, strains IT
dollars and resources

*By John Brigden, Esq.
Senior Vice President
Symantec Corporation*

Leveraging Technology to Enable Automatic Legal Holds

Storing all business records poses litigation risks, strains IT dollars and resources

Contents

Introduction	4
Routine document deletion policies: Proceed at your own risk	4
Backup is for recovery, not discovery	6
Retain what must be kept without keeping everything	7
Use technology to manage your technology	8
Shared roles and responsibilities	9
Selecting a vendor partner	10

Leveraging Technology to Enable Automatic Legal Holds: Storing all business records poses litigation risks, strains IT dollars and resources

Introduction

The explosive growth in electronic communications has resulted in a corollary growth of email as a primary source of legal discovery when organizations are faced with litigation. Recognizing that production of email in litigation or regulatory investigations is virtually inevitable given the predominance of email in the enterprise, organizations must now grapple with how to implement effective and efficient litigation holds in the electronic age. As recent high-profile cases demonstrate, traditional processes for litigation holds are being challenged as inadequate in the context of electronic communications. If a company uses technology to run its daily business operations, it will be expected to use similar technologies to search for, collect, and produce requested or subpoenaed business records.

So what is an in-house lawyer to do? A common approach taken by in-house legal departments when implementing a legal or regulatory hold on potentially responsive documents is to coordinate with the organization's IT department to retain all email records, backup tapes, and other data repositories in perpetuity. If a subpoena does arrive, the legal department can then require the IT organization to collect potentially responsive documents from the retained electronic records, which often means conducting electronic searches through huge volumes of data. This approach is impractical, time-consuming, and costly. Instead, the corporate legal and IT teams should work together—sharing roles, responsibilities, and budgets—to develop and implement an effective litigation hold procedure as part of the company's overall records management policy.

Routine document deletion policies: Proceed at your own risk

Until recently, companies were safe if they followed policies that called for the deletion of all email records after a short period, typically 30 to 90 days. The motivation for doing so was to hold down records storage and management costs, which continue to grow year over year. According to market research firm IDC, this explosion of corporate email represents not only an increase in the number of messages individuals send and receive, but also an increase in the size of email attachments. IDC reports that in 2004, the size of business email volumes sent annually worldwide increased by 47 percent over those of 2003, and more than doubled those of 2002.¹

¹ IDC, "Worldwide Email Usage 2005–2009 Forecast: Email's Future Depends on Keeping Its Value High and Its Cost Low." 34504, 12/05.

Leveraging Technology to Enable Automatic Legal Holds: Storing all business records poses litigation risks, strains IT dollars and resources

This growth in the number and size of email messages places an enormous strain on a company's IT resources, hence the reasoning behind a policy of regularly deleting records. However, several court rulings, most notably *Zubulake v. UBS Warburg, 2004*, have called into question this approach to records management because it often fails to take into account litigation process demands.

In *Zubulake*, the court ruled that a party must take affirmative steps to preserve documents, including:

1. Issuing a litigation hold at the outset of the litigation or whenever litigation is reasonably anticipated, such that all sources of discoverable information are identified and retained
2. Communicating the litigation hold directly to all key employees
3. Repeating the litigation hold instructions
4. Monitoring compliance with the litigation hold
5. Instructing all employees to produce potentially relevant documents in their files

Given these detailed preservation obligations, which are triggered whenever litigation is "reasonably anticipated," it is easy to understand how a routine deletion policy can result in the deletion of records that may be relevant to the litigation. Unless an organization is confident that it knows how to find and retain all records that may be relevant to a lawsuit or investigation at the outset of the matter, a routine deletion policy can lead to the destruction of that which, in hindsight, should have been retained.

The *Zubulake* ruling is not the lone decision establishing strict standards regarding the preservation of electronic records, but according to Timothy J. Carroll, who co-chairs the records management practice at the national law firm Vedder, Price, Kaufman & Kammholz, P.C., it is the most significant. "I believe the Southern District of New York judge who issued the *Zubulake* ruling did a tremendous job of clarifying the issues that had been contained in other cases around the country and incorporating them into her opinion," Carroll maintains. "It is probably the most fully developed opinion on this subject."

Leveraging Technology to Enable Automatic Legal Holds: Storing all business records poses litigation risks, strains IT dollars and resources

Backup is for recovery, not discovery

In response to *Zubulake* and other relevant rulings, legal departments across all industries sounded the alarm that email and other forms of electronic communication should be preserved and not destroyed. As a result, the pendulum swung from routine deletion policies to a “keep it all” approach in which Legal required IT to save all email, unaware of the enormous consequences that task presents to IT, both from a budget and a resources standpoint.

Typically, companies save email to backup tapes at regular intervals, such as the end of every business day, week, or month. This results in thousands, even millions, of email messages and attachments being kept on volumes of unindexed tapes, usually stored offsite. These backup tapes are excellent for their intended purpose: to enable disaster recovery of the data where an entire mailbox, system, or even data center needs to be recreated quickly. But backup systems are not designed for information discovery, where responding to a request means finding specific email messages and attachments based upon the context (e.g., date, sender, recipient) and content (e.g., keywords, subject line, attachments) of the information. Also, to keep storage and management costs in line, these tapes are usually recycled every few weeks or months. If these tapes become the “repository” of a company’s email, then tapes that may have responsive records must be suspended from recycling in response to a litigation hold. Failure to do so can result in documents that should have had litigation holds placed on them being lost forever.

Another source of unstructured email is employee laptops. These local email caches, known as .PST files in the Microsoft® Outlook® and Microsoft Exchange environments, pose a tremendous challenge during the legal discovery process. These files are highly susceptible to corruption and/or accidental loss (for example, if the laptop is stolen) or destruction (if the laptop crashes). Retrieving these .PST files means laboriously copying all business records from each laptop and then searching through them to find specific documents. Often this information is on the laptops of highly paid executives, causing inconvenience and lost productivity of key employees when the laptops are taken away and imaged.

Once the data is restored, it must then be extracted for presentation in court. Depending on the size and scope of the discovery request, this entire process can take days, weeks, or even months, especially when attachments in formats that cannot be searched electronically, such as .pdf, have to be converted to text-searchable files.

The costs of recovering email messages and attachments from volumes of unindexed backup tapes and individual employees’ laptops and desktops are enormous, and now that burden must be borne by the company served with a lawsuit or subpoena.

Leveraging Technology to Enable Automatic Legal Holds:
Storing all business records poses litigation risks, strains IT dollars and resources

Retain what must be kept without keeping everything

Notwithstanding the swinging pendulum of responses to the e-discovery conundrum, a pragmatic, reasonable approach to managing electronic information is available. The requirement to retain business records pertaining to ongoing or “reasonably foreseeable” litigation does not mean companies have to absorb these costs and preserve all records indefinitely. As the Sedona Working Group concluded in its *Best Practice Guidelines and Commentary for Managing Information and Records in the Electronic Age*, “an organization need not retain all electronic information ever generated or received.” Rather, the test should be whether there is any continuing value or need to retain it. Companies are obligated to maintain only those records that:

- Document a specific business-related event or activity
- Demonstrate a specific business transaction
- Identify individuals who participated in a business activity
- Support facts of a particular business-related event, activity, or transaction
- Are needed for other specific legal, accounting, business, or compliance reasons

At a minimum, therefore, what is clearly excluded from these retention requirements is the substantial number of email messages that are personal or spam. IDC’s research finds that in 2004, spam represented 50–95 percent of all inbound email, somewhat higher than 2003 levels and triple the 2002 levels of 15–30 percent. Preserving personal email and spam is unnecessary and a waste of money and storage resources. Moreover, transient electronic information without long-term value should be removed promptly from the system, once it is determined not to be subject to a legal hold.

The key to an effective and efficient records retention and deletion process, therefore, is the ability to automatically delete those email messages that do not need to be retained. Once the retention period applicable to those email messages that are not covered by a legal hold has expired, a company should have the infrastructure in place to delete them. Carroll says best practices require a company to preserve “record email” in accordance with their overall records retention schedules, and retain “non-record email” for only a short period. Regularly disposing of “non-record email” after 60–90 days reduces a company’s document management and storage burden and minimizes litigation risks. As Carroll pointed out, this approach is widely accepted since the National Archives Records Administration and various states have adopted similar approaches for managing non-record, or transitory, email.

Leveraging Technology to Enable Automatic Legal Holds: Storing all business records poses litigation risks, strains IT dollars and resources

“The key is documenting the process,” says Carroll. “It doesn’t have to be perfect, but the program must be reasonable and have been adopted in good faith. If the court believes that your company has disposed of records you should have retained in accordance with a legal or statutory requirement, you will be deemed to not have acted in good faith. So it’s critical to assess where you are, what litigation hold program will work for your company, and what roles and responsibilities Legal and IT must share to preserve records and document the entire process.”

Use technology to manage your technology

Just as recent advances in electronic communications technology created the need to rethink traditional document retention policies, technology advances are also the key to tackling this challenge. Retaining only “record email” pursuant to a state-of-the-art retention policy that works in conjunction with a software-based email archiving solution minimizes storage costs while ensuring the preservation of records required for regulatory compliance and/or legal hold.

An effective email archiving system immediately and automatically indexes all messages passing through the email system (e.g., Microsoft Exchange, Lotus Domino®, Lotus Notes®), stores them in their original form (email messages and attachments) in a centralized repository with specified retention periods, and ensures the email is not altered or deleted.

The system should allow authorized reviewers to quickly pinpoint specific email required for litigation support. This reduces the time spent recovering requested email records from weeks to just a few days, saving the previously exorbitant costs of completely meeting the e-discovery request. The support of global marking schemes eliminates unnecessary duplication of a review effort when discovery requests overlap, as they frequently do.

An email archiving system also provides tangible benefits beyond achieving regulatory and e-discovery compliance. With an indexed online archive, customers can search available content using different keywords and search terms, including Outlook message categories. The Symantec Enterprise Vault™ solution indexes email, including attachments, and more than 255 file types. For example, the ability to search data based on Microsoft Exchange categories enables a law, accounting, or professional services firm to quickly recall all email messages as well as attachments across an organization that relate to a particular category or search term.

Also, by reducing the size of data stores in environments such as Microsoft SharePoint® Portal Server or Microsoft Exchange, organizations improve both the performance of primary applications and the speed with which they can protect the underlying data. Search tools within Enterprise Vault, such as the ability for users to search the archive, enable IT groups to improve their Service Level Agreements (SLAs) simply by automating many administrative tasks.

Leveraging Technology to Enable Automatic Legal Holds: Storing all business records poses litigation risks, strains IT dollars and resources

Finally, the archive acts as an online repository for older items that are moved from primary application storage (e.g., Microsoft Exchange Server) according to customer-defined policies. Archiving technologies that apply single instance storage and compression to files further reduce the footprint of data. By controlling the size of the message store, the applications and servers hosting them remain focused on real-time transactions. The online archive also enables customers to rationalize their storage resources and dedicate primary storage to dynamic and transactional data. Older, less frequently accessed content can be moved to a secondary or tertiary storage device, saving money for more strategic purposes.

Shared roles and responsibilities

So how does a company develop and implement a records management system that meets the needs of both Legal and IT? The first step is to get both sides in the same room at once. Too often, Legal is surprised by the records retention and deletion policies imposed by IT, and IT is surprised to learn certain records should be retained for compliance and/or legal reasons. The CIO's chief concerns revolve around technology issues such as information sharing, keeping the company's email system running without interruption, and disaster recovery, as opposed to the general counsel's priorities, which include the ability to safeguard and recover evidence.

"When we go in to help a client develop its email retention policy, we demand that both IT and Legal be present at the initial meeting," says Carroll. "We see that, often, IT and Legal personnel have never even met before."

Proactive coordination and planning among in-house and outside legal counsel and IT personnel are necessary to design a proactive approach to legal holds that is able to respond effectively when needed. It should include:

- A records management program that includes a litigation hold component to allow for the immediate suspension of the scheduled deletion of records, hard-copy and electronic, that may be relevant in pending or reasonably anticipated litigation
- The identity of employees to be notified of the litigation hold, and an acknowledgement procedure for affected employees
- Specific steps and assignments for preserving backup tapes, archiving email, and, if necessary, notifying third-party vendors
- A method to monitor compliance with any litigation hold in effect

Leveraging Technology to Enable Automatic Legal Holds: Storing all business records poses litigation risks, strains IT dollars and resources

- Periodic follow-ups with employees to reiterate the litigation hold instructions, and procedures for notifying new employees
- A procedure for rescinding the litigation hold, notifying necessary third-party vendors, and restoring the record retention schedule for disposition of records

In addition, funding for implementing an effective records management system should come from both groups' budgets. IT's budget is tied strictly to storage and other technology issues, while Legal's budget is more fluid in order to enable its response to litigation when the subpoena arrives. Managing the costs of proactively archiving and placing legal holds on specific records is easier if both sides work together and contribute budget dollars.

Selecting a vendor partner

More often than not, IT already has existing relationships with software and hardware vendors, and should take the lead in working with them to design and implement a records management and litigation hold system based on their concerns about storage costs, as well as the directives established by Legal. IT will then decide whether to leverage existing relationships or start the bidding process.

“This whole process doesn't have to be hard,” says Carroll. “Companies have become convinced that this is an overwhelming ordeal that cannot be accomplished, and that's simply not true if Legal and IT make the commitment to form a closer working relationship—sharing roles and responsibilities, as well as budgets.”

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world.

The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and Enterprise Vault are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft, Outlook, and SharePoint are registered trademarks of Microsoft Corporation in the United States and other countries. Lotus Domino and Lotus Notes are trademarks or registered trademarks of International Business Machines Corporation, used under license therefrom. Other names may be trademarks of their respective owners. Printed in the U.S.A.
1/07 11850168