



Building an ROI Business Case for Email Archiving

Redgrave Daley Ragan & Wagner LLP



Introduction

Over the past several years, the reliance that organizations place on e-mail as their primary form of business communication has grown exponentially. The role of e-mail has expanded from a convenient way to correspond within the organization to the predominant channel of communication for business critical information and official company records. As a result, email systems are often pushed well beyond their intended purposes and are forced to serve as storage devices for vast amounts of information.

The purpose of this white paper is to describe what organizations do in the absence of email archiving and how such practices can raise the risks and costs associated with data storage and electronic discovery in litigation. This paper will identify the potential cost savings that can be achieved in the IT and Legal departments when an organization implements an email archiving such as Symantec's Enterprise Vault as a solution to its data growth problem.¹

The Current Situation: Headaches for IT and Heartburn for Legal

This rapid and nearly unchecked growth of electronic data generated and stored on email systems has created significant challenges for organizations of all sizes. The need for added storage space for all of this data has strained the nerves and budgets of corporate IT departments, while the obligation to comply with new and sometimes conflicting regulatory requirements or to respond expeditiously to a subpoena or discovery requests in litigation has kept many lawyers awake at night.

Between the substantial burdens imposed on over-extended IT departments and the exorbitant costs associated with electronic discovery, many organizations have come to believe that "there must be a better way" of managing email messages. They are right. Implementation of an email archiving system that is configured to work with an organization's records retention policies, as well as its unique legal and regulatory profile, serves to alleviate the corporate-wide strain on time and budgets as well as reduce many of the risks and costs associated with having business critical information stored on email systems.¹ Organizations looking for a solution to unmanaged emails should consider the benefits of email archiving as a way to tackle the growing storage requirements, increased regulatory pressures, and growing demands and costs associated with electronic discovery.²

Consider these statistics:

- According to a 2006 Radicati Group Inc. study, there are currently about 1.4 billion

¹ Symantec has developed an ROI calculator in which an organization can input its own measurements regarding costs associated with data storage and/or responding to discovery requests in litigation and assist in determining potential cost savings to be achieved through the adoption of an email archiving system.

active email accounts in the world.³

- In 2006, approximately 171 billion email messages will be sent daily. About 30% of those emails will be legitimate traffic; 70% will be spam.⁴
- By 2009, it is anticipated that 331 billion email messages will be sent daily.⁵
- By 2016, the number of electronic records produced may double every sixty minutes, according to the Collaborative Electronic Notebook Systems Association (CESNA), and international electronic recordkeeping industry organization.

The Impact of Unmanaged Emails on the IT Department: Storage Overload, IT Strain and User Work-arounds

In a survey conducted by Kroll Ontrack of 177 email administrators who manage 250 or more mailboxes, 37% of companies reported that they store email only on the server. When an organization stores email in this manner, storage space is at a premium. As such, many IT departments set mailbox limits for their users in an attempt to reduce the amount of email to be stored. According to Kroll, 72% of the companies surveyed have established mailbox quotas.

Although setting mailbox quotas makes sense intuitively, it often leads to unintended negative results. Considering that a typical corporate user generates a total of 19.5MB of email traffic per day,⁶ users often run into their mailbox quotas and are prevented from sending or receiving email messages. As a result, some users delete important emails from their mailboxes to comply with the quota or they circumvent the mailbox quota entirely by creating personal .PST/.NSF files as a work-around.

Some of the problems with PSTs and NSFs:

- * increased IT storage costs and inability to safely identify and destroy documents that no longer need to be kept for legal or business reasons
- * increased risk of data loss and file corruption
- * increased e-discovery collection and review costs
- * increased risk of sanctions and penalties for failure to preserve and produce evidence
- * loss of user productivity



The deletion of emails or the creation of .PST/.NSF files often puts organizations at risk for loss of business critical information, noncompliance with regulatory requirements, noncompliance with records management policies (including deletion of unneeded documents and data), and data spoliation charges in litigation. Additionally, the proliferation and nature of .PST/.NSF files add to the costs and burdens associated with electronic discovery because they may be difficult to locate and collect, they usually contain substantial amounts of non-relevant or duplicative data, and their ad hoc nature creates pockets of unchecked data that may not be discovered until after a production deadline. An organization that (knowingly or unknowingly) retains a substantial amount of documents or data beyond its retention period will likely face higher costs and greater risks should that information be subject to discovery in litigation.

In an internal study conducted by DuPont, in responding to a discovery requests over a three-year period,

√ DuPont reviewed 75 million pages of text

√ Found that more than 50% of the documents that it reviewed were kept beyond their required retention period, and

√ Calculated that cost of reviewing documents past their retention periods was **\$12 million.**⁷

In addition to .PST/.NSF proliferation, organizations without email archiving systems typically rely on tape-based archives of their messaging systems. Such organizations will usually backup their data onto tapes at regular intervals and then recycle the backup tapes over a set period of time, or send them off-site for disaster recovery purposes. Backup procedures and backup tapes are generally designed for disaster recovery purposes (i.e., to allow an organization to function after unplanned events such as device failure or accidental deletion). Like email message systems, however, backup tapes were never designed for the purposes in which they are currently being used. As such, backup tapes do not, cannot, and were never intended to provide an easy, efficient and reliable method for searching and retrieving specific information by date, user or subject matter. Organizations that are forced to rely on backups as their historical archive often spend more time and money attempting to locate relevant data and expose themselves to greater legal and regulatory risk.

The Impact of Unmanaged Email in the Legal Environment: Higher Costs and Higher Risks



The costs associated with electronic discovery in litigation can be staggering. According to a study conducted by Socha-Gelbmann, spending on electronic discovery has doubled in the last few years and will likely continue to do so in the near future.⁸

- The average Fortune 500 company experiences 125 non-frivolous lawsuits a year.⁹
- A corporation with \$1.5 billion in revenues averages more than \$8 million per year in corporate litigation costs.¹⁰
- Organizations typically spend at least \$2-4 million in legal discovery costs for every billion dollars in sales.¹¹

According to 2005 survey conducted by the law firm Fulbright & Jaworski, nearly 90% of corporations in America are engaged in some type of litigation.¹² The discovery burdens associated with litigation are a growing concern among all organizations. In a survey of 840 U.S. companies, co-sponsored by the ePolicy Institute, 21 percent of respondents had had their employee email and instant messaging subpoenaed in the course of a lawsuit or regulatory investigation. This figure is up from 14% in a 2003 survey.¹³

Before Litigation Begins: The Duty to Preserve Information

For any company that reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put a “legal hold” in place that serves to ensure the organization preserves potentially relevant documents and electronically stored information. Without an email archiving system, an organization often provides notice of a “legal hold” to various employees, or potential document “custodians”, who may have relevant documents and data stored in their files or on their computer. The Legal Department often must coordinate this preservation obligation with the IT Department in an effort to identify and locate the potential sources of data and information and suspend any automatic deletion of relevant documents and information.

Despite these legal requirements, many organizations have failed to put a sufficient backup-and-restore procedure in place. In the past few years, numerous organizations have found themselves at the wrong end of a spoliation allegation and have been order to pay substantial fines or face other sanctions due to their inability to provide requested emails due to a failure to preserve or timely locate them.

- \$1.45 billion ruling against Morgan Stanley for being “grossly negligent” in failing to produce email and email attachments as well

as failing to locate potentially responsive back-up tapes

- \$2.75 million ruling against Philip Morris USA after it was revealed that 11 senior employees failed to preserve emails subject to a legal hold

After a Lawsuit is Filed: Costs Associated with Electronic Discovery Events

Once a lawsuit has begun, an organization responding to discovery requests in litigation must locate, collect, review, and produce electronic documents and data to the requesting party. In some cases, an organization must go through the additional burden of locating and restoring backup tapes that may contain relevant information. Many of these tasks are often handled by third-party vendors and outside counsel.

Depending on the number of document custodians in a particular case, the amount of data a custodian generates, and the possibility of resorting to backup tape restoration, the costs associated with each electronic discovery event (i.e., responding to discovery requests) can reach millions of dollars per lawsuit. For an organization that is frequently named in a lawsuit and engaged in multiple electronic discovery events, these costs can multiply exponentially based on: the number of lawsuits filed, the claims alleged in each case, the number of custodians from whom data must be collected, the amount of data to be collected, and the location and format of the data (e.g., is it stored off site on a backup tape?). For just one example, Boeing, which averages two discovery requests per day, estimates that it costs \$1 million for every 15 emails it has to find.¹⁴

Locating Data

In terms of locating data for an electronic discovery event, organizations are often faced with numerous types and formats of data that are stored in various information systems, platforms and departments across numerous geographical regions. Few organizations have the ability to search for relevant information enterprise-wide and much of the information created or stored today is not stored in a way that it can be quickly or easily searched. For many organizations, simply locating the data subject to a discovery request presents a significant challenge and can impose a substantial expense.

Collecting Data

If data collection for an electronic discovery event is performed “in-house” by the organization’s IT staff, the soft costs required for data collection can be substantial. They can include, but are not limited to:



- Time used by employees related to searching for relevant information from multiple search locations (e.g., personal computers, laptops, email servers, backup servers, archive servers, offline disk or tapes)
- Legal and IT management time and effort to strategize and oversee the discovery process
- Disruption of regular business activities
- Greater potential for unintentional data loss, modification or corruption

If the organization retains a third party vendor to collect the data, significant hard costs also may be incurred if the vendor charges for its employees' time by the hour, for expenses incurred in traveling to various collection locations, hardware used in the collection process, and for every GB of data collected in the process. The fees per gigabyte collected can be in \$500 to \$750 range, if not higher, and are often charged before any de-duplication process is employed.



Attorney Review

Only after the data has been located and collected can the review process begin. In the absence of an email archiving systems, attorneys may review vast amounts of duplicative and non-relevant information. While attorney review rates often vary by location, they often range between \$50-200 per hour. When the attorney review process is limited by time constraints imposed by delays that often accompany data collection and possible restoration, aside from paying attorneys hourly review fees around the clock, organizations also run the risk of missing a critical file or turning over sensitive or privileged information, and potentially creating additional legal risk and greater liability.

Processing for Production

The final step in an electronic discovery event is producing the requested documents and information to the opposing side. Although parties can agree upon the form of production, an organization often incurs additional costs paid to third party vendors related to production. These costs are associated with the need for scanning images, bates-numbering images, loading images onto CD Roms, and storing or “hosting” the images for ongoing use in the litigation. Many of these costs are driven by the number of images to be produced. Where, without an email archiving system, there are inefficiencies throughout the prior steps in the process, an organization is likely to incur greater production costs due to the presence of potentially duplicative or non-relevant images in its production set.

Backup Tape Restoration (if necessary)

In some cases, organizations may be required to restore data from backup tapes. In addition to the time that may be spent locating and collecting backup tapes,² manual tape restoration costs \$2,000 to \$5,000 per tape, resulting in total charges in typical litigation cases exceeding \$200,000 per case.

Email Archiving as the Enterprise-Wide Remedy: Alleviate the Pain, Save Money and Reduce the Risks

An organization without a messaging management system should consider implementing an email archiving system such as Symantec’s Enterprise Vault to protect

² Webcor Builders, a general contractor in the San Francisco Bay area which has about 350 email users, reported that it once tool nearly 60 hours to sift through old backup tapes in search of emails that had been requested in a lawsuit with one of its subcontractors. Now having implemented an email archiving system, Symantec’s Enterprise Vault, Webcor’s chief information officer stated that the same task would now take less than an hour. See “Send and Save”, Peter Loftus, The Wall Street Journal, September 19, 2005.



against the loss of business critical information and the imposition of fines or other sanctions for the loss of discoverable emails.

In addition to avoiding the negatives, email archiving brings along inherent positives. For starters, it allows organizations and their counsel to efficiently search for, retrieve and review relevant e-mail and other electronic information in response to discovery requests in litigation. Additionally, email archiving provides better controls to an organization to prevent the data from being modified, corrupted, or damaged at any point in the process.

As described below, the hard and soft costs associated with electronic discovery events are substantial. Implementing an email archiving system reduces the time spent and costs associated at each step of the electronic discovery process:

<i>Step</i>	<i>Without Email Archiving</i>	<i>With Email Archiving</i>
Locate	IT, Legal or a third party vendor must locate requested information in whatever form it exists and wherever it resides (e.g., on the application server, in a PST, on a back-up tape that may be stored off-site or unlabeled).	Scalable and secure, email archiving automatically captures and indexes messages and attachments, which leads to instant search and retrieval of content.
Collect	IT or third party vendor must collect relevant data remotely, if possible, or by going from custodian to custodian to copy relevant files.	Email archiving provides for single-instance storage to eliminate multiple locations required to be located and collected.
Review	Before production, attorneys review documents to assess responsiveness, privileges. Without an email archiving system, the potential for attorneys to review duplicative information exists. Reading through emails and files is often a tedious task that can be very costly, as the review is typically performed by	Email archiving can eliminate PST files such that locating and collecting email messages can be done automatically and remotely. Organizations can also ingest legacy data from backup tape (if needed) to create a historical vault to simplify future efforts. Production costs and review



	<p>in-house attorneys, outside counsel, or contract attorneys working at the direction of and under the supervision of counsel.</p>	<p>time are greatly reduced as duplicative data is eliminated from the archive.</p>
Production	<p>Once the above steps are completed, the images to be produced to the opposing side are processed. Often, a third party vendor will be used in this process and will bill by the amount of documents and data to be produced. Additionally, third party vendors often host the documents and data produced in the litigation and charge by the GB for hosting and storing such data.</p>	<p>Export to native file system and message formats (including MSG, NFS, HTML and PST) to third party source or review tool.</p> <p>Email archiving can provide “legal hold” allowing organizations to suspend destruction of specific items in cases until the matter is over if required.</p>
Restore, if necessary	<p>If necessary to go to backup tapes, once they are located and collected, they often must be restored to a reviewable format.</p> <p>Depending on the nature and location of the data, restoration can be extremely expensive and time consuming. In many cases, data restoration processes often take so long that attorneys are left with limited time to review and produce evidence to the requesting party.</p>	



As shown above, implementation of an email archiving system could provide substantial cost savings to an organization at every stage of responding to discovery requests in litigation. The need for outside vendors is reduced or eliminated and the amount of time spent locating, collecting and reviewing information for possible production is dramatically reduced. For organizations that are often faced with discovery requests, these benefits multiply.

Furthermore, with email archiving, once the litigation has concluded and there is no longer a business or legal reason to store email messages in the archive, such messages can be disposed of at appropriate intervals based on an organization's records management policy and litigation and regulatory profile. The time and cost associated with locating, identifying and subsequently destroying unneeded data and documents after lawsuit ends is greatly reduced with an email archiving system.

¹ An email archiving system automatically extracts messages, attachments and information about the messages from email servers based on predefined policies. The content is then indexed and stored in a read-only format for an appropriate length of time according to the organization's records retention policies.

² As stated by The Clipper Group, "email archiving offers a spectrum of benefits. Larger, public companies may turn to it for purposes of regulatory compliance and legal discovery, and then be pleased with the storage savings and increased reliability. Small-and mid-sized companies may look to it to address challenges of capacity management and backup windows, and then realize the serious business value of a full-text searchable archive." The Clipper Group Explorer "You Should be Excited about E-mail Archiving", April 7, 2006.

³ The Radicati Group, "Market Number Summary Update, Q1 2006"

⁴ The Radicati Group, Inc., Microsoft Exchange Market Share Statistics, 2006 at 13-14.

⁵ The Radicati Group, Inc., Microsoft Exchange Market Share Statistics, 2006 at 13.

⁶ The Radicati Group, Inc., Email Archiving Market, 2005-2009 (June 2005). Using comparison figures provided in Mary Mack, Esq. and Matt Deniston's book, "A Process of Illumination" (at 64), 19.5 MB of data is the equivalent 975 pages of paper.

⁷ DuPont Case Study: Attributes of an Effective Document Retention Program.

⁸ Socha-Gelbmann Independent Electronic Discovery Services Study, March 2003.

⁹ Renew Data, Proactive Preservation Management, Finding Best Practices from 2002-2004, at 4.

¹⁰ Fulbright & Jaworski, Second Annual Litigation Trends Survey, at 2.

¹¹ Cohasset/Symantec White Paper July 2006 at 21.

¹² Fulbright & Jaworski, Second Annual Litigation Trends Survey.

¹³ "Send and Save", Peter Loftus, The Wall Street Journal, September 19, 2005.

¹⁴ Byte and Switch Insider, Archiving, A Plan of Attack, 2005.