

# Choosing the Right Archiving Solution

**An Osterman Research White Paper**

*Published May 2009*

**SPONSORED BY**



## Executive Summary

---

According to an Osterman Research survey of IT decision makers conducted in February 2009:

- 57% of mid-sized and large organizations have a need to manage email server storage more effectively by offloading it to less expensive storage.
- 46% have a need to handle routine e-discovery requests.
- 42% have a need for their end users to recover their own missing, deleted or older emails.
- 34% have a need to extract old email and other electronic content for regulatory audits.

Further, the same survey found that only 29% of organizations actually have systems and policies in place to prevent employees from deleting content that should be retained on a long term basis, despite the fact that 56% of these organizations have been ordered by a court or regulatory body to produce employee email or instant messages.

The bottom line is that a large and growing proportion of organizations have a need to retain and access old email and other electronic content, but relatively few have systems in place that can index, archive and allow authorized users to search this content. Osterman Research has found that fewer than 50% of organizations currently have an archiving system in place. Most organizations, on the other hand, simply discard content that they should preserve; or they retain it using backup tapes, local message stores, file servers or other repositories that are difficult, expensive and/or time-consuming to access. It is also important to note that a backup system is not an archiving system – backups and archives are important and represent a best practice for organizations of all sizes and in all industries, but they are not interchangeable processes or technologies.

*Only 29% of organizations actually have systems and policies in place to prevent employees from deleting content that should be retained on a long term basis, despite the fact that 56% of these organizations have been ordered by a court or regulatory body to produce employee email or instant messages.*

### WHAT ORGANIZATIONS OF ALL SIZES NEED

All organizations should deploy an archiving solution that can help them to preserve electronic business records and other important content stored in email systems, real-time communication systems, collaboration databases, file stores and other repositories. A failure to preserve this content and make it easily accessible to those who need it can have serious repercussions on an organization's bottom line and its ability to conduct business in the future.

## ABOUT THIS WHITE PAPER

This white paper discusses the various reasons to archive email and other electronic content, and it provides some guidance about how to select the appropriate archiving system that will meet an organization's requirements. This white paper is sponsored by Mirapoint. Information about the company is provided at the end of this document.

## Determining Your Need for Archiving

---

Email archiving is an efficient and cost-effective way to address the legal and regulatory requirements of email and business data retention. Almost all organizations are required to retain data, whether they are public companies, small organizations or government agencies, and if they operate in certain industries. Archiving can also help companies tame email storage growth and free IT staffs from the time-consuming task of hunting for lost or deleted emails.

## LEGAL OBLIGATIONS TO PRESERVE DATA

Email contains a growing proportion of business records that must be preserved for long periods. Further, email is increasingly requested during discovery proceedings because of the Federal Rules of Civil Procedure (FRCP) and related issues. As a result, it is critical that email be made available for legal discovery purposes.

Formally enacted in 1975, the FRCP governs court procedures for civil suits filed in the US federal courts. It states that the discovery of electronically stored information, including email messages, instant messages, word processing files, spreadsheets, and so on, is now a mandatory point of discussion. When subpoenaed for information, the responding party has a maximum of 30 days to respond according to Rule 34.

The current version (2007) of the rules requires the responding party to “[... ] produce documents as they are kept in the ordinary course of business [... ]” Rule 34: 34(b)(2)(E)(i). This means that if the responding party uses data online and searches it electronically, they cannot supply that data as hard copy. The amendment also requires opposing parties to discuss e-discovery issues within 120 days of a lawsuit's filing.

When a hold on data is required, it is imperative that an organization immediately be able to begin preserving all relevant data, such as all email sent from senior managers to specific individuals or clients. An archiving system allows organizations to immediately place a hold on data when requested by a court or on the advice of legal counsel.

If an organization is not able to adequately place a hold on data when required, it can encounter a variety of serious consequences, ranging from embarrassment to serious legal sanctions or fines. Litigants that fail to preserve email properly are subject to a wide variety of consequences, including brand damage, additional costs for third-parties to review or search for data, court sanctions, directed verdicts or instructions to a jury that it can view a defendant's failure to produce data as evidence of culpability.

## REGULATORY OBLIGATIONS TO PRESERVE DATA

There are a large and growing number of regulatory obligations to preserve email. Some of the higher profile requirements are:

- **Sarbanes-Oxley Act of 2002**  
The Sarbanes-Oxley Act of 2002 requires all public companies and their auditors to retain such relevant records as audit workpapers, memoranda, correspondence and electronic records – including email – for a period of seven years. Company officers are obliged to report internal controls and procedures for financial reporting and auditors are required to test the internal control structures. Businesses have to ensure employees preserve information – whether paper- or electronic-based – that would be relevant to the company’s financial reporting.
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**  
All organizations operating in the healthcare field need to comply with HIPAA to ensure the safety of Protected Health Information. Organizations are required to protect the data from unauthorized users, as well as to retain for six years a broad range of documentation regarding their compliance.
- **Securities and Exchange Commission Rules**  
Members of national securities exchanges, brokers and dealers are obliged to preserve all records for a minimum of six years, the first two years in an easily accessible place (SEC Rule 17a-4). The affected records are broad and encompass originals of communications generated and received by individuals within financial institutions, including inter-office memoranda and internal audit working papers. Also included are automated messages sent to all customers, which could include email blasts. The records may be "immediately produced or reproduced on 'micrographic media' [microfilm, microfiche or similar] or by means of 'electronic storage media'.

Among the many other requirements for data retention are FINRA 3010, the Investment Advisors Act of 1940 (hedge funds), the Gramm-Leach-Bliley Act, IDA 29.7, FDA 21 CFR Part 11, OCC Advisory, the Financial Modernization Act 1999, Medicare Conditions of Participation, the Fair Labor Standards Act, the Americans with Disabilities Act, the Toxic Substances Control Act, the UK Companies Act, the UK Company Law Reform Bill - Electronic Communications, the UK Combined Code on Corporate Governance 2003, the UK Human Rights Act, Basel II, and the Markets in Financial Instruments Directive.

- **Financial Industry Regulatory Authority (FINRA)**  
FINRA is a non-governmental regulator formed in 2007 by the merger of various functions of the New York Stock Exchange and the National Association of Securities Dealers. FINRA manages a wide variety of rules that are imposed upon the more than 5,000 brokerage firms and nearly 675,000 registered representatives it oversees.
- **Model Requirements for the Management of Electronic Records (MoReq)**  
MoReq is a specification, originally developed in 2001, that defines the functional requirements for the manner in which electronic records are managed in an Electronic

Records Management System. MoReq has been used widely in Europe and has been updated with MoReq2.

The regulations above are but a very small sample of the regulations focused on data retention that impact archiving requirements and practices. Additional regulations are shown in a table later in this report.

## TAMING EMAIL STORAGE GROWTH

Organizations don't have to be Google to experience email storage growth. The dual drivers of cheaper disk storage and the increased size of email messages, thanks to attachments such as images and videos, is fueling the email storage explosion. Messaging storage is growing at an average of 31% annually, which means that a terabyte of storage today will swell to nearly 2.5 terabytes in just three years.

Just over one-half of respondents (52%) to a February 2009 survey of messaging decision makers by Osterman Research said they either had a need or a strong need to slow the growth of messaging-related storage. Increasing message size was the leading problem for organizations, cited by 54% of respondents – worse than spam or malware.

*Between 70% and 90% of all business correspondence in a typical company is email-based. From compliance with regulations to the role of email in legal cases, good email preservation is key to meeting a company's obligations.*

Archiving can be a very useful tool in reducing the volume of storage on email servers. One way to use archiving as a storage management tool is through the use of stubbing, in which email messages are replaced with “stubs” – roughly 10Kb links that point to content that has been migrated from users' mailboxes to the archive. When a user clicks on a stub, the message and attachment are retrieved from the archive and presented to the user as though the message were still in their mailbox. An alternative is to stub only attachments, leaving the message itself intact and replacing the attachment with a link. As with email stubbing, when a user clicks on the link, the attachment is retrieved from the archive. Another alternative is to migrate emails and attachments to the archive without the use of stubbing, allowing users to search for content directly from the archive.

Regardless of the particular method used, the advantages of using archiving to control email storage growth include:

- Large email messages and files are removed from live storage, resulting in faster backups and restores.
- IT can continue to impose quota limits on end users in order to keep email stores relatively small, but users rarely bump into these limits because content that consumes significant storage space is migrated from email server stores.

## TYPES OF DATA TO ARCHIVE

Roughly 90% of data that is provided by both sides in a legal dispute is email messages; the balance is made up of other files and, increasingly, instant messaging conversations. Here are the data types that should be archived:

- **Email**  
Between 70% and 90% of all business correspondence in a typical company is email-based. From compliance with regulations to the role of email in legal cases, good email preservation is key to meeting a company's obligations.
- **Instant messaging conversations**  
As instant messaging move from being a consumer-focused chat tool to becoming a useful business tool for internal and external communications, organizations must consider archiving these messages. A full 20% of respondents to the February 2009 Osterman Research survey said they had a need to archive instant messaging now, while 28% said they would have a need to do so in 12 months.
- **Files**  
Business files, such as Microsoft Office documents, have played a role as evidence in court. As these files are often contained within email messages as attachments, it is important that these files are archived in addition to the messages themselves. Files must also be retained to satisfy industry regulations, including HIPAA.
- **SharePoint and other collaborative data**  
Archiving can be used to address some of the reported limitations of Microsoft SharePoint, such as the lack of replication and the fact that SharePoint files and metadata are stored in an SQL database, which can increase backup and recovery times as more files are created. Further, archiving is useful to capture information generated by Lotus Sametime and other collaboration systems.
- **Other data types**  
Microsoft Exchange and Outlook PST files are both a blessing and a curse. End-users use personal .PST archives to address the storage limits on mailboxes, since they can create .PST files of old email messages and store them on their computers. However, doing so makes it difficult for IT staff to easily locate and retrieve such files for e-discovery purposes. Also, .PST files can become corrupted, losing valuable data. Archiving removes the need for .PST files.

## FREEING IT FROM EMAIL RECOVERY TASKS

Email archiving allows companies to let their end users recover emails themselves without the assistance of the IT department. A 2007 survey by Osterman Research found that IT departments face an average of 107 end-user requests for email search and discovery annually, or about two per week. The time spent on recovery is significant if businesses have to restore individual emails from backup tapes, which can be time-consuming to restore, and also have a high rate of failure and corruption.

## **BUSINESS INTELLIGENCE WITHIN EMAILS**

As employees rely on email as the primary communications tool it is important for companies to be able to extract business intelligence from email messages. Some archiving systems enable customers to quickly locate emails up to 15 years old and extract information, such as the identity of users' email correspondents and what information passed between them. This could be useful, for example, when a new employee is required to trace back correspondence between his or her predecessor and a customer. There are also sophisticated tools that can perform automated, large-scale retrieval and rigorous in-depth analysis of archived content.

## **DISASTER RECOVERY FOR EMAIL**

Many organizations may not traditionally include email in their disaster recovery plans because they believe it is too expensive or because they didn't consider email to be mission critical. But with employees relying on email as their primary form of communication and their primary file transport mechanism, enabling workers to quickly and efficiently gain access to their email archives and to resume communications with clients after an interruption is important.

There is a growing movement of vendors offering continuous data protection (CDP), also referred to as continuous backup or real-time backup. CDP automatically saves a copy of every change made to the data, allowing administrators to restore data to any point in time. The change is captured to a separate storage location and there are different methods of capturing changes depending on customer needs. CDP allows customers to protect against data corruption because it restores a previous, uncorrupted version of the data.

## **What are the Consequences of Not Archiving?**

---

As well as the risk of losing legal cases and the resulting damage to a business' reputation, business leaders and auditors can be fined and/or face a prison sentence for non-compliance of regulatory rules.

## **AN INABILITY TO SATISFY OBLIGATIONS**

The FRCP is but one example of how companies could fall afoul of regulations. The FRCP does not set the length of time for preservation of data. Organizations can continue to delete records in the normal course of business, but only those with a good data retention policy are well positioned to go through litigation with minimal damage. An organization without coherent preservation policies could find itself paying major penalties during the discovery process if it promises to produce data that it later discovers was already destroyed. Email archiving, among other things, helps organizations to focus on developing data retention policies.

## **LAWSUITS ARE VERY EXPENSIVE TO ADDRESS**

History has shown that lawsuits involving data retention affect companies of all sizes and that companies with poor data retention policies can endure severe consequences. The

sample cases below illustrate that both defendants and plaintiffs could lose cases and damage their reputations if they fail to produce data through e-discovery in a timely manner.

- **Zubulake v. UBS Warburg, 02-cv-1243, U.S. District Court for the Southern District of New York**  
The three-year Zubulake sexual discrimination suit is a landmark case in the United States for its wide range of e-discovery issues. UBS was required, at its own expense, to produce all electronic materials relevant to the case. During the e-discovery process, it was discovered that certain backup tapes were missing and that emails had been deleted. The court also found that UBS had failed to comply with its own retention policy. UBS was ordered to pay the plaintiff \$29.3 million.
- **Rhoads Industries Inc v. Building Materials Corp. of America, 2:070-cv-04756, U.S. District Court for Pennsylvania Eastern**  
This case is an example where the plaintiff's lawyers accidentally turned over more than 800 privileged emails when they provided the defense lawyers with copies of 78,000 emails.
- **Keithley v. The Home Store.Com Inc., 3:03-cv-00447, U.S. District Court for Northern California**  
In describing the defendant's approach to discovery as "lackadaisical", the court in this patent infringement suit found that Home Store.com failed to maintain a written litigation hold policy when backup tapes were written over. The defendant produced other data only when faced with possible sanctions. The judge also found the defendant failed to preserve evidence until one year after the plaintiff filed the complaint and three years after the defendant received a demand letter threatening litigation.
- **Qualcomm v. Broadcom 3:05-cv-01958, U.S. District Court for Southern California**  
The patent case between Qualcomm and Broadcom illustrates that plaintiffs could lose if they fail to produce evidence in a timely manner. Qualcomm attorneys failed to hand over data, which included 200,000 pages of emails and other correspondence, until four months after the trial. As a result, the judge held that several Qualcomm patents should be rendered invalid. Qualcomm was ordered to pay all of Broadcom's litigation fees of about \$10 million.

*History has shown that lawsuits involving data retention affect companies of all sizes and that companies with poor data retention policies endure sometimes severe consequences.*

## CONSEQUENCES OF FAILING TO MEET LEGAL HOLDS

If an organization is not able to adequately place a hold on data when required, it can encounter a variety of serious consequences, ranging from embarrassment to serious legal sanctions or fines. Litigants that fail to preserve email properly are subject to a wide variety of consequences, including brand damage, additional costs for third-parties to review or

search for data, court sanctions, directed verdicts or instructions to a jury that it can view a defendant's failure to produce data as evidence of culpability.

Also, while companies responding to a subpoena may argue that the information is inaccessible due to the burden and cost of producing it, the court may still demand it if it agrees that the requesting party has good cause to view the data. A poorly managed retention policy could also result in the inadvertent disclosure of privileged or proprietary materials to the requesting party.

## THE NIGHTMARE OF E-DISCOVERY USING BACKUP TAPES

Sifting through backup tapes for e-discovery is not only expensive, but it is also extremely time consuming:

- The first task is finding the tapes, and in many companies the tapes could be locked in a number of closets or storage lockers. Sometimes these tapes are missing labels and use a naming convention that is not known to anyone other than the person who labeled them – and that person may have left the company.
- Reviewing information on backup tapes is no easy task. For example, a compressed LTO-3 tape can hold 750 gigabytes of email, or approximately 56 million printed pages of text.
- The FRCP mandates that companies keep data from Exchange servers, backup systems, offsite tapes and .PST files. The cost of sifting through this media averages \$500 to \$1,000 per gigabyte, according to published reports. This could amount to a six- and seven-figure cost for even small organizations that could generate several terabytes of such data.

Email archiving enables organizations to store old emails, large attachments and redundant messages in a central repository that is easily accessible. This frees up space on existing servers for other business applications, and helps to speed up email server backups and restores. When used with e-discovery tools, email archiving software can enable organizations to search millions of email messages, calendar items and other messaging documents in a matter of seconds.

## SUMMARY OF RETENTION REQUIREMENTS

An abbreviated summary of data retention requirements is shown in the following tables.

### Key Data Retention Requirements North America

Regulation	Retention Rules
Sarbanes Oxley Act	Relevant records must be retained for seven years. Company officers are required to report internal controls and procedures for financial reporting and auditors are required to test the internal control structures. Businesses are required to ensure employees preserve information, both electronic- and paper-based, that would be relevant to the financial reporting processes. Fine and/or jail sentence of up to five years for non-compliance.

**Key Data Retention Requirements  
North America  
(concluded)**

Regulation	Retention Rules
Health Insurance Portability and Accountability Act	Safeguard the privacy of Protected Health Information. Non-compliance can result in a fine of up to \$25,000 per year for incompliance. Fine of up to \$250,000 and a maximum 10 years imprisonment for individuals involved in wrongful conduct with identifiable health information
Securities and Exchange Commission	Retain all records for a minimum of six years, the first two in an easily accessible place.
Federal Rules of Civil Procedure	No mandated length to which records must be retained. Responding party must respond within 30 days of a request for data is issued. Parties must present data as they are kept in the ordinary course of business. Rule 34(a)(d)(1)(B). Court-ordered sanctions are available for failing to preserve e-mails relevant to anticipated or ongoing litigation.

**Key Data Retention Requirements  
Europe**

Regulation	Retention Rules
Data Retention Directive	In response to terrorist bombings in London in July 2005, the European Union in December of the same year passed a data-retention directive requiring all telephone and Internet traffic be stored for up to two years.
Data Protection Directive	This directive was originally implemented in 1995 to protect the data of individuals and the free movement of such data. The rules are applicable not only EU businesses but also to anyone who uses equipment inside the EU to process data. For example, a U.S.-based online retailer serving customers in the EU would need to follow the regulation if they process personal data and use EU-based equipment to process that data (i.e. the customer's computer).

**Key Data Retention Requirements  
Asia**

Regulation	Retention Rules
Hong Kong Personal Data (Privacy) Ordinance	This regulation ensures personal data is accurate, up-to-date and kept no longer than necessary. Individuals have the right to access their data and to request that their data is corrected if they believe it to be wrong. There are a variety of consequences to non-compliance, including a fine of HK\$50,000 and a two-year jail sentence.
Hong Kong Code of Practice on Consumer Credit Card Data	In general, credit card issuers are required to keep consumer account data for five years from when the data was created, or 5 years after account termination.
Japan Personal Information Protection Act	This act ensures the privacy of information that is handled by government and private entities that collect or use personal information of 5,000 or more individuals. Organizations should ensure that personal data are kept secure from loss and unauthorized access and disclosure; notify individuals of how their personal information will be used; and to follow an individual's request for correction to their data. There are a variety of consequences to non-compliance, including a fine of up to 300,000 yen or a maximum six-month prison sentence for individuals who violate an order.

**Key Data Retention Requirements  
State, Provincial and Local**

Regulation	Retention Rules
California Education Code	The code mandates a minimum of four-year retention policy for records but one year for emails.
California amendment to FRCP	California has a different view to the judge in the Zubulake case who ruled that electronic information could be deemed inaccessible if the cost of recovery is too high and if the resulting information may not be useful. California's e-discovery amendments appear to presume that all ESI is accessible, leading lawyers to note: "California's deviation from the federal rules [...] indicates California's recognition that Zubulake is outdated due to technological advancements."
California Fair Employment and Housing Act (FEHA)	Code 12946 of this act requires employers and employment agencies to maintain and preserve any and all applications, personnel, membership or employment referral records and files for a minimum of two years. Also, companies involved in employment-based legal complaints are not permitted to destroy records until all appeals or related proceedings are terminated.
Florida 119.01(1)(e)	"Providing access to public records by remote electronic means is an additional method of access that agencies should strive to provide to the extent feasible. If an agency provides access to public records by remote electronic means, such access should be provided in the most cost-effective and efficient manner available to the agency providing the information."
Louisiana Public Records Act	Public records include "information contained in electronic data processing equipment".
Massachusetts SPR Bulletin No. 1-99, last revised May 21, 2003	The commonwealth requires all its government officials to retain all business-related email messages and metadata and that such messages are considered public records. Massachusetts also requires retention of the message's metadata. Messages have to be retained and printed and filed in accordance with the agency's paper filing procedures. Large messages should be stored electronically.
Missouri Sunshine Law	A request can be made of any email record if the email requested was focused on public business and was sent to two or more recipients.
Ohio Publics Records Act	Requesters can ask to see public records kept by government agencies. Such records can be stored in a variety of media including email, voice mail and video. The requester has the right to choose the medium -- paper, film, electronic file, etc -- they would like the record to be duplicated. This means the agency has to organize and maintain its records so the request can be fulfilled promptly and at no cost during regular business hours, or to provide copies at cost within a reasonable period of time. The Ohio Supreme Court determined that a public office has a duty to recover contents of deleted emails and provide access to them.
Oregon ORS 192.410(6)	Includes email as a public record for purposes of the states open records statutes, but voicemail is specifically excluded as a public record.

**THE COST OF IT INVOLVEMENT IN DATA RECOVERY**

IT staff spend a mean time of 5.3 person hours in a typical week recovering users' deleted or missing emails and files, according to a 2009 Osterman Research survey. A further 4.9 person hours are spent responding to discovery requests or other requests for emails or other data. That workload is on top of other email-related tasks that IT staffs must perform, such as email server backups, managing archiving systems, and other backup procedures.

By contrast, email archiving enables end-users to search for deleted or missing emails quickly from their Web browsers or email clients, without requiring assistance from IT.

## THE COST OF ADDING MORE STORAGE VS. EMAIL ARCHIVING

Even though storage gets cheaper every year, IDC estimates that the cost related to managing storage continues to be more than the storage itself. It estimates that the annual cost to manage the world's installed base of external storage is about 60% of all enterprise storage-related spending, including software, power, cooling, administration personnel, and services. It is also reported that storage commands at least 11% of IT hardware budgets.

By contrast, email archiving can reduce the total cost of ownership for storage by migrating data to lower cost storage systems and minimizing the amount of server-based storage required in email and other systems.

## Important Issues to Consider in Choosing a System

---

### DELIVERY MODELS

Among the many variants of email archiving systems available are four basic methods for deploying archiving capabilities:

- **Software: installed on in-house servers, managed by in-house personnel**  
The advantages of this approach are that it can be the least expensive option of those noted here, it provides a significant amount of flexibility, and it allows an organization to re-use existing hardware. The disadvantage is that this option can be more expensive to deploy and maintain, since an organization must configure servers, install software and manage both internally.
- **Appliances: deployed in-house, managed by in-house personnel**  
The advantage of this approach is that software and hardware are provided in a single, rack-mountable unit so that they work together seamlessly, and the cost of deployment is less than if software and hardware must be deployed separately. However, appliances offer somewhat less flexibility than internally deployed software and hardware and their cost for larger organizations can be higher than internally deployed software on a per user basis if an organization has excess hardware that it can repurpose. That said, much depends on the environment and appliances are typically less expensive than software-based solutions.
- **Hosted/managed service**  
The primary advantages of this approach are that there are virtually no up-front costs and, hence, no capital expenditures; very little IT involvement in managing the system; and immediate scale and high availability. Because these services are priced on a per-seat basis, overall archiving costs can be more predictable. Further, the deployment of additional services or the extension of retention time can be much simpler with the use of a hosted or managed service. However, a hosted/managed service can be (but is not necessarily) more expensive per seat for larger organizations.

- **Hybrid archiving**

This approach combines an on-premise and a hosted component, in which an on-premise appliance is used to encrypt messaging traffic between the customer's site and the provider's data center in which the data is stored.

## **MESSAGING SYSTEM PLATFORM(S) SUPPORTED**

An important consideration in choosing a messaging archiving system should include the email platform(s) that the system will support. Some archiving systems support only a particular messaging system, while others are system-agnostic, preserving all email content regardless of the platform. An organization that supports multiple messaging systems, or that may consider migrating to a new platform at some point, should seriously consider an archiving system that will support all of the platforms that generate email.

## **SCALABILITY**

Email and other content archiving systems must be able to store very large amounts of data. For example, consider an organization of 1,000 email users, each of whom generate 50 archivable messages on a typical workday will create a total of 13 million emails each year. If this content must be preserved for seven years, all other things holding constant a total of 91 million emails will be created.

*An important consideration in choosing a messaging archiving system should include the email platform(s) that the system will support. Some archiving systems support only a particular messaging system, while others are system-agnostic, preserving all email content regardless of the platform.*

## **HIGH AVAILABILITY**

Messaging archiving systems must capture all emails and so must be highly available. For example, if an email archiving system experiences downtime while the email system itself does not, then business records in email may not be retained as required by law, legal obligations or best practice.

## **EXTENSIBILITY TO OTHER, NON-MESSAGING REQUIREMENTS**

Email is, for the majority of organizations, the single most important repository of business records. However, there are a number of other repositories that must be archived for all of the reasons that are discussed in this report: legal and regulatory compliance, reduction of storage costs, etc. These repositories can include document management systems, collaboration systems like SharePoint or Sametime, CRM systems, inventory control systems and the like. It is important for an organization that is considering archiving to take a long term view toward the types of information it will need to archive and to consider the ability for its systems to manage this content moving forward.

## **EASE OF USE**

The ease-of-use for any archiving system is a very important consideration for a couple of reasons. First, in order to minimize user-training requirements, the interface should be as

simple as possible for IT to use when data is requested from the archive. More important, however, is that often non-IT groups (e.g., internal legal counsel, external legal counsel, paralegals, senior managers, consultants, etc.) will need to have access to the archive, making a minimum amount of training an even more important requirement as the number of potential users of the archiving system increases.

## BACKING UP THE ARCHIVE

Another very important consideration is backing up the archive so that archived data can be restored in the event of a natural disaster or other disruption to the primary archiving system.

# Moving Forward With Archiving

## JUSTIFYING ARCHIVING TO MANAGEMENT

One of the most important considerations in the process of selecting an archiving solution is to first justify the need for archiving to senior decision makers, since not everyone agrees that email and other content archiving is a sound business practice. For example, in the February 2009 survey noted earlier, 13% of IT decision makers felt that deleting all email content on a regular basis is the least risky option, since it reduces the likelihood that incriminating evidence will be found during legal discovery, a regulatory audit, etc.

Justification of email and other content archiving will vary depending on the industry in which an organization operates, the number of users it has, its corporate culture and other factors, but the following provide some level of justification:

- **Archiving is akin to life insurance**

While archiving may not be a critical requirement to a particular organization on a day-to-day basis for a particular organization, but a single e-discovery exercise or regulatory audit in which data can be rapidly gathered and assembled using an archiving system can save an organization from financial ruin.

For example, in June 2005 AMD filed suit against Intel and requested that email for a small number of Intel employees be preserved. The Intel employees in question were to copy the requested email to their hard drives. However, some employees did not follow instructions properly, resulting in the loss of email that should have been part of the discovery effort over a period of more than three months. The *Wall Street Journal* reported that Intel spent \$3.3 million to process tapes to recover the necessary emails. While Intel can clearly absorb this cost fairly easily, a smaller company could have been bankrupted by just one such incident.

*A single e-discovery exercise or regulatory audit in which data can be rapidly gathered and assembled using an archiving system can save an organization from financial ruin.*

- **Archiving can make users more productive**  
By automatically migrating content in the email store to an archiving system, employees can avoid the estimated 30 to 60 minutes per week they spend on staying under their mailbox-size quota limitations. This can save an estimated 25 to 50 hours per year per employee or \$900 to \$1,800 in employee productivity costs annually.
- **Archiving preserves corporate memory**  
In the absence of an archiving capability, content in email and collaboration systems either disappears as employees delete old content to make way for new, or the content dissipates into file servers, USB thumbdrives, local archives, employees' home computers, smartphones and other content stores that are largely inaccessible to the organization as a whole. Archiving capabilities will preserve this information and make it accessible to anyone who requires it.

Further, email archiving provides a range of capabilities that may or may not be required today, but that could be useful in the future. For example, an organization may decide it needs to archive email primarily for e-discovery purposes. However, by implementing an email archiving system specifically for this purpose from a vendor that provides extensibility of the system, the organization has also implemented a storage management capability that it will need two years into the future.

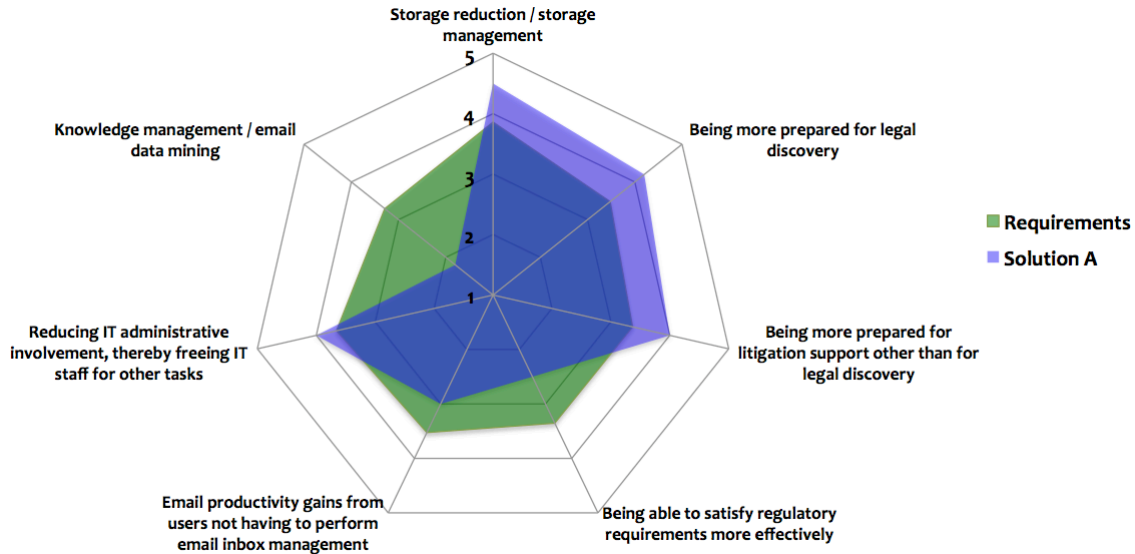
## GRAPHICALLY MAPPING YOUR REQUIREMENTS

As IT managers and other evaluate email and other content archiving options, it is useful to graphically map those requirements to the capabilities of the solutions under review. We recommend the following approach:

- Survey internal users to determine the specific applications for archiving and the applications for which archiving will be used. For example, an internal survey in a financial services company should reveal a very high emphasis placed on email archiving for regulatory compliance and legal discovery purposes, and much less importance placed on data mining and storage management.
- Plot these requirements graphically on a radar chart to create a map that shows the importance of various features relative to others. The chart will also reveal how “complete” a solution must be in order to satisfy that organization’s requirements.

For example, Osterman Research asked 138 mid-sized and large organizations the following question in a February 2009 survey: “On a scale of 1 to 5, how important are the following factors when evaluating the return on investment or need for an archiving solution for your organization, where 1 is ‘not important at all’ and 5 is ‘it’s very important’”. As shown in the following figure, we mapped the mean of the responses we received (shown in green) as the requirements for archiving among the organizations that we surveyed. Keep in mind that this represents an average of responses across all of the organizations surveyed and so will be less specific than if organizations in just one industry were surveyed.

### Sample Map of Archiving Requirements And a Solution's Ability to Meet Them



- We then recommend mapping the capabilities of each solution under review, also on a 1 to 5 scale, where 1 might be “not at all satisfactory” and 5 is “very satisfactory”, and superimposing it on the map of capabilities to determine how well each solution fits the requirements of the organization.

As shown in the figure above, the blue area represents a hypothetical solution’s ability to satisfy the various requirements of the average organization that we surveyed. Note that the hypothetical solution exceeds the organization’s requirements for storage management, legal discovery and reducing IT administrative involvement in the archiving process. At the same time, however, the solution falls short in the areas of knowledge management/email data mining, the ability to satisfy regulatory obligations and employee productivity gains.

- Any number of criteria can be added to a radar chart, including scalability, message throughput per hour, and the like.

The goal of this type of analysis is two-fold:

- First, it is important to establish a common set of criteria on which archiving solutions are evaluated. Each vendor will often have its own set of evaluation criteria and product performance specification – comparing these can be difficult and very time consuming.
- Second, a graphical representation that shows functional requirements mapped directly against each solution’s capabilities can be helpful in speeding the elimination process for solutions that simply will not satisfy an organization’s archiving needs.

As part of the process for evaluating various archiving solutions, a more detailed set of requirements, questions and criteria should be established for the needs of particular departments or functions, but the analysis discussed above provides a good starting point for evaluating competing solutions.

### FOCUSING ON THE LONG-TERM BENEFITS

An email and content management system is a long-term investment that will yield benefits for many years in the context of e-discovery, its ability to satisfy regulatory audits, improving storage management, and the like. As a result, it is incumbent on decision makers to consider the impact of an archiving system on these requirements for many years into the future. For example, an email archiving system implemented today will be able to satisfy e-discovery requirements imposed upon an organization seven years from now. The same archiving system may allow an organization to reduce its storage requirements by just 10% per year, but with a cumulative impact of reducing storage requirements by 77% during the same seven-year period. In short, unlike an email system that may be replaced every three or four years, an archiving system will have longer term and more cumulative impacts on an organization.

*An email and content management system is a long-term investment that will yield benefits for many years in the context of e-discovery, its ability to satisfy regulatory audits, improving storage management, and the like.*

## Summary

---

An archiving system designed to preserve email and other content for long periods of time can provide any sized organization with a diverse set of benefits, including the ability to satisfy e-discovery and regulatory audit requirements, the ability to migrate content from expensive storage on email servers to less expensive archival storage, and the ability to make employees more productive by eliminating their email management tasks, among other benefits. In order to select from among the growing variety of archiving solutions available, organizations should carefully define their current and anticipated requirements for archiving functions and then map each solution under consideration to these requirements. Doing so will allow an organization to understand how each solution can meet – or not meet – its requirements.

## Sponsor of This White Paper

---



**Mirapoint Software, Inc.**  
**1215 Bordeaux Drive**  
**Sunnyvale, CA 94089**  
**+1 800 937 8118**  
**www.mirapoint.com**

Mirapoint's unique appliance model simplifies the task of building and maintaining a Secure Messaging Infrastructure that can meet the new messaging needs of the enterprise. Our appliances deliver bullet-proof security and superior performance with five-nines reliability, while dramatically reducing the cost of enterprise messaging. When Mirapoint appliances work together as integrated building blocks of an enterprise messaging infrastructure, the result is even more powerful. They provide a centrally-managed messaging infrastructure that can meet today's needs for security, reliability and compliance, and address

new requirements like group collaboration, mobile access and instant messaging.

The Mirapoint ComplianceVault, when functioning with the Mirapoint Message Server and RazorGate appliances, passively and discretely copies all messages sent or received within an organization, indexes the messages and places them into a permanent archive. The message archive is backed up securely to tape and then deleted from the originating journal mailbox.

Mirapoint technology is proven, with over 100 million mail boxes served and secured worldwide for customers like Ford, STMicroelectronics, RSA Security, British Telecom, China Telecom, and University of Georgia.



**Mirapoint Platinum Partner**



Tel North: 0151 2031400 Tel South: 0118 9071600

Email: [Info@castleforce.co.uk](mailto:Info@castleforce.co.uk) Web: [www.castleforce.co.uk](http://www.castleforce.co.uk)

IT Security Reseller – Penetration Testing – IT Security Consultancy – IT Security Awareness Training

## Contributors to This White Paper

---

This white paper was written by Michael Osterman, principal of Osterman Research, Inc. and Linda Leung.

Ms. Leung is an independent technology writer with 20 years of experience reporting on the high-tech sector. She has held senior editorial roles in print and online publications in the United Kingdom and the United States, including *Computing* and *Network World*. She is based in the San Francisco Bay Area and can be contacted at [leungllh@gmail.com](mailto:leungllh@gmail.com).

© 2009 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.