Email Archiving: Common Myths and Misconceptions

White Paper

MessageOne, Inc.
11044 Research Blvd.
Building C, Fifth Floor
Austin, TX 78759

Toll-Free: 888.367.0777
Telephone: 512.652.4500
Fax: 512.652.4504

www.messageone.com

MessageOne®

Introduction

From the executive team to rank and file employees, email has become the enterprise filing cabinet of choice. Much more than mere correspondence, email is now used to send and store critical business documents; contracts, proposals, marketing plans, employment contracts and in general the intellectual work product of most companies.

To protect intellectual property and maintain compliance with rules and regulations, email must be preserved and carefully managed. Email archiving is no longer an optional service but a necessary component of a company's IT infrastructure. The failure to provide effective archiving can result in fines, lost legal battles, and the inability to survive through periods of crisis.

A recent Osterman Research Report noted that despite the many risks of ineffective archiving systems, 80 percent of organizations lacked a "true archiving" solution and 75 percent "are at risk of losing important business records contained in messaging systems." This research report also revealed several misconceptions about email archiving that often delay the purchase and implementation of an effective email archive. As a result, these companies are vulnerable to costly lawsuits, fines, and the cost and time necessary to search for email manually.

Five of the most common misconceptions about email archiving include:

1. My industry is not regulated, so I don't need to archive.
2. Email archiving will expose me to risk.
3. My backup system is my archive.
4. Exchange 2007 solves my email archive needs.
5. Hosted email archiving solutions are too expensive.

This white paper explores these common myths about email archiving, and provides guidance and solutions to solving email management and archiving issues.

Myth 1: My industry is not regulated so I don't need to archive.

Many companies believe that if their business is not part of a regulated industry, they do not have to worry about email archiving.

There is a common misconception that only certain industries are regulated. These typically include financial services dealing with the SEC and health care industries dealing with HIPAA regulations. What tends to be overlooked are all of the organizations that need to be in compliance with employee related regulations; Equal Employment Opportunity Commission, Americans with Disability Act, and the Fair Labor Standards Act. Also overlooked when considering regulated industries are the regulations that affect every day business practices including Sarbanes-Oxley (SOX) and the Federal Rules of Civil Procedure.

Of these, the recent changes to the Federal Rules of Civil Procedure (FRCP) have had the most widespread impact on email storage and retention policies. These changes are forcing many organizations to review and re-architect corporate e-Discovery and email archiving systems.

Impact of FRCP on Email Retention and Archiving

The Federal Rules of Civil Procedure govern the conduct of all civil suits brought in federal district courts. Many states have also implemented their own e-Discovery requirements based on these FRCP rules.

On December 1, 2006, the FRCP was revised to include new amendments that govern the collection and production of email and electronically stored information (ESI) as evidence. Several amendments to the FRCP directly impact email management. The following table provides a quick overview of the new amendments to the FRCP and their ramifications on business communications.

Table 1: **New Federal Rules of Civil Procedure Governing E-discovery**

Rule Number	Summary	In Plain English
Rule 26(a) 1 and 3	Electronically stored information is discoverable and lawyers must discuss ESI in the initial planning conference and specifically include it in the initial mandatory disclosures.	E-documents must be produced. You must know at the beginning of a case what relevant electronic information you have, where it is, and how hard it is to access.
Rule 26(a) 2	Disclosure can only be denied when not "reasonably accessible".	You must be able to quickly produce all relevant electronic information from active systems.
Rule 26(b)(2)	Addresses when cost or effort justify not producing documents.	You must know early in proceedings if documents exist that are costly to produce.
Rule 26(b)(5)	Protects against privileged information leaks.	Allows counsel to safely share information.
Rule 37(f)	"Safe Harbor" Addresses loss of evidence through purging.	You will not be sanctioned if you can demonstrate sound purging policies and good faith operation.

With the new FCRP regulations, it is almost impossible to comply with email discovery requests without a comprehensive email archive system that provides sophisticated tools to build accurate archives and complex e-Discovery search and retrieval capabilities.

These amendments create an environment in which CIOs and IT managers must collaborate with legal counsel, understand legal issues, and translate them into requirements and solutions for their IT infrastructures. The stakes of litigation are often high. Organizations that are unable to meet these new requirements may be penalized in court and will risk fines and unfavorable court rulings.

With an effective implementation of an email archiving system, retention policies can be set and automatically implemented. Data is never lost, and companies have robust search and retrieval functionality to meet the legal and compliance challenges facing all industries, today.

Myth 2: Email archiving exposes me to risk.

Some companies believe that saving email is tantamount to keeping a "smoking gun." Mistakenly believing that "what I don't save, won't hurt me" is no more effective than closing your eyes to make a problem disappear. Implementing the shortest possible retention policies – typically 30 or 90 days – across the organization does not yield protection from the threat of litigation nor meet compliance requirements.

While a message may be eliminated from corporate email servers, the probability is high that it lives on in the possession of the people who received or were copied on the email. Thus, deleting email with a short retention period policy can arm adversaries with critical information that doesn't exist in the company archive. At the very least, short retention periods increase the difficulty and cost of responding to e-Discovery requests.

Without an archive responding to litigation is costly

The inability to quickly produce email for litigation can be expensive. The cost of executing one large e-Discovery search from tape often surpasses the cost of purchasing an email archive solution. In Coleman (Parent) Holdings, Inc. v. Morgan Stanley and Co., failure to produce executive e-mails in a timely manner resulted in order to pay $1.45 billion in punitive and compensatory damages. In another recent lawsuit, the judge instructed the jury that they should consider an organization's inability to produce email as an indication that they must have something to hide.

CIOs, IT, and legal departments must work with departments across the organization to determine retention policies and schedules that best serve the requirements of the business. Laws and best practices are evolving and whatever archiving system is implemented, the ability to set multiple policies and change them as needed must be considered a requirement.

Myth 3: My backups are my archive.

Today, a majority of companies rely on tape backup systems as an archive. Tape backups are a snapshot in time and when used as a recovery archive, omit transactions from the point of failure to the last good backup. Tape is also susceptible to corruption. Often a recovery process requires loading several tapes before finding uncorrupted data. Unfortunately with each successive tape, the data loss window grows.

The time, cost and human resources necessary to restore and manually search through tapes – is very high. In the case of Murphy Oil USA, Inc. v. Fluor Daniel, Inc., email from more than 700 employees was requested. The email had been saved to 93 back up tapes and cost the organization six months and $6.2 million to restore. With an archive, not only would the cost of e-Discovery been greatly reduced, but the time needed to search and restore email could have been reduced from months to minutes.

Archiving systems with strong indexing and search capabilities provide a competitive advantage by enabling counsel to quickly assess the company's position. In a lawsuit, counsel can determine in minutes if there is a true problem in the email archive.

Implementing litigation holds

Another problem with tape backups masquerading as an archive is that it is extremely difficult to implement multiple retention periods. Archiving provides the ability to set and automate multiple retention periods and set Legal Holds in response to litigation – backup tapes do not.

A litigation hold orders all information relating to a dispute that is the subject of current or **'reasonably anticipated'** litigation to be preserved for possible production during litigation. Archiving stops the destruction of email in a centralized, programmatic way, allowing Legal Holds to be added and deleted as needed. Backup tapes and the manual sorting of relevant messages by users is not enough today.

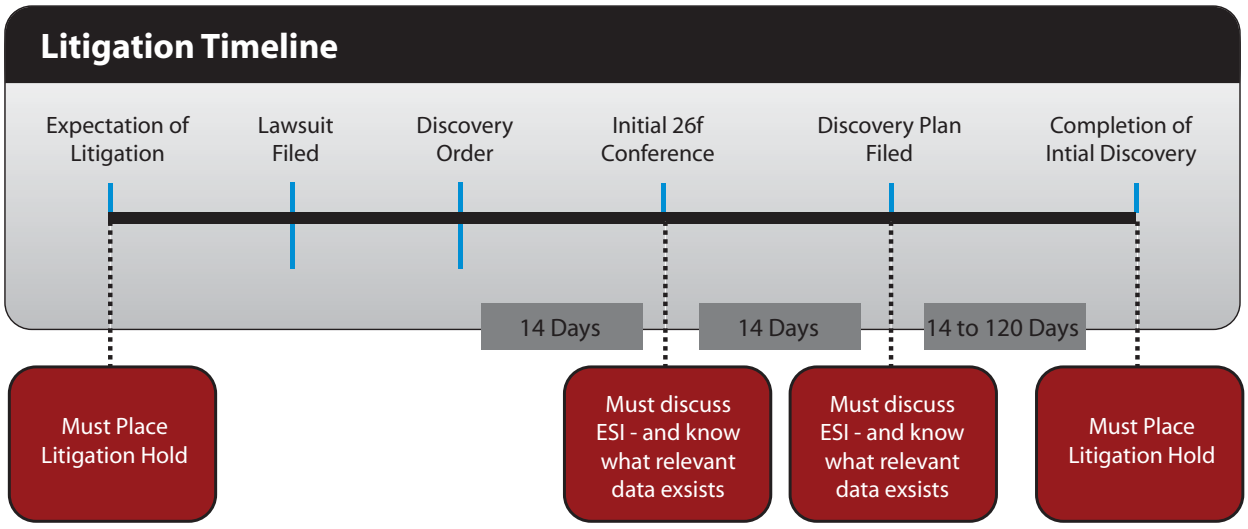
Myth 4: Exchange 2007 solves my archiving needs.

As the latest release of the most commonly used corporate email platform, Exchange 2007 represents the future of email. However, while Exchange 2007 provides a solid foundation, it does not provide an email archiving solution to meet today's email storage, compliance and litigation challenges.

Exchange 2007 provides managed folders for archiving that rely on end users to manually set individual archive retention periods – lacking the ability for centralized management of granular deletion and retention policies. Exchange 2007 also does not provide an effective mechanism for implementing and managing legal holds on individual mailboxes to prevent the deletion of messages. Effective archiving retention schedules and Legal Holds must be managed centrally, must be implemented automatically without user interaction, and must be based upon policies determined appropriate for the business.

Exchange 2007 also does not provide adequate e-Discovery capabilities or an effective global cross-mailbox search capability. Once a company is served, and e-Discovery requests are made, organizations have very little time to respond and produce required electronic evidence. As shown in Figure 2, typically between 14 – 120 days are available to respond to e-Discovery requests. Robust search and indexing capabilities are a critical requirement for archiving solutions.

Table 1: **New Federal Rules of Civil Procedure Governing E-discovery**



Exchange 2007 is an important step in the evolution of email management but does not include archiving capabilities adequate for most organizations. It also does not provide email continuity or protection during many types of local infrastructure outages. If it cannot be guaranteed that messages are not lost during a crisis or outage, the archive will not be complete and accurate.

Myth 5: Hosted solutions are too expensive.

The decision on whether to implement an archiving solution in-house or to use a managed or on-demand service is an important one. While each has unique benefits, the on-site solutions are susceptible to local infrastructure outages, are difficult to manage and can be expensive to modify as laws and best practices evolve. These problems are solved with on-demand, hosted services but many organizations have mistakenly assumed that hosted solutions were financially out of their reach.

This misconception fails to take into account the hidden costs of buying and implementing an in-house archiving solution. In-house systems are susceptible to local infrastructure outages, configuration errors, and require substantial maintenance. The IT staff has to perform patch management, upgrades, user-capacity management, server capacity management, and index maintenance. Expensive high availability and disaster recovery solutions must be also provided and these also increase maintenance burdens.

On-demand solutions are more cost effective because they provide a predictable cost structure, and the risk of managing and expanding the archive system is shifted to the service provider. Since the data is securely stored off-site, managed services have distributed, built in disaster recovery features to provide a more tamper-proof, and ultimately more accurate archive.

Email archiving makes sense in today's world

Email is increasingly more critical to organizations, it is more difficult to manage and the costs of losing email or an untimely response to a legal request are potentially disastrous. Effective archiving, however, results in confidence in regulatory compliance, a competitive advantage in legal discovery, and more efficient IT operations:

- **Regulatory Compliance** – Email archives ensure that email is retained for the time periods required by the needs of the company, and as specified by the regulations of the company's industry.
- **E-Discovery and Litigation Support** – The ability to globally search all email and attachments in seconds for email relevant to a pending legal issue provides management and counsel the ability to rapidly decide on a course of action. Millions of dollars in costs and months of effort in searching archived tapes can be avoided.
- **Storage Management** – With the rapid and continuing growth in email volume, stubbing old or duplicate attachments can minimize the growth of email stores and optimize the backup and operational performance of email systems.
- **Knowledge Management** – Email archives help employees organize and retain key information and documents, allowing for the self-restoration of inadvertently lost documents.
- **Disaster Recovery** – Email archives retain a copy of each email sent and received to provide business continuity and the ability to restore and recover lost email.

By choosing the right email archive solution, the organization can meet its archiving needs effectively and efficiently. With a strong email archiving solution in place, gaining control over corporate email will save time, money and many headaches.

MessageOne's EMS Email Archive™

MessageOne offers an on-demand archiving service, EMS Email Archive, designed to painlessly address the many challenges of archiving email for organizations of any size.

EMS Email Archive provides centralized control over retention and deletion policies, Legal Holds, compliance, storage management and e-Discovery without the risks of data loss or downtime:

- Centrally implement, record and change retention policies and Legal Holds
- Start with any number of mailboxes and grow as needed
- Execute complex e-Discovery searches in seconds
- Stub attachments to reduce data stores by up to 80%
- Integrate with Outlook and Active Directory to reduce costs and headaches
- Combine archiving and disater recovery to lower costs and increase archive accuracy
- Deploy in a day, zero maintenance, lowest TCO

Business practices and regulations continue to evolve, yet many archiving systems have fixed global retention policies that were built into the archive architecture. EMS' flexible policy engine is the only solution that enables companies to set retention an deletion periods and Legal Holds of any length; by user, group or server. Once set, EMS allows them to be changed at any time to meet changing needs.

EMS Email Archive securely stores single copy of each message for use in disaster recovery (DR), archiving, legal discovery, policy compliance and storage management. By unifying the storage and management of DR and archiving, EMS provides a more accurate, tamper-proof archive, without the costs and complexity of dueling retention policies, duplicate storage, and multiple high-availability solutions. The archive is always available and compliance policies are always working.

Once stored, EMS makes it easy to search selected mailboxes or the entire environment using any search criteria. Perform sub-second searches across headers, body, subject, file names, and over 370 attachment types to accelerate decisions with a sure and complete knowledge of the contents of all relevant email.

Duplicate and unused attachment copies make up as much as 80 precent of message storage. EMS can replace these in the primary email system with stubs to single copies stored in the archive. EMS Email Archive enables granular stubbing policies based on size, age, and type and these can be set for users, mailboxes, servers or groups. EMS is the first on-demand service to be fully integrated with Microsoft Outlook®; when attachments are needed they can be seamlessly retrieved from Outlook by clicking on the attachment name.

As an on-demand service, the costs for deploying and operating EMS Email Archive are known upfront with little or no initial investment required. As business needs grow, EMS can easily provision increased archiving storage allowing virtually unlimited mailboxes for any number of end-users without adding additional maintenance work for the IT staff. EMS is designed to meet the needs of the largest companies, but companies can begin with any number of users. Start with a key set of executives, an IT pilot, or a litigation driven Legal Hold; deploy in a day and grow as fast as needs change.

MessageOne saves money, reduces management headaches, improves employee productivity, and puts lingering archiving myths or misconceptions to rest.

Contact MessageOne Today

For additional information including pricing and a free demo, please visit **www.messageone.com** or call toll-free at **888-367-0777.**