



The Growing Email Archiving Dilemma

11 considerations for controlling your email environment

According to industry analysts, email volume in organizations is growing by more than 30 percent annually, and the average user receives 7MB of data per day via email. As a result of this growth, the handling of email has become a critical business, IT and regulatory issue—driving the need for email archiving solutions. Most organizations looking for an email archiving solution are motivated by four factors: mailbox/server management, compliance/records retention, eDiscovery/litigation support, and knowledge management/IP protection. In addition to these challenges, IT departments want to know how to control costs within the email environment, while keeping important data accessible for business, legal and regulatory users.

Table of Contents

Executive Summary	3
Archiving and Email Management	4
Four Major Requirements for Email Archiving	5
Mailbox and Server Management	5
Compliance/Records Retention, Regulation and Corporate Governance	6
Legal eDiscovery/Litigation Support	8
Knowledge Management and IP Protection	11
11 Considerations for Controlling Your Email Environment	12
Old Math vs. New Math	14

Executive Summary

Email has become the lifeblood of many business processes, from business communication to tech support to eCommerce. According to Gartner Research, email volume in organizations is growing by typically more than 30 percent annually, and the average user receives 7MB of data per day via email.¹ As a result of this growth, the handling of email has become a critical business, IT and regulatory issue, driving a need for email archiving solutions in many organizations.

In fact, email archives have become an intrinsic part of email architecture, so they need enterprise-ready resilience, policy-based controls, comprehensive metadata archiving and search capabilities. Each new requirement adds to the cost and complexity of these systems, and today the expanding requirements for eDiscovery in litigation and compliance are putting even greater importance and demands on email archiving.

With these escalating demands come new considerations for organizations when selecting email archiving solutions. While analysts talk about the break-even point between on-premise and Storage-as-a-Service email archiving solutions, the increasing demands on email archives are fundamentally changing the equation. Break-even calculations are often based on older hosted archiving models with limited functionality and high pricing based on very expensive storage.

Storage-as-a-Service email solutions built on the latest grid technology and sourced from the right vendor can satisfy new archiving demands both reliably and cost-effectively in ways that an on-premise solution cannot – with pay-as-you-go pricing, robust technology and expertise to help you meet emerging regulatory, legal and other requirements. These solutions must also be considered in the context of overall organizational email needs since the right archiving solution can simplify and strengthen your overall email management systems and processes.

¹Source: Logan, Debra. "Managing the Growth of Content and eDiscovery in an Uncertain Legal Environment." Gartner Summit Event, November, 21, 2008.

ARCHIVING AND EMAIL MANAGEMENT

Email management has become increasingly complex due to evolving data security, governance, continuity and other requirements. Over time, many organizations have added functionality to their original messaging platforms, often as discrete point solutions, to meet these growing requirements. Many IT departments are already finding these siloed solutions difficult to manage and upgrade. They are also finding it difficult or impossible to apply security, data retention and other policies consistently across this disjointed infrastructure; to retrieve complete data when needed for business purposes; or to provide continuous access to all of the email data in the organization.

The sheer volume of email today creates additional challenges for IT, such as how to control infrastructure costs while keeping important data accessible for business, legal and regulatory users. Storing large amounts of email on mail servers drives up the costs of storage infrastructure and adds to system maintenance chores. Large-scale storage is a function that mail servers have not been designed or optimized to carry out.

If the email management infrastructure is already straining, the requirements of email archiving will only add to these problems. As you begin to consider archiving solutions, begin with three overarching questions about your current email infrastructure:

- **How efficiently are you able to manage your current email systems?**

Complexity can increase quickly with an email archiving system. Your archiving solution should not create extra work for IT staff.

- **Are you applying policies consistently across your email infrastructure?**

Email policies are critical in meeting compliance and legal requirements. (In fact, compliance and legal requirements can change so quickly that many organizations find that they need expert help figuring out how to set these policies and implement them in the email system.) You should be able to quickly and easily apply security, data retention and other policies across your entire email management infrastructure, including archiving.

- **Are you accounting for data and metadata across all systems?**

For example, how many email management systems must IT interact with in order to understand all the metadata associated with an email? You should be able to quickly and easily retrieve email and all the associated metadata, whether it exists in your primary email system or in the archive.

If these areas are already a challenge, your organization probably needs a simpler, more cost-effective solution to your overall email management and archiving infrastructure.

FOUR MAJOR REQUIREMENTS FOR EMAIL ARCHIVING

A vast amount of formal and informal business information now exists in email systems, either as messages or attachments. Email has become a repository of organizational history and know-how that companies need to retain, access and search. The role of email as a repository is feeding a demand for email archiving driven, according to analysts, by four major requirements:

- Mailbox and Server Management²
- Compliance/Records Retention, Regulation and Corporate Governance³
- Legal eDiscovery/Litigation Support⁴
- Knowledge Management and IP Protection

Mailbox and Server Management

The purpose of email archiving is to retain email and its associated metadata for an extended period of time (as determined by your corporate data retention policies). Some IT managers try to use Microsoft® Exchange itself as an archive, but this approach is not efficient, safe or cost-effective. Exchange is not set up for efficient system-wide search and retrieval of email or metadata. Large mailboxes also cause degradation in performance of mail servers. On the other hand, if users run up against a mandated limit on mailbox size, many will save to a personal folder (.pst file) on a local disk. This can leave the only existing copy of sensitive corporate information on an easily read file on an easily stolen notebook computer that is nearly impossible to manage centrally.

On-premise archiving from the primary email server saves space, but it has tradeoffs. Adding an archival system to the in-house email system increases IT costs and complexity more than many organizations expect. Many first-generation, on-premise archive solutions are no longer functioning effectively because of the sheer volume of email, and access to that email has exceeded the design criteria for those systems.



²Source: IDC Vendor Spotlight. "Using a Hosted Service for Holistic E-mail Management." October 2008. (Sponsored by Mimecast.)

³Source: Couture and DiCenzo. "Outsourcing E-Mail Archiving, 1Q08 Update." Gartner Research: February 2008.

⁴Source: Logan and Bace. "The Emerging eDiscovery Market." Gartner Research: July 2007.

It can take at least as long to back up the archive system as to back up Microsoft® Exchange, so system performance is affected. Also, many of these systems are not architected for efficient search and retrieval and such delays can affect productivity.

In contrast, a good email archiving solution can protect information while simplifying mailbox management for users and mail server management for IT. An email archiving system that makes messages instantly and easily available through the normal email environment protects information, offloads the primary email system and promotes productivity, because users don't need to spend time worrying about which emails to save and which to keep.⁵

Compliance/Records Retention, Regulation and Corporate Governance

Regulations such as the Sarbanes-Oxley Act (SOX), SEC rules, GLBA and HIPAA in the U.S., and the Companies Act Combined Code, EuroSOX and the Financial Services and Markets Act 2000, the Data Protection Act and the Freedom of Information Act in the UK, require the protection and retention of various types of business records. Emails frequently fall into these categories. For example, the Freedom of Information Act in the UK requires records management as a corporate program that should bring together responsibilities for "records in all formats [including electronic records], throughout their lifecycle, from planning and creation through to ultimate disposal."⁶ National, state and industry regulations vary in the kinds of documents that must be retained and the required period of retention, as well as in other aspects. In many cases, the interpretation of regulatory requirements is unclear, and prevailing interpretations can be affected by ongoing case law. For example, many U.S. organizations are still trying to establish what it will take to achieve legal compliance with the revised Federal Rules of Civil Procedure, which took effect at the end of 2006.

Email archiving for compliance adds considerably to storage needs and it poses new requirements on information retrieval. Continuity is also critical because if the right information is not retained or available, the organization can be out of compliance.



⁵ Source: Cone, Edward. "Dealing with Data Overload." CIO Insight. January 27, 2009.

⁶ "Freedom of Information Act 2000," Lord Chancellor's Code of Practice, Section 6 of Section 46. 2009. www.justice.gov.uk/guidance/docs/foi-section46-code-of-practice.pdf.

In addition, archiving for compliance demands flexible, policy-based control over which emails are archived and how long they are retained. Many companies have not yet implemented policies around records retention due to changing legislation and case law, which makes it difficult to determine what has to be retained and for how long. If there is a policy that data should be retained for three years, then data should consistently be destroyed immediately upon that three-year expiration date so that the company shows ongoing compliance with their own records retention policy. Unfortunately, many organizations' policies are determined not by their business needs but by the limitations of their archives. If the email archiving solution has the capacity and flexibility to meet changing needs, and if the solution makes it easy to set and change policy, organizations can start immediately with a conservative retention policy and then adjust and refine it as requirements evolve.

Archiving can also provide information that helps to set corporate governance policies on email usage. For example, archive searches and logs might reveal patterns of behavior such as misuse of email communications. Archiving can then be used to enforce and protect corporate governance initiatives such as acceptable use policies for email. (In Europe and in the U.S., if an employee challenges action taken in response to a violation, you must be able to prove that the policy has been applied consistently in order for the action to be upheld. Even for internal disciplinary action, good quality evidence is needed to avoid lengthy employment tribunals or even legal action for unfair dismissal.) Archiving comprehensive metadata along with email makes it possible to show how policies have been applied.

In the case of a data leak, organizations need their email archives to identify the source and/or context of the leak. If the leak is malicious, archived metadata will make it possible to do forensic drill down, which can help with recovery and with possible litigation resulting from the breach.

Legal eDiscovery/Litigation Support

The Focus on eDiscovery

In many cases, and by law in some countries, litigants are now required to give discovery of electronically stored information (ESI), and email is a critical part of this because it is used to show timing, knowledge, motivation, intent, etc. Legal eDiscovery is an evolving requirement, and organizations need to plan their archiving to meet requirements not only in their own countries but also, in the case of multi-nationals, across the world.

Many organizations think about email archiving without thinking about the logistics of eDiscovery afterward. The assumption is that as long as the email is stored on some kind of media, it will be accessible later. Unfortunately, this is a mistake that can cost millions later on when the archiving medium proves inadequate to meet the needs of eDiscovery.

Evidential Quality

Use of an electronic document as evidence depends on the ability to meet evidentiary standards that include relevance, authenticity, hearsay and the original writing rule and on balancing probative value against unfair prejudice.⁹ Establishing authenticity and the chain of custody can be especially difficult with email because it is constructed of multiple components (headers, body and attachments), which are easily modified and because emails tend to replicate, leaving different versions scattered in different places (e.g., on users' desktops). In a traditional fragmented, on-premise environment, different systems, such as those used for perimeter security, can act on email independently, in ways that may alter its context or meaning.

You need to know what happened to the data so that you can establish ironclad authenticity and chain of custody. Without a well-documented chain of custody, an informed lawyer on the opposing side can make the case very difficult.

EMAIL AS EVIDENCE

Electronic information as evidence is governed by a diverse set of laws and requirements worldwide:

- While the concept of email as evidence has existed for some time, its use has become increasingly prevalent in the U.S. since the rules were defined in the 2006 modifications to the Federal Rules of Civil Procedure (FRCP).
- The FRCP closely mirrors the corresponding obligation in the UK, which can be found in Part 31 of the Civil Procedure Rules (CPR). British Standard 10008, effective as of December 2008, calls for “evidential weight and legal admissibility of electronic information specification.”
- Time requirements for eDiscovery also vary by country. In the U.S., the time allowed is 120 days to prepare for the “meet and confer” regardless of the complexity of the discovery.⁷ On the other hand, early access to the data can help a party state their case more effectively in the “meet and confer” session, which is often when the scope of discovery is determined.
- In the U.S., some eDiscovery requirements may be waived if the party from whom discovery is sought can prove that “the information is not reasonably accessible because of undue burden or cost”.⁸ In other countries where discovery rules are more ad hoc, eDiscovery can go on for years, tying up resources and incurring ongoing legal costs.

⁷ Source: Room, Stewart. “Email as Evidence: 12 Steps to Ensuring Good Evidential Quality of Email.” Mimecast, 2008.

⁸ Source: <http://www.uscourts.gov/rules/civil2007.pdf>

⁹ Source: Lorraine v. Markel (D Md.), opinion by U.S. Magistrate Judge Paul W. Grimm, May 4, 2007.

For eDiscovery, the archive needs to save metadata that establishes chain of custody in order to prove the authenticity of the email evidence. You should be able to show what retention and other policies were applied as well. Searches must be able to quickly and accurately find and identify various versions and copies of an email and all the relevant metadata. (Good metadata can also provide context that helps establish relevance.)

- **Search Precision and Speed**

Organizations tend to assume that eDiscovery will involve one wide-ranging query. In practice, eDiscovery should involve initial queries and then iterative drill down. If you are the plaintiff, you want to cast a wide net. If you are the defendant, you don't want to cast the net too wide and risk exposing sensitive information that may not be relevant. Strong, iterative searching helps your legal team quickly locate and assess the available information, so you can plan your position for the "meet and confer" in the U.S. or preparatory meetings in Europe. To enable this, the archive should allow very precise search criteria and have fast (seconds or sub-second) response to facilitate the assessment of data.



Search speed obviously affects user productivity (hence, labor and litigation costs) but it can also impact or even determine the ability to conduct an effective case. Fast, iterative searches for early case assessment make more effective use of your legal resources' time, improve the quality of evidence, and enable you to build a more effective case sooner. The faster you can locate the available evidence, the better you can prepare for, or even prevent, litigation. For example, imagine that during the early case assessment you discover that a rogue employee is culpable of wrongdoing. If your eDiscovery is fast and you can find this out on day one, you have time to build a case that distances the organization from that employee's actions or you can decide to settle prior to a costly litigation process. In other cases, you may be able to avoid legal action altogether by quickly producing contrary evidence that negates the plaintiffs claims.

- **Ability to Produce Deleted Emails**

Effective eDiscovery requires that the archiving system can still retrieve emails that have been deleted by users from the primary email system, along with their metadata and attachments – provided that the archived email is still within the time limit specified by corporate retention policies. In a recent case, a plaintiff claimed sexual harassment and produced email as evidence. The company asserted that the plaintiff's email evidence was taken out of context, but because the users involved had deleted their copies of the relevant emails, the company couldn't prove its case.

- **Cost of Servicing Requests**

When you consider costs, consider both user productivity in doing searches and the projected cost of storage, along with the usual IT outlays. eDiscovery for litigation is quite different from compliance.

Compliance normally involves archiving a known set of data, so storage and search needs are comparatively predictable, although expensive. Archiving for litigation, on the other hand, is protecting against the unknown. You could be sued by a business partner, a customer or even an internal employee, and what might seem an innocuous email today could prove to be a vital piece of evidence in that context. So, for eDiscovery purposes, you may choose to archive much more information and searches will tend to be ad hoc and wide-ranging. Your archiving system needs to support a flexible retention policy to meet evolving eDiscovery standards, and it needs to provide fast, flexible searches.

Knowledge Management and IP Protection

Your organization's IP flows through email on a daily basis, as messages, attachments and metadata. If you give people sub-second access to archived email, employees will come to use email as another content management system. And, unlike formal content management systems which tend to be used only for finished documents, email searches can be used to retrieve a wealth of ideas and details. Having instant access to historical email from within a familiar environment like Microsoft® Outlook® also changes the way people use and view email, making them more willing to track down details, clarify ideas and dig deeper into issues.

Archiving can also help avoid accidental deletion or loss of an email containing information that is important to workflow or IP protection.

For example, a high-tech company faced with a patent lawsuit used archived email authenticated through archived metadata to prove that they were first to come up with a specific product design.

As email becomes a repository for your organizational working knowledge, continuity becomes increasingly important so that users don't lose access to the stored information. An archiving solution that provides nonstop availability will help ensure users' productivity and business continuity and reduce calls to the IT help desk. Storage-as-a-Service archiving solutions may more readily facilitate continuity than having to replicate the archive in two internal facilities. In a continuity scenario, having access to both current and historical email is as critical as ensuring that new email continues to flow into the organization.

THE COSTS OF LITIGATION

According to a survey, litigation and costs are on the rise for companies of all sizes:

- **98% of mid-size companies had from 1-20 \$20 million lawsuits and the other 2% had as many as 50**
- **58% of companies surveyed had between 1 and 50 new lawsuits in 2007**
- **Almost 40% of the largest companies surveyed spent \$5 million or more annually on litigation**

Source: 2007 Fulbright and Jaworski Litigation Trends Survey

11 CONSIDERATIONS FOR CONTROLLING YOUR EMAIL ENVIRONMENT

The drivers outlined above define a set of eleven core considerations – taking into account the organization’s overall email management requirements and challenges – when choosing email archiving solutions. These considerations include:

- 1 Completeness of Archived Data**

The archiving solution should be able to store and retrieve all copies and versions of an email, along with associated metadata and attachments.
- 2 Search Quality**

Consider performance, accuracy and ease of use. Organizations are often surprised at the poor speed and effectiveness of the search capabilities of their archives after deployment. Often, pre-deployment testing is done with small amounts of data, and, as the archive size and user base increase, users and IT are dismayed by the time it takes to conduct a search and the even longer time it takes to extract files from the archive.
- 3 Ease of Use**

Email archiving solutions should integrate with the user’s existing email environment and tools, so that access and retrieval are done through the user’s normal environment (such as Outlook). The simpler and faster things are for users, and the less change they need to deal with, the more likely they are to comply with policies that protect the integrity of email. As every IT department knows, user unhappiness quickly translates to more work, costs and headaches for IT personnel.
- 4 Capacity**

Archiving systems must be able to manage, retrieve and deliver large volumes of data. Capacity planning for email archiving is difficult and is affected by growth in email volume and average size of email and attachments. Volume requirements can expand rapidly with new regulatory requirements, new legal interpretations, or policy refinements. This means archiving systems must be able to scale quickly.
- 5 Accessibility**

To ensure productivity and business process flow, users should be able to access the archive from anywhere they can access their primary email system.
- 6 Ease of Administration**

Archiving can add significantly to the complexity of email management systems if it requires administrators to learn one more interface. Redundancy requirements can add complexity, especially if both the archive and live email systems must be redundant. Long-term retention may also introduce problems with older data formats or platforms becoming obsolete, making recovery difficult or requiring costly data migrations that increase the risk of data loss. In general, the broader and more integrated the archiving solution is with email management functionality, the simpler it will be for administrators to manage.
- 7 Security**

The email archive should have role-based access controls and privilege levels to provide basic security, and the archive should be housed in a secure data center.
- 8 Confidentiality**

The archived data must be encrypted both at rest in the archive and in transit to and from the primary email system.

- 9 Integrity**
Data integrity should be maintained through cryptographic hashing to prove the data hasn't been tampered with and also through chain-of-custody metadata.
- 10 Availability**
Continuous availability can be ensured with an archive that includes multiple, mirrored copies of originals. (Mirroring is less vulnerable than traditional copying.)
- 11 Cost**
Cost comparisons should include both hard and soft costs (i.e., both capital outlays and TCO). IT organizations tend to underestimate the costs of email archiving, because capacity and other requirements can change so rapidly. To begin with, an on-premises email archiving system typically requires a database, a backup and replication server, a storage area network (SAN), archiving software and search software.

The initial estimates for storage and server hardware can quickly go by the wayside if slow backups or poor search performance start impacting user productivity and satisfaction and if legal counsel suddenly changes retention requirements and doubles the amount of information that must be retained (quadrupling storage requirements, when you consider redundancy). System management costs can also multiply as administrators have to upgrade and patch software as well as re-index the archived data.

The priority of these considerations will depend on business requirements, but all of them should be considered when choosing an email archiving solution.



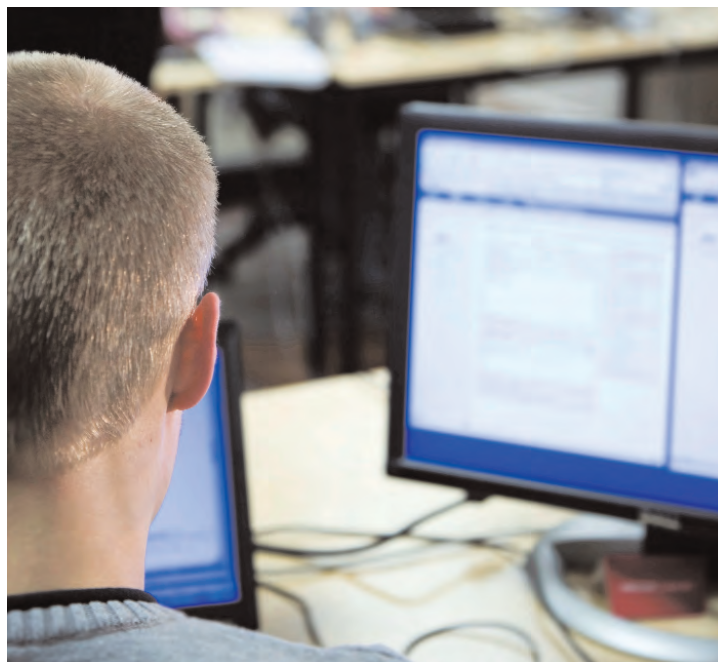
OLD MATH VS. NEW MATH

Most organizations consider some basic factors in deciding whether to implement an on-premises archiving solution or to choose a Storage-as-a-Service solution. For example, Ferris Research contrasts system installation and management complexity vs. in-house control, performance, privacy of information and TCO.¹⁰ As benefits of “as-a-Service,” analysts such as Ferris, Gartner¹¹ and IDC¹² list lower costs, lower IT complexity, better business continuity and security, shorter time to operation and sometimes the perceived legal advantage of a neutral third party holding your data. But even these traditional criteria are often incomplete, and organizations should also consider:

- The emergence of eDiscovery and recent legal judgments have put critical business importance on search speed and accuracy, which are difficult to achieve without integrated, purpose-built archiving solutions.
- With the growing reliance on email for eDiscovery and business continuity, email archives must be available at all times. You can be served with an evidentiary request even in the middle of an IT outage and you must keep archiving to maintain compliance as well. Getting your Recovery Point Objective¹³ (RPO) and Recovery Time Objective¹⁴ (RTO) to near zero is a very expensive proposition for in-house email archiving, whereas a Storage-as-a-Service provider with multiple data centers can provide flawless continuity without extra costs.
- The right Storage-as-a-Service vendor will provide rule-based access control and tamper-proof forensic audit logging as part of their service to help validate chain of custody and prevent and detect breaches.

The initial purpose of email archiving was simply to store data to meet emerging regulatory requirements. Some organizations interpreted regulatory requirements to mean that data had to be archived off-premises. But many companies built out their in-house storage infrastructure to archive email.

However, many of these organizations found they had seriously underestimated how long it takes to implement an on-premise archive. The amount of hardware and data, project costs and difficulty of search were all surprises. It is not unusual for a large organization to take six to nine months to implement an archive. (This doesn’t even count the whole budgeting and prioritization cycle.) In the meantime, legal and compliance risks can mount up. Even after an archiving system is deployed, costs can change unexpectedly.



¹⁰ Ferris Research, Report #798. “Email Archiving Solutions: On-Premise vs. SaaS.” October 2008.

¹¹ Cain, Matthew. “Email and the Cloud.” Gartner Research: June 2008. See also Couture and DiCenzo. “Outsourcing Email Archiving, 1Q08 Update.” Gartner Research: February 2008.

¹² IDC Vendor Spotlight. “Using a Hosted Service for Holistic Email Management.” October 2008. (Sponsored by Mimecast.)

¹³ The “recovery point objective” is the point in time to which you must be able to recover data as defined by your organization. For example, if your RPO is one hour, that means you must be able to recover all data to within an hour before the data loss. If your RPO is zero, that means all data must be recoverable: i.e., there is no level of “acceptable loss.”

¹⁴ The “recovery time objective” is the time within which a business process and data must be restored after system failure or disruption in order to avoid unacceptable loss of business continuity.

If the organization grows, or if regulatory or legal requirements change, the archive may need major upgrades to meet demands. If the organization shrinks or the requirements change, there is no way to reduce the sunk costs of an on-premise archiving system.

However, new developments in email archiving have fundamentally changed the equation. Multi-tenant Storage-as-a-Service archiving solutions are available with per-user, pay-as-you-go pricing. A good Storage-as-a-Service solution can remove the risks and complexity of archiving, showing you up front what kind of functionality and response you can expect and what it will cost. Implementation can happen quickly, often within hours, and an experienced, proven vendor can provide instant expertise to help your organization set up. They can consistently apply policies and procedures designed to meet emerging legal and regulatory requirements. (Always choose a vendor whose core business is email management and archiving and who has in-house expertise in policy management, compliance, and eDiscovery.)

The current challenging and litigious business climate demands that you have archiving solutions with optimal user productivity and flawless performance, but the financial climate demands that most organizations do this without making new capital investments. A Storage-as-a-Service provider with multiple data centers using the latest grid computing technology should be able to deliver:

- Always-on availability and continuity, without the costs of redundant in-house systems
- Blazing fast and accurate searches across large and growing datasets
- Complete, simple IT control over policy and security
- Transparent ease of use and accessibility for end users
- Zero capital outlay and predictable costs based on users, not storage
- Deployment within days, or even hours

These benefits come from a Web-based, massively parallel architecture and economies of scale that would not be cost-effective or practical for an on-premise solution. A Storage-as-a-Service solution also allows an organization's IT team to shift their focus to the wider business needs of their organization.

Taming Email Complexity and Removing Risks

Email archiving is a necessity, especially with the emerging requirements of eDiscovery, but it shouldn't become a drag on budgets or staff. Leveraging the latest technology and architected with all the functionality you need, a ready-to-use online Storage-as-a-Service solution from an experienced, proven vendor such as Iron Mountain can provide everything an enterprise needs, removing the growing risks and complexities of business email management with a single platform. Importantly, this Storage-as-a-Service solution can come at a fraction of the cost of alternative strategies, saving companies as much as 60% in ongoing costs.

Business is risky enough. The email archiving system shouldn't be a liability. The right solution will mitigate key risks and deliver business advantage with less cost and effort on your part.

ABOUT MIMICAST

Mimecast delivers SaaS-based enterprise email management for archiving, discovery, continuity, security and policy. By unifying disparate and fragmented email environments into one holistic solution that is always available from the cloud, Mimecast minimizes risk and reduces cost and complexity, while providing total end-to-end control of email. Founded in the United Kingdom in 2003, Mimecast serves 2,500 customers worldwide and has offices in Europe, North America, Africa, the Middle East and the Channel Islands.

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE:IRM) helps organizations around the world reduce the costs and risks associated with information protection and storage. The Company offers comprehensive records management and data protection solutions, along with the expertise and experience to address complex information challenges such as rising storage costs, litigation, regulatory compliance and disaster recovery. Founded in 1951, Iron Mountain is a trusted partner to more than 90,000 corporate clients throughout North America, Europe, Latin America, and Asia Pacific.

For more information, visit the Company's Web site at www.ironmountain.com.

Portions © 2009 Iron Mountain Incorporated. All rights reserved. Iron Mountain, the design of the mountain and Iron Mountain Digital are registered trademarks of Iron Mountain Incorporated. The reproduction of this white paper is limited to distribution by Iron Mountain Digital only.

Additional copyright and other rights worldwide in this white paper are the property of Mimecast Limited and those may only be reproduced with Mimecast Ltd.'s permission. Mimecast is a registered trademark of Mimecast Limited. All other trademarks and registered trademarks are the property of their respective owners.



IRON MOUNTAIN®
120 Turnpike Road
Southborough, Massachusetts 01772
(800) 899-4766

Iron Mountain Digital is the world's leading provider of Storage-as-a-Service solutions for data protection and recovery, archiving, eDiscovery and intellectual property management. The technology arm of Iron Mountain Incorporated offers a comprehensive suite of solutions to thousands of companies around the world, directly and through a worldwide network of channel partners. Iron Mountain Digital is based in Southborough, MA.