

The Email Management Crisis

New Research on Seven Critical Email Management Problems

EXECUTIVE SUMMARY

Email is one of the most effective and widely used methods of business communication surpassing interoffice memos, conference calls, and phone calls and exceeding faxes, direct mail and advertising in business-to-business communications. Over 70% of users confess to sending and storing confidential information such as sales proposals, marketing plans, competitor profiles, contracts and intellectual property via email. Users classify 56% of the email that they receive as either important or critical and spend approximately 34% of their work day using email.¹ By 2009, emails will double from 64.9 to 120 billion messages. These emails contain essential business information and must be archived and accessible at all times. Consequently, message stores are growing at greater than 30% per year and IT managers cite email archiving as one of their leading problems.²

Given the critical role that email plays, IT managers are realizing that successful email management is key for job security. The grand slam of email issues is performance, disaster recovery, compliance, and eDiscovery. Email systems were not designed for long-term storage and as a result, performance is negatively impacted if email storage thresholds are not managed properly. Disaster recovery and business continuity are cited by 70% of senior executives as their primary reasons for email archiving.³ When systems are down so is productivity, negatively impacting bottom lines. Compliance requires that retention policies be put in place enabling corporations to meet new regulations and mandates. With CIOs and CEOs being held liable for compliance, jobs and corporate well being are on the line. eDiscovery is the latest burden that CIOs are shouldering. Through 2010, companies that have not adopted formal eDiscovery processes will spend nearly twice as much on gathering and producing documents as they will on legal services.⁴

The email management crisis is comprised of these email facts:

1. Email is the most commonly used and most critical business tool.
2. Email is now discoverable and must be readily accessible.
3. Email must be saved and easily retrievable to comply with legal and regulatory mandates.
4. Email needs to be continually accessible so that business is not interrupted.
5. The increased use of email has resulted in more documents that need to be archived.
6. The increased use of email has created a greater need for data stores leading to a management nightmare that is growing out of control.

A solution must be found that enables IT to store all essential documents, produces documents on demand, reduces storage costs and is as automated and end user accessible as possible to minimize the demands on IT.

Iron Mountain along with MessageOne, an Iron Mountain partner, commissioned this research report to understand the growth, complexity, and importance of email archiving systems for organizations. This research shows that companies face issues at every level including the volume, content, management, storage, security, and retrieval of emails. On a broader scope, organizations must address compliance requirements, legal and eDiscovery needs, business continuity and employee productivity, storage demands and costs, and regulatory mandates.

This report explores the requirements of an effective email archive system and suggests integral components of a solution.

¹ Demir Barlas & Tamina Vahidy, "The Email Glut", Line56, January 24, 2006

² Troy Werelius, "Trends in Email Archiving", Computer World Storage Networking World Online, August 21, 2006

³ James Sherwood, "Disaster Recovery Cited as Strongest Driver for Archiving", CRN, October 12, 2006

⁴ John Bace & Debra Logan, "The Costs and Risks of eDiscovery in Litigation", Gartner, December 1, 2005

Email Trends: The Growth, Complexity, and Importance of Email within Organizations

GROWTH

Email is now a pervasive part of business life. The average user sends and receives 85 emails a day and spends 34% of their day working within email.⁵ Osterman Research has found that nearly 80% of organizations use email to handle business transactions and close orders. Due to the ease of email, many users rely on it not only for messaging but also for their primary filing and storage method leading to tremendous strain on network systems. IT departments are being pummeled from all directions with users demanding more space and executives demanding the curbing of costs.

COMPLEXITY

Managing, archiving, and restoring emails are of chief concern to executives. In the past, management issues were focused solely on the expense of storing excessive emails on the network. Now, management issues include limiting costs, assuring compliance with regulations, being able to track where emails are located, positioning organizations to respond to discovery requests, and locating specific messages that may only be stored in offsite backups or local PST files. Complicating things even further, the scope of email management has grown to include disaster recovery and business continuity, all of which must be considered when evaluating archiving solutions.

IMPORTANCE

Businesses are not the only ones to realize the value of email documents; courts also recognize their importance. Emails are of integral value for compliance and litigation. Litigation discovery is sometimes cast in the shadow of compliance, but should not be overlooked since it can have a much more significant impact. With the increasing use of electronic documents, emails are frequently the first targets of litigators.

Ready access to archived materials is critical since cost and difficulty in retrieving information is irrelevant to the courts. Failure to produce requested documents has resulted in severe consequences with CIOs and CEOs frequently being found liable.

⁵ Michael Osterman. "How Much of Email is Important?"; NetworkWorld, February 7, 2006

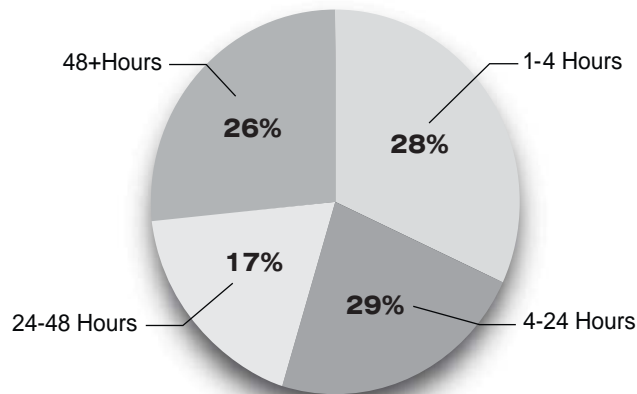
The Email Crisis: The Seven Critical Problems

PROBLEM #1: Email Disaster Recovery

For users of Microsoft® Exchange, there have traditionally been no good options for disaster recovery. While many solutions exist, they all have large gaps and drawbacks. As demand for constant email availability increases, tolerance for the shortcomings of these solutions has decreased.

Many organizations can manage when email is down for only a few minutes. Unfortunately, outages frequently last for much longer. With survey results showing that in any given one year period there is a 75 % likelihood of an unplanned email outage, the question becomes not if your email will go down, but when. The average duration of email outages varies from one hour to over 48 hours. Now that email is a business critical application, outages of as little as one hour are generally unacceptable.

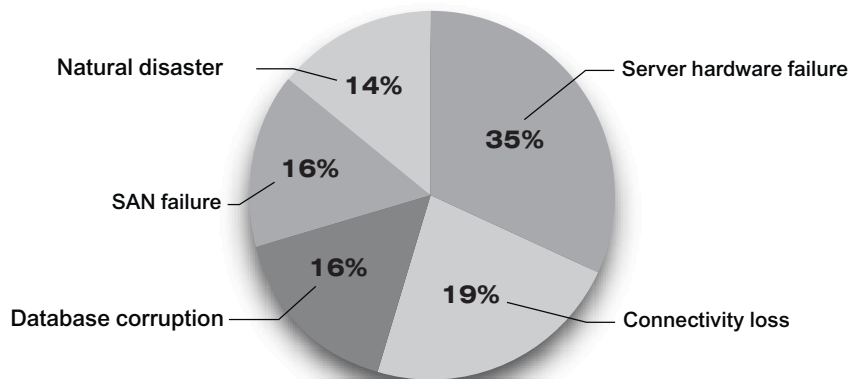
Figure 1: **Email Outages by Duration**



Source: MessageOne survey of email downtime

There are a number of reasons why email goes down. The majority are technological which is particularly troubling because these issues are the most difficult to prevent. Database corruption and SAN failure are the most problematic. Their failures result in long outages and force organizations to rely on periodic backup tapes to identify the last backup prior to corruption. While natural disasters are the least common cause of an outage, the outages that they cause last the longest and tend to be the most catastrophic.

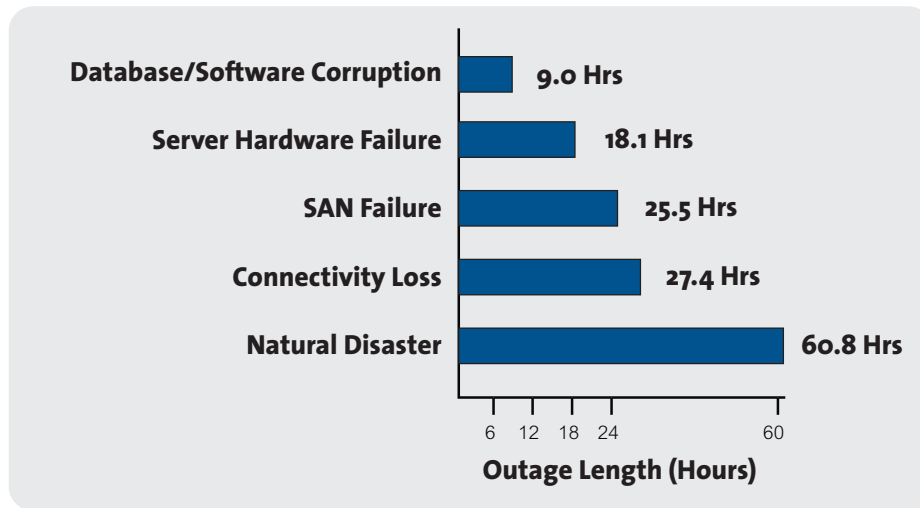
Figure 2: **Email Outages by Cause**



Source: MessageOne survey of email downtime

In reviewing the length of downtimes, it is important to assess how that downtime would impact your organization. Companies are few and far between who can function successfully for over 60 hours without email. As employees continue to become more vocal about demanding 100% uptime, their tolerance for downtime has decreased substantially. They are not productive and they become punitive and feel entitled to place the cause for this lack of productivity squarely on the shoulders of IT.

Figure 3: Downtime by Failure Cause



Source: MessageOne survey of email downtime

In most organizations, email recovery time objectives (RTO) are not aligned with users’ expectations. Typically, organizations settle for an RTO of 4-24 hours. Unfortunately, this number is out-of-line with executive expectations that email will always be available. A recent survey indicated that users found email outages become extremely painful after a period of about 10 minutes. Even in organizations where all stakeholders have agreed on a 24-hour RTO, a lengthy email outage may put IT jobs at risk.

While users expect a very quick RTO, the reality is that most organizations are not prepared to meet a 24-hour RTO for email. Organizations that rely on clustering, replication, and tape backup have no protection from data corruption, configuration problems, Active Directory® corruption, Windows® viruses and malware, or other failures. When these strike, there is no option but to rebuild from tape – a process that can take as long as 48-72 hours.

For most email administrators, disaster recovery remains painful, expensive, and fraught with potential risks. IT managers should implement a solution that provides continual email service, full recovery, and low RTO.

While organizations most often focus on the cost of large-scale recovery, it can also be very difficult and time-consuming to restore individual messages or mailboxes after end users have accidentally deleted them. To solve this problem, end user self-serve recovery solutions allow users to retrieve lost files independent of IT. This should be a required feature of your solution. By allowing end users to independently recover their files, you can reduce costs and the impact on IT. One company found that their average cost of a help desk call was \$17.23, with over 52,000 calls per year those calls translated to a cost of more than \$900,000.⁶ If the request to find an email requires restoration from backup tapes, the cost can easily exceed \$2,500 per request.

⁶ Roberta J. Witty, Kris Brittain. "Automated Password Reset Can Cut IT Service Desk Costs", Gartner, December 13, 2004

PROBLEM #2: Managing Complex Email Retention & Deletion Policies

Under most U.S. laws and regulations, email messages are considered business records. As records, they are subject to a variety of internal rules that dictate retention and deletion. IT must protect selected email records from destruction or manipulation to comply with legal and regulatory mandates. At the same time, they must delete unneeded emails to prevent unnecessary use of data stores.

In the current regulatory environment, there are complex rules that determine which business records should be retained and the appropriate timeframe before deletion. As these rules are applied to email, mail administrators need to find new technologies and processes to manage email retention and deletion in accordance with their corporate retention schedule.

To make things more difficult, there is no consensus between departments on how retention policies should be applied. Typically, there are four distinct interest groups, each with a unique perspective on email archiving:

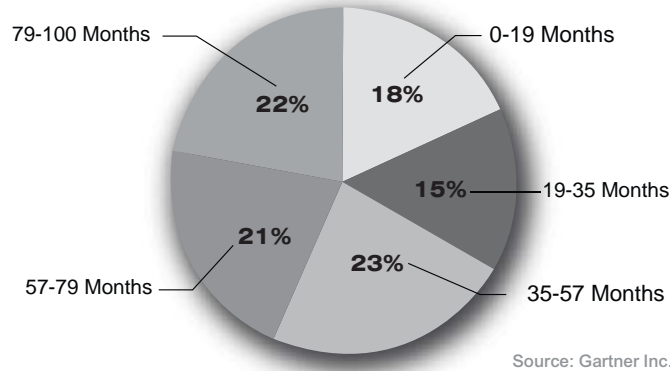
- **Users:** Believe that they need to keep everything, forever.
- **IT:** Need to balance the cost of storage with management and system capabilities.
- **Legal:** Prefer the most minimal retention possible to reduce risks and eDiscovery costs but often mandate longer retention periods to comply with regulations.
- **Compliance:** Desire long retention to assure that no legally mandated records are inadvertently deleted.

Figure 4: **Managing Complex Email Retention and Deletion Policies: 4 Distinct Approaches**

| | |
|--|--|
| 1. Delete Everything – All emails are deleted on a regular basis, normally 60 to 90 days. | |
| Benefits: A very inexpensive option as IT involvement is minimal. No staff confusion about what should be saved. | Problems: High likelihood that this option violates multiple regulations. Users will save emails in other locations representing a hidden cost in enforcing the email policy and greatly increasing the cost of discovery during litigation. Fines for non-compliance make this cost prohibitive. |
| 2. Delete Some Things – Certain messages are periodically deleted. | |
| Benefits: Reduced storage costs. | Problems: The “cherry picking” of selectively saving and deleting makes this a costly option. Non-compliance adds to enforcement costs. Organizations face an increased liability if they mistakenly delete things in violation of regulatory requirements. |
| 3. Save Some Things – This policy specifies what to save instead of what should be deleted. | |
| Benefits: Data that must be saved is not inadvertently deleted. As data is saved, it is also organized making it easier to search. | Problems: Discovery costs are still high as end users will relocate items scheduled for deletion. It is difficult to predict in advance what should be deleted. Extensive time and resources must be allocated for training, enforcement and auditing. |
| 4. Save Almost Everything – Delete spam and personal emails and save nearly everything else in a form that is easily retrieved and searched. | |
| Benefits: Compliance with regulatory requirements is assured. Litigation discovery is simplified and less expensive. Reliance shifts from employees to systems. Users rarely relocate information away from email. | Problems: Potentially harmful messages may be retained along with helpful ones. (Harmful emails are almost always saved anyway. Employees save damaging emails as a way of protecting themselves, the company, or for nefarious reasons.) Storage costs are higher than saving nothing. Ease of discovery, enforcement and compliance generally offsets the incremental storage costs making it less expensive than the options of deleting some things or saving some things. |

A recent Gartner survey illustrates the varying mindsets regarding the appropriate length of time for record retention.⁷

Figure 5: **Length of Time for Record Retention**



These varying lengths of retention may be partially driven by an organization’s classification of data. Many companies have varying retention periods for different types of data. ARMA International suggests four categories as a guide for retention policies:

1. **Vital Records:** Any records that an organization must have to conduct business and would not be able to replace if they were destroyed.
2. **Important Records:** Support an organization’s business operations and, if destroyed, would be replaceable, but only at great cost.
3. **Useful Records:** Are helpful in conducting business operations and if they were destroyed, would be easy to replace or the organization would not greatly feel their loss.
4. **Nonessential Records:** Have no predictable value to the organization and should be destroyed after their initial use.

Care must be taken to assure that retention policies also meet compliance needs. Retention requirements vary by act, state and type of business. Examples of retention periods include:

| Regulation | Type of Record | Retention Period |
|---|--|---|
| Age Discrimination in Employment Act | Hiring documents | One year from date of personnel decision |
| Age Discrimination in Employment Act | Employee benefit plans | Duration of plan plus one year |
| Americans with Disability Act | Personnel records of involuntary terminated employees | One year from date of termination |
| Fair Labor Standards Act and National Labor Relations Act | Payroll records, sales and purchase records | Three years |
| Fair Labor Standards Act and National Labor Relations Act | Interview records, ID of minority applicants | Length of training program plus three years |
| Occupational Safety and Health Act (OSHA) | Records of legally required medical exams | Length of employment plus 30 years or other specific OSHA mandate |
| Occupational Safety and Health Act | Records documenting exposure to hazardous materials | 30 years |
| Rehabilitation Act of 1973 | Records regarding handicap discrimination disputes | Three years |
| Title VII of the Civil Rights Act of 1964 | Personnel records regarding any discrimination charges | Through final disposition |
| Title VII of the Civil Rights Act of 1964 | All personnel or employment records | One year from date records were created |

Solutions must be implemented that allow a customized, automated retention and deletion policy. Additionally, users should be able to individually access stored emails to minimize their reliance on IT.

⁷ Debra Logan, Matthew W. Cain, "How to Formulate an Email Retention Strategy", Gartner, May 2006

PROBLEM #3: Complying with eDiscovery Requests

eDiscovery is any process where electronic data is sought, located, secured and searched with the intention of using it as evidence in a civil or criminal case. The discovery of electronic documents is becoming a critical trend in litigation. Many firms cite eDiscovery as their number one legal concern. As email is increasingly used in business transactions, the discovery of these e-documents grows in significance. The Chicago law firm Vedder, Price, Kauffman & Kammholz states that the cost of restoring email can be \$2 per message including the costs of review.⁸ Neal Rubin, senior litigation counsel at Cisco Systems, believes that the cost of eDiscovery is \$1,200 for every person who has information relevant to a case. In the case of *Murphy Oil USA, Inc. v. Flour Daniel, Inc.*, emails from more than 700 employees were requested. The emails had been saved to 93 back up tapes and cost the organization \$6.2 million to restore and six months of their time.

Electronic documents far out number paper documents in quantity and are much more difficult to recover due to volume, method of retrieval, and cost of restoration. In fact, the costliness and difficulty of producing e-documents has led some opposing counsels to begin using eDiscovery as a legal tactic, increasing their eDiscovery requests to place financial and hardship burdens upon defendants.

Adding yet another twist to the eDiscovery maze are recent changes to the Federal Rules of Civil Procedure (FRCP), specifically Rule 26, which became effective December 1, 2006. The FRCP and Rule 26 must be adhered to when producing evidence for most federal court cases. New amendments have direct impact on your email management plans. Rules of note include:

- **Rule 26(a)** stating that electronically stored information is discoverable. In the past, courts have held differing opinions on this with some excluding e-documents from eDiscovery and some including them. Now, it is clear that all e-documents are discoverable.
- **Rule 26(f)** stating that parties must meet early in the process to discuss eDiscovery issues. This amendment makes it important for organizations to be able to identify early on what they can and can not produce. By having ready access to all emails, counsel can be fully prepared for this initial meeting and in many cases, will be able to decide early on if they should settle or proceed with the case.
- **Rule 26(b)(2)** offering direction regarding e-documents that are too difficult or costly to access. When effective email management is in place, it allows you to quickly determine if there are some e-documents that you can only retrieve at great cost or effort. This amendment provides guidelines on when cost or effort can be used to justify not producing an e-document.
- **Rule 26(b)(5)** limiting the damage caused when privileged information is inadvertently provided to opposing counsels. This amendment serves as a safeguard to organizations who are trying to be thorough in their eDiscovery responses. It limits the impact of privileged information that is unintentionally shared.
- **Rule 37(f)** addressing the loss of evidence through routine email purging. A sound email policy is key, as it allows organization to illustrate their purging policy and demonstrate their compliance with all regulations.

Failing to follow these rules can result in significant fines, unfavorable court rulings, senior executives being held liable, bad publicity, and negative public opinion to name a few pitfalls.

Several organizations have attempted to cite difficulty in procuring e-documents as an excuse for failing to produce them. The courts are reluctant to accept that excuse and have enacted heavy penalties. In many cases, judges have viewed the lack of documentation as an expression of guilt.

Many courts are dictating that defendants shoulder the cost of electronic discovery. With amounts ranging from thousands of dollars into the millions, it is imperative that businesses produce documents quickly and thoroughly. The courts are relatively unconcerned about the cost of eDiscovery; their main focus is on the production of documents that can provide necessary evidence in determining their rulings.

⁸ Ameet Sachdev, "E-mails Become Trial for Cousins", Chicago Tribune, April 10, 2005

As a final complication, rules are not universal. Courts in Arkansas, California, Delaware, Florida, Illinois, Kansas, Mississippi, New Jersey, Texas and Wyoming all have state specific legal opinions about eDiscovery that may differ from those in the FRCP (Federal Ruled of Civil Procedure), which apply only to federal courts. However, the expectation is that Federal procedures will be adopted by most state jurisdictions.

With all of these pitfalls, how can you assure that your organization is prepared to meet eDiscovery needs? Two things are necessary:

1. **A strong retention policy:** It is imperative that you save the things that need to be saved and delete the things that can be deleted. Prevent emails from being saved in formats that are difficult to search (.PSTs or backup tapes) or your eDiscovery costs will skyrocket.
2. **Comprehensive tools for message search and recovery:** It does you no good to save documents if you can't find them and find them quickly. Your mail archive must be able to globally search current and saved emails and hundreds of types of attachments by user, location, and content so that you get the information that you need within quick time frames.

The eDiscovery process will never be painless. However, with a strong retention policy and effective search solutions, it can be far less costly and painful.

PROBLEM #4: Controlling Exchange Data Store Growth

According to Radicati Research, the number of emails is expected to double by the year 2009 growing to 120 billion messages. The size of emails is also growing due to increases in the numbers of emails with attachments and an increase in the size of those attachments. A recent Osterman survey found that with the average user sending 15-16 megabytes per day, a 5,000 person organization can experience 75 gigabytes of email daily. Consequently, the need for storage is growing proportionately.

The rapid growth in the size of message stores leads to the following problems for email administrators:

- **Slow Backup and Recovery:** More data means longer backup times and longer outages when email systems fail. It is not uncommon for larger organizations to face full recovery time windows in excess of 48-hours. Because the speed of the Exchange interface for data import and export is largely fixed, backup and recovery times are directly proportional to the size of the message stores. As email volumes continue to grow, this problem will continue to compound over the next few years.
- **Complex Maintenance:** As mail stores grow rapidly, administrators must manually balance users with different mailbox sizes and growth rates across different storage groups. This process is complex, risky, and time-consuming. In addition, the time required for standard maintenance processes such as defragmentation is directly proportional to the size of the message stores.
- **Expensive Storage:** As message stores grow, IT organizations must add expensive storage and highly skilled staff to manage complex storage environments.

IT departments have three options to address the rapid growth of message stores. Typically organizations address storage growth by purchasing additional storage capacity to expand dedicated message stores. This results in lengthier maintenance, more complex searches, and increased costs. The second option is to apply mailbox quotas that force users to delete messages and control the growth of their individual mailboxes. These quotas are very unpopular, and can lead to other problems such as users creating rogue .PST archives in violation of company policy.

The final option, which is rapidly gaining prominence, is the implementation of third-party storage management solutions. These new storage management solutions can reduce data stores by seamlessly moving bulky attachments out of Exchange and into lower cost and easier to manage message repositories. These solutions reduce data stores by as much as 80% while still providing end users with seamless access to their personal messages and attachments.

PROBLEM #5: The PST Time Bomb

In an effort to deal with the onslaught of email traffic, organizations have explored several options – setting mailbox limits, requiring users to archive their own emails, or deleting all emails after a specified period of time. None of these options have been effective. Users object to mailbox size restrictions and frequently begin underground archiving, refuse to archive emails, and put companies at risk with regulators holding them culpable for stored emails that were missed during legal discovery searches.

Underground archiving is a practice that occurs when end users begin creating archives in locations counter to email policy requirements. In many cases, this practice originated at the request of IT who had a main focus of freeing up space on the network. One of their preferred methods for underground archiving is the creation of .PST files. Today, most organizations have reversed these policies in favor of central control over email storage, which greatly facilitates search and recovery for legal and compliance requests. Today, the problem is so pervasive that 38% of IT managers list eliminating local .PST files as one of their top five email concerns.

With eDiscovery a major concern, IT now understands the importance of effective email management and of assuring that all emails are stored in one place according to corporate policy. Thus IT administrators find that they have now shifted their problem focus from IT to legal and compliance. The stop-gap measures of small mailbox sizes and scheduled deletions that IT implements to save time and money inevitably result in enormous costs later when legal and regulatory documents must be produced. Organizations with poor policies find that documents are frequently irretrievably lost, putting them at great risk. They must have solutions that give end users seemingly unlimited mailbox sizes, store documents in a central location, and provide easy to use search capabilities.

PROBLEM #6: The Security Administration Burden

Five years ago, eliminating spam and viruses was the top issue for email administrators. By 2005, most organizations had implemented solutions that effectively eliminated spam and viruses from their email environment. By late 2006, many of these solutions had become complex to manage and had failed to keep up with the rapid evolution of spamming techniques.

It's been very difficult for the majority of vendors to keep up with the rapid changes in spam techniques. In 2006, many spammers switched to image-based spamming techniques that render visible messages from multiple images that are rapidly animated or assembled when opened by an end user. Because these messages contain little or no text, and because these images are very difficult for spam engines to read, most email security solutions have seen their spam-blocking effectiveness significantly erode.

In addition, many solutions require significant manual administration by users and administrators to ensure effective security. Typically, administrators will need to continually update user accounts, lists of user aliases, global lists of trusted and blocked addresses and domains, as well as the specific filtering rules and thresholds required to determine whether messages are identified as spam. Similarly, end users must maintain their own block and safe lists to ensure that important messages from trusted senders are never identified as spam. This manual administration has resulted in significant costs and decreasing effectiveness for many organizations.

As spam volumes continue to increase at an alarming rate, the maliciousness of spam content has worsened as well. For example, new phishing threats have emerged where targeted communications are sent to company employees in an effort to steal login credentials to important corporate systems.

To combat these threats, companies are adopting a new generation of security solutions that scan hundreds of thousands of attributes of incoming messages and use machine-learning technology to reliably identify spam. In addition, the best solutions are now fully automated and integrated with the directory to block false addresses at the perimeter, to synchronize personal contacts with corporate safe lists, and to automate the process of adding and deleting users and user aliases. These third-generation solutions improve effectiveness while significantly lowering complexity and the total cost of ownership.

PROBLEM #7: Managing Wireless Devices

End users are no longer tethered to their desk and chained to their PCs for information. An increasing portion of employees are going mobile and relying on BlackBerry® devices and other wireless devices as their primary email connection. In fact, the growth of wireless devices is far outpacing the growth of traditional email. Mission critical personnel represent the greatest portion of wireless device users and they have a correspondingly strong demand for constant access to information. In many organizations, access for wireless users is far more critical than for any other group. Consequently, a downed email system has a much greater impact on this group. There are several reasons for this:

- A disproportionate number of key personnel (senior executives, IT, sales) are reliant upon their BlackBerry devices for their daily responsibilities and to deliver their corporate commitments.
- When emails go down, BlackBerry devices function as a metaphorical flashing neon light broadcasting “Failure, Failure.” Users attempting to send emails are confronted with a red “X” denying them that right. This icon makes it immediately apparent that there is a problem. As BlackBerry users are generally high profile users, their frustrations about down time are usually broadcast far and wide in an organization and receive high visibility. Most IT departments prefer to be recognized for their achievements and dread having spotlights shone on their failed systems.
- BlackBerry outages are particularly painful as their users are reliant upon them to do their job. When BlackBerry devices go down, productivity doesn’t just slow, it screeches to a halt. This is extremely problematic as these users represent the lifeblood of the company and when they stop producing they can bring the entire organization to its knees.

Most wireless platforms are not designed for high availability and offer no clustering or replication. Thus, it is incumbent upon IT to provide fail safe measures for assuring uptime.

Conclusions

The email management crisis is impacting all organizations. Users are sending more emails of greater length with more attachments. Sheer volume alone would be cause for alarm yet the email problem has been compounded as businesses rely on it for their most critical business functions; courts have declared emails a discoverable form; data stores spiral out of control; and management, archiving, and recovery are at their height of importance.

Corporate email systems such as Microsoft Exchange and Lotus Notes® were not designed as long-term message stores and were not built to address the challenges identified in this report. As a result, a variety of complementary solutions have come to market to fill these gaps and eliminate the key risks facing email administrators, IT managers, and CIOs. While solutions vary greatly, almost all are built around a central mail archive that stores a copy of all incoming messages and then applies retention and deletion policies specified by the mail administrator.

The best email management services and messaging archives are able to address all of the difficult problems identified in this report:

1. **Compliance:** Organizations need to assure that messages are retained in compliance with corporate and regulatory requirements, protecting them from costly fines and lawsuits.
2. **eDiscovery:** You must be able to meet the legal demands of opposing counsels, the FRCP, and other mandates. The ability to do so quickly and thoroughly saves you time and money.
3. **Storage Management:** IT teams need to reduce data store sizes to speed backup, recovery, and maintenance windows.
4. **Disaster Recovery:** The most powerful archives provide continuity during email outages and the ability to restore lost messages to the primary after a catastrophic failure.

These requirements are rarely isolated. More commonly they represent the scope of needs that IT must address. Therefore, organizations are seeking solutions that provide the following benefits:

- **Policy-based retention:** Enables complete corporate control over email retention and deletion. You must have the ability to customize retention periods for the organization, specific groups, and individuals assuring that emails are not retained for a longer period than necessary. Each area within your company is unique and their retention periods should be as well. By closely adhering to these varying retention periods, you can reduce your data storage demands and ultimately, your costs. Email management should be as simple as possible requiring you to delete or flag emails only once.
- **True storage management:** Your solution should reduce your data storage needs, reduce administration efforts, and lower storage costs. Emails should be “stubbed” where attachments are stripped off and stored in the archive until users choose to access them through Outlook®.
- **Sub second search:** You need to have the ability to search quickly, inexpensively and thoroughly. Searches utilize a lot of data and are very complex. You must be able to do granular searches to find what you specifically need.
- **Self-serve restore:** Users need to have direct access to archives so they can search and recover emails on their own and minimize the impact to IT. Solutions should have full integration with Outlook providing users with a seamless experience where they can search archives, stub and unstub attachments, and manage email security and spam from Outlook.
- **Full outage protection:** Archived data must be available at all times. You are archiving because your documents have value which means that you will need to access them. Their availability should not be reliant upon network availability.

There are a number of vendors offering email solutions. Few offer a comprehensive solution. Iron Mountain, a leader in email management, offers a bundle of email management services built around a central archive that addresses all of the problems listed in this report for as little as \$6 per user per month.

IRON MOUNTAIN'S TOTAL EMAIL MANAGEMENT SUITE: THE NEW EXCHANGE ARCHITECTURE

For CIOs and email administrators, email can be a no-win proposition fraught with risk. Too often, your job is on the line if you are unable to:

- Easily implement message retention policies
- Quickly and easily find required messages for legal, HR, or compliance purposes
- Prevent email & BlackBerry from ever going down
- Totally eliminate email data loss windows between nightly backups
- Control the growing size of email data stores
- Block new types of spam and viruses

While piecemeal solutions exist to solve many of these problems individually, the result is overly complicated, expensive, and difficult to manage and maintain. Iron Mountain's Total Email Management Suite is the first and only solution capable of addressing all of these concerns in a single, simple service.

Iron Mountain Digital helps companies eliminate email downtime and data loss concerns in their primary environment while also delivering the benefits of email archiving. With Iron Mountain's Total Email Management Suite, companies can easily archive messages based on company policies, improve the performance of production email systems, make email messages available during production outages, and enable rapid discovery of email for legal or HR purposes. Iron Mountain's Total Email Management Suite is the only email archiving solution that can ensure email never goes down (including BlackBerry devices) and can also ensure that there is never data loss in a disaster recovery situation. Iron Mountain Digital has been the choice of over a thousand companies and can be deployed in as little as one day.

As a managed service that fully integrates with Microsoft Exchange, Active Directory®, and Microsoft Outlook, the Total Email Management Suite enables a new email architecture that eliminates downtime, eliminates the risk of data loss, reduces cost, and shrinks maintenance, backup, and recovery times by as much as 80%.

IRON MOUNTAIN DIGITAL ELIMINATES ALL SEVEN CRITICAL EMAIL PROBLEMS

Iron Mountain's Total Email Management Suite includes a cost-effective email archiving service for email continuity, recovery, storage management, legal discovery, and compliance and a managed service for comprehensive email security.

Figure 7: Iron Mountain's Total Email Management Suite



As part of the Total Email Management Suite, the Active Archiving Service for Email securely stores email offsite based on specific email retention policies. Once email is stored, companies can ensure continuity and recovery, improve the performance of production email systems, save messages in compliance with regulatory requirements, and facilitate rapid discovery and production of email for legal purposes.

Iron Mountain's Total Email Management Suite is the only managed service capable of solving all 7 critical email problems:

1. **Email Disaster Recovery** – Iron Mountain's Total Email Management Suite is the only solution on the market that can ensure that companies will never lose access to email and that no message will ever be lost. In the event of an outage in your primary mail environment, the Continuity Service for Email allows users to activate a standby email system in less than 60 seconds and provide full email capabilities including direct access to historical email contained in the archive. Essentially, the service makes email outages invisible to end users and the outside world by redirecting Exchange and BlackBerry devices to the managed service.

Once your servers are restored, the Active Archiving Service helps recover any emails that may have been lost since your last good backup. This provides a "near zero" data loss window even though a company may only back up their servers to tape once a day.

Unlike high availability solutions built upon clusters, replication, or storage area networks, the Iron Mountain's Total Email Management Suite is not vulnerable to database corruption, Active Directory corruption, configuration errors, Windows viruses, or Windows malware. As a managed service built upon Linux®, the service is able to offer full interoperability with Microsoft Exchange while eliminating all of the dependencies on your primary infrastructure, staff, technology, and mail environment. Best of all, the service is a fraction of the cost of other less-effective solutions.

2. **Managing Complex Email Retention & Deletion Policies** – The Active Archiving Service for Email provides comprehensive management of email retention and deletion. The service allows administrators to set granular retention and deletion policies using any criteria. Unlike other solutions, retention periods can be set in days, months or years and can be varied user-by-user or group-by-group. Retention periods can even be set by distribution list. The service automatically ensures that messages are stored properly and deleted at the appropriate time. The Active Archiving Service makes it easy to comply with the many regulations that dictate email retention.
3. **Complying with eDiscovery Requests** – The Active Archiving Service makes it easy for legal counsel to search selected mailboxes or the entire environment using any search criteria. The service provides sub-second full text search and retrieval of all email and 370 types of attachments. Search results can easily be exported to a legal discovery system or to a dedicated Exchange mailbox for legal review.

Unlike other solutions, the Active Archiving Service allows companies to search for messages by content or user. Since the service is fully synchronized with Active Directory®, it's able to find messages sent and received by a user, no matter which email alias or address was used. The service also allows administrators to limit search privileges to a scoped review so that discovery searches by consultants or outside counsel are limited to relevant mailboxes and content.

4. **Controlling Exchange Data Store Growth** – The Active Archiving Service is the only managed service that is fully integrated with Exchange, allowing administrators to set granular attachment stubbing policies. When attachments are stubbed, they are removed from the Exchange data store but still accessible via the archive directly from the original Outlook message. With the service, companies can provide infinitely expandable mailboxes while simultaneously decreasing Exchange data stores by as much as 80%. The results include happier users, dramatically decreased backup, recovery, and maintenance windows, and provide improved Exchange reliability. The service allows administrators to set granular rules that determine when messages are stubbed and deleted from the primary system.

- 5. **Defusing the PST Time Bomb** – By using storage management to provide users with infinitely expandable mailboxes, the Active Archiving Service removes the incentive for users to create rogue .PST archives on their desktop. Since most organizations have .PST files throughout the enterprise, the service allows direct PST import into the central archive, providing central search and policy management as well as direct end-user access.
- 6. **Relieving the Security Administration Burden** – Iron Mountain’s Total Email Management Suite is the only solution on the market that can ensure that companies will never lose access to email and that no message will ever be lost. In the event of an outage in your primary mail environment, the Continuity Service for Email allows users to activate a standby email system in less than 60 seconds and provide full email capabilities including direct access to historical email contained in the archive. Essentially, the service makes email outages invisible to end users and the outside world by redirecting Exchange and BlackBerry devices to the managed service.

Unlike any other email security managed service, the service is fully integrated with Microsoft Exchange, Outlook, and Active Directory. It’s the only managed service to leverage real-time directory synchronization to fully automate user management, to synchronize personal contacts to ensure valid emails are never identified as spam, and to ensure that invalid addresses are blocked at the perimeter. In addition, the Security Service for Email allows users to manage safe / block lists directly from Microsoft Outlook.

- 7. **Managing Wireless Devices** – Iron Mountain Digital ensures that critical users will always be able to send and receive corporate email from their BlackBerry devices, even if your corporate mail system, data center, network, and staff are unavailable.

With the Continuity Service for Email, BlackBerry® support is seamless. When your email system becomes unavailable and the service is activated, it automatically activates client software on every BlackBerry device that allows email services to continue without interruption during any mail system outage or maintenance window. Users can also access their email inbox, calendar, and contacts as well as historical email through Iron Mountain Digital’s web-based client.

Iron Mountain’s Total Email Management Suite

Active Archiving Service for Email

The Active Archiving Service for Email provides email archiving policy management for eDiscovery, storage management, compliance, and disaster recovery.

Continuity Service for Email

The Continuity Service for Email is a standby email system that ensures that you never lose access to email and BlackBerry® – no matter what.

Security Service for Email

The Security Service for Email automatically eliminates spam, viruses, and unwanted content from your email environment.

CONTINUING INNOVATION FROM A TRUSTED PARTNER

Over the past 50 years, Iron Mountain has grown to be the world leader in records and information management. Unlike any other solution today, Iron Mountain's Total Email Management Suite provides a total solution for email and BlackBerry continuity, security, recovery, archiving, eDiscovery, and storage management.

For most organizations, email is the most important business application. For senior IT executives, email management brings many risks: outages are common, security threats are everywhere, data loss windows are significant, legal and compliance requests are increasingly complex, and server and storage performance challenges continue to escalate. Learn how Iron Mountain can eliminate these threats while lowering the cost and complexity of managing your email environment.

©2007 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks and Iron Mountain Digital is a trademark of Iron Mountain Incorporated. All other trademarks and registered trademarks are the property of their respective owners.



745 Atlantic Avenue
Boston, Massachusetts 02111
(800)-899-IRON

Iron Mountain Digital, the world's leading provider of data backup/recovery and archiving software as a service (SaaS), offers a comprehensive suite of data protection and e-records management software and services to thousands of companies around the world. For more information, visit www.ironmountain.com/digital.