

Email Archiving: Mitigate Risk

Managing Compliance, eDiscovery, and Records Requests



EXECUTIVE SUMMARY

Each day, organizations face numerous and increasing challenges in areas of compliance audits, responding to pending lawsuits and court inquiries, dealing with continuity in business knowledge, wrestling with operations for employee turnover and downsizing, as well as adhering to data retention policies.

FACT: An organization of 1,000 email users, each of whom generates 35 business records... will generate nearly 120 million archived emails during a seven-year retention period.¹

FACT: 24% of organizations have employee email subpoenaed.²

FACT: 15% of organizations have lawsuits triggered by employees' email.²

FACT: Only 37% of companies currently use an email archive.³

Regulatory compliance and responding to electronic discovery requests are mandatory, yet often imprecise, and the question remains of how best to satisfy these requirements and minimize risk.

Meanwhile, IT organizations are being asked to contain, reduce, slice, and dice costs, while maintaining IT service levels for core applications such as email messaging.

All of these painful challenges bring significant costs and risks to the organization, placing even more demand on email administrators' limited time and their ability to service end users' needs.

Email archiving can help organizations address and solve these challenges and when properly applied, will:

- Support IT controls for data retention, aging, and records access to meet compliance objectives,
- Reduce legal risk and liability by providing efficient e-discovery,

If one can't produce certain email records quickly with 100% confidence... if end users are harassing your IT staff because they can't be productive with their electronic communications... if your IT department is getting called day and night to restore email servers... email archiving is not only a must-have, it's a must-do-now.

CHALLENGES

As email traffic continues to grow across your organization annually, it creates a multitude of challenges and problems related to email archiving.

First, you need the technology to systematically archive messages and rapidly retrieve any message upon request.

Second, you need to maintain or improve IT services and service levels with an ever-shrinking budget.

Third, you must negotiate the multiple business issues of regulatory compliance, business mining, electronic discovery, user productivity, email server management, data retention policies, and the potential disruption from a costly audit.

NEWS ITEM:

Qualcomm fined \$8.5 million for failing to produce email during discovery. Four months after the trial, over 200,000 pages of emails and other correspondence were handed over.⁴

NEWS ITEM:

In the landmark U.S. case, UBS Warburg was ordered to pay \$29.3 million to plaintiff Zubulake for sexual discrimination. During e-discovery, it was determined that certain backup tapes were missing, emails had been deleted, and UBS failed to comply with its own retention policy.⁵

NEWS ITEM:

Ciba-Ceigy in 1995 court case was forced to search 30 million email messages at a cost of 60,000 GBP.⁶

NEWS ITEM:

Chevron settles \$2.2 million sexual harassment lawsuit based on offensive email "jokes."⁷

NEWS ITEM:

Roughly 90% of data that is provided by both sides in a legal dispute is email messages.⁸

Coping With Regulatory Compliance

If you're concerned with The Sarbanes-Oxley Act (SOX), The California Security Breach Notification Act, Gramm-Leach-Bliley Act (GLBA), Basel II, NASD Regulations, The Federal Information Security Act, and the Health Insurance Portability and Accountability Act (HIPAA), you should be even more concerned about your enterprise's vulnerability regarding email archiving, compliance, and security.

To comply with **SOX**, an organization's email system must authenticate senders, encrypt confidential information, track and log message traffic, and support the indexing, archiving, and retention of messages. Ideally, one could implement email policies to filter communications between the executive team and accountants and archive those communications for a future review of accounting practices.

Meanwhile, **NASD Regulations** consider email to 25 or more prospective retail customers as sales literature. Therefore, it must be approved prior to use by a registered principle of the company, then archived as part of the company's records for three years from the date of last use.

The Federal Information Security Act of 2002 (FISMA), developed by the National Institute of Standards and Technology (NIST) in 2002, requires all federal agencies and their partners to establish, consistent, risk-based security processes. Because every agency relies on email to support operations and assets, agencies must address email security in order to comply with FISMA.

HIPAA, The Health Insurance Portability and Accountability Act of 1996, has evolved into a far-reaching bill that calls for the protection and management of all patient health information. The HIPAA Privacy Standard, Section 142.308 of Subpart C, Security and Electronic Signature

Email Archiving: Do More With Less

Standards, sets forth requirements for “technical security services that guard integrity, confidentiality, and availability.”

Most regulations have requirements in areas such as:

- Retaining data for a certain number of years,
- Aging or purging policy around the data,
- Encrypting data for privacy,
- Tamper-proofing or proof of data integrity,
- Ability to selectively identify information to never be deleted,
- Having data that is easily searchable and accessible, and
- Gaining restricted access to the data through email archiving.

In the past, users attempted to use existing backup/restore solutions to fulfill data retention and purging policies, but the increasing requirements listed above underscores how backup/restore falls far short in meeting today’s challenges.

Responding to Electronic Discovery, Lawsuits, and Records Requests

Your organization doesn’t need be in the middle of a lawsuit in order to feel the pain and pay the costs of producing all “relevant information.” Records requests are served daily upon local, state, and federal agencies. Higher educational institutions and K-12 districts not only have records disclosure policies, but sensitive areas regarding children and young adult communications including harassment and discrimination. Corporations must manage ex-employees smoothly during resource transitions. When in doubt, requesting parties will request “everything” available and legally permissible — in order to fish for useful information. Unfortunately, too often, this causes very expensive efforts by the responding party.

When any of these events occurs, organizations must be able to produce relevant records such as email in a timely fashion and typically while under legal pressure. However, according to Baseline.com, approximately two-thirds of companies live on the edge with no policies in place for proactively saving, purging, managing or archiving their email files.

Minimizing Costly Audits

Responding to audits is costly, and demonstrating “due care and diligence” is often subjective. In today’s economy, whether you are IT staff in an enterprise trying to demonstrate that email retention policies are implemented effectively or a service professional such as a physician in a medical practice concerned about showing compliance with HIPAA requirements to store three years of email, your goal is to decrease the time and money spent on internal or external audits while increasing confidence in the results.

Today’s pain stems from the significant time spent by expensive resources (IT administrators or physicians) responding to audits with very laborious manual procedures, e.g. restoring email servers from backup tapes, or browsing and reading through emails in an email client like Microsoft Outlook. With external regulatory audits, this also does not include any legal or staff costs associated with court appearances to obtain/access public records, and the accompanying exposure to local, state or federal authorities.

ADDRESSING THE CHALLENGES

The numerous challenges for email archiving can appear both overwhelming and daunting:

- **To address compliance**, one needs to implement not only long-term data-retention and aging policies, but must demonstrate secure information storage and easy, online access to the information.
- **To address e-discovery and records requests**, one needs additional features: support of legal holds on sensitive information related to court cases, proactive policy notifications about sensitive emails, ability to analyze historical or legacy information sitting in local Outlook .PST files, support of legal workflow and case management for proper handling and analysis of sensitive information, and if necessary, ability to produce court-admissible evidence based on original, unmodified emails.
- **To address high costs** of audits and other records requests, one must be able to find, analyze, and act upon relevant information instantly. And in order to mitigate legal and liability risks, one needs to have high confidence in the results, whether it is information or the absence of.

Email Archiving: Do More With Less

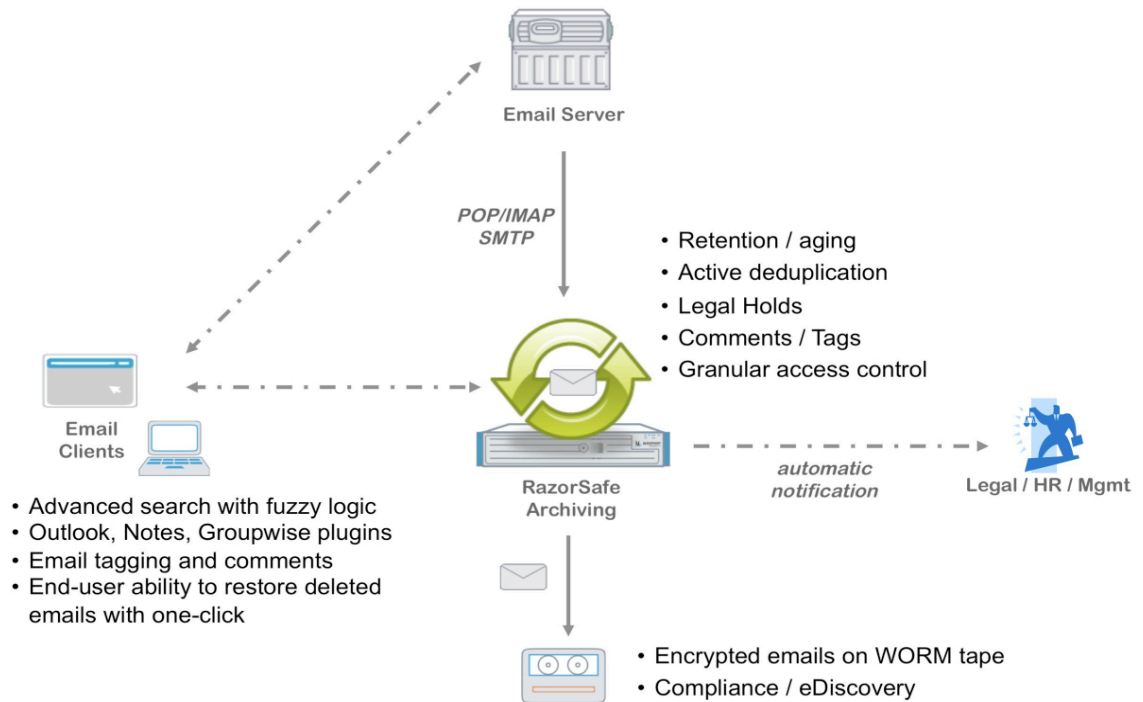
SOLUTION

Mirapoint's RazorSafe™ email archiving appliance addresses e-discovery, email server management, end-user productivity, business mining, and compliance/audit challenges in an all-in-one solution. It aids organizations which are:

- Facing audit requests for email,
- Responding to lawsuits and records requests,
- Dealing with employee turnover and business continuity challenges,
- Reducing email management costs without cutting service or features, or
- Purging all email beyond a certain date to remain compliant.

Architecture

Mirapoint's architecture encompasses an open, standards-based approach with an emphasis on simplicity, reliability, and low Total Cost of Ownership:



Addressing the Pain

- **Complying with Regulations.** RazorSafe implements flexible retention and aging policies based on sender, recipient, domain, keywords, and advanced search criteria. These features support compliance with data retention and aging policies, support legal case management, decrease audit costs, demonstrate diligence and care, and follow best practices for data safety, integrity, and restricted access to information. By providing AES256 encryption of original emails to write-once read many (WORM) tape, RazorSafe

Email Archiving: Do More With Less

ensures both privacy and the ability to prove that original emails have not been tampered with, for both regulatory compliance and legal requests.

- **Responding to e-Discovery and Records Requests.** With its advanced search capabilities include word proximity, weighting, and advanced Boolean logic, RazorSafe reduces the time and costs associated with e-Discovery or records requests. Instead of taking months or years to respond, subpoenas or court requests can be met typically within minutes or hours (e.g. Federal Rules of Civil Procedure specify a 30-day time to respond).

RazorSafe indexes and searches across all email headers, body, and attachments, bringing higher confidence in knowing if relevant emails exist or not, and minimizing the risk of discovering surprising information later.

Legal or human resource representatives can export messages securely for review. With confidentiality notification and legal hold policies, RazorSafe can proactively highlight sensitive communications before they become a problem, as well as comply with legal requirements of not deleting data should a case involve legal matters.

- **Decreasing Costs.** By providing advanced search and workflow features, RazorSafe can significantly decrease audit costs, lower legal discovery costs, minimize administrator time in managing user emails and mailboxes, and reduce storage costs. Additionally, RazorSafe leads the industry with a low Total Cost of Ownership and high reliability. With lower capital expenditures and operating expenses than server-based and hosted offerings, RazorSafe eliminates the need for continuous security patching of the operating system, saving time and increasing reliability.
- **Managing Technology Change.** RazorSafe's all-in-one appliance architecture was designed based on open standards and open access in order to provide maximum flexibility and future-proofing:
 - Supports all major email servers: Microsoft Exchange™, Lotus Notes Domino™, Novell Groupwise™ and Mirapoint Message Server™.
 - Supports all major email clients with native plug-ins: Microsoft Outlook, Lotus Notes, and Novell Groupwise
 - Supports open standards (POP/SMTP/IMAP) for retrieving email, not proprietary methods tied to a particular email server.
 - Minimizes impact on email server by avoiding Exchange stubbing and by offloading searches to the RazorSafe custom-purpose appliance.
 - Exports search results in open .eml, allowing for extraction and sharing of email information

Additionally, since the RazorSafe solution contains copies of all email, it ensures high-availability to email, even if the email server goes down or during a migration of email server technologies or infrastructure. All of this provides future proofing against technology change.

CONCLUSION

The deployment of an adequate email archiving system can provide numerous important benefits for any size enterprise, educational institution or government entity, including support for pain points across legal and regulatory compliance obligations; ever-expanding storage requirements; and knowledge management obligations. Mirapoint's RazorSafe email archiving solution offers:

- **An all-in-one appliance** with the industry's lowest TCO with minimal administration resources, saving an enterprise hundreds per user per year
- **Plug-and-play simplicity** with ease of installment and deployment in minutes
- **Open, standards-based** architecture with broad support across all major email servers and clients
- **99.999% reliability** from the market leader in appliance-based email archiving
- **Proven technology** with 120+ million mailboxes served and secured worldwide over more than 1,800 customers from the industry's first email security appliance company.

REFERENCES

¹ 2008 Osterman Research, Inc.

² American Management Association: *Workplace E-Mail, Instant Messaging & Blog Survey, 2006*

³ Information Week Analytics *E-Mail Archiving survey of 865 business technology professionals.*

⁴ *Qualcomm vs. Broadcom, Case No. 05cv1958-B (BLM), January 7, 2008.*

⁵ 2009 Osterman Research, Inc.

⁶ *Information Age: Letting go of email, February 10, 2006.*

⁷ *New York Times: Chevron Settles Sexual Harassment Charges, February 22, 1995.*

⁸ 2009 Osterman Research, Inc.

About Mirapoint Software, Inc.

Founded in 1997 and based in California's Silicon Valley with offices worldwide, Mirapoint is a global leader in the mail server appliance market with over 120 million mailboxes secured worldwide, and the leader in appliance-based email archiving. By combining email security application expertise with extensive messaging appliance experience, Mirapoint offers the industry's first and only integrated email security, archiving and mailbox appliances with a dramatically lower total cost of ownership (TCO), as well as security, control, simplicity and peace of mind.

World Wide Sales Contact

Kaizen Ventures, Inc.

New York Office

Tel: +1.866.979.4080 | Fax: +1.631.382.8160

Email: sales@kaizen-ventures.com | [Web: www.kaizen-ventures.com](http://www.kaizen-ventures.com)

©2009 Mirapoint Software, Inc. All Rights Reserved. Mirapoint is a registered trademark and Mirapoint RazorSafe and Mirapoint RazorGate is a trademark of Mirapoint Software, Inc. All other trademarks are the property of their respective owners.