

The Growing Need to Archive Email

**An Osterman Research White Paper
Prepared for WaLa Systems**

May 2006



The Focus of this White Paper

'Email archiving' is one of those terms that evokes a variety of responses from messaging managers. Individuals in heavily regulated companies, such as broker-dealers, see it as a critical element of good messaging management in order to satisfy regulatory requirements. Others see it as a 'nice to have' feature that might provide some additional value to their organization. Still others see it as undesirable because of the potential for preserving incriminating evidence that could harm an organization during a legal action or regulatory audit.

This white paper is intended to address all three groups. Its goal is to help you understand the wisdom of at least considering the deployment of an email archiving system. The white paper discusses the various benefits that such a system can provide and why archiving email for long periods can provide more benefits than detriments for just about any organization.

This white paper also discusses the value proposition offered by WaLa Systems, providers of an appliance-based email archiving system that is designed for organizations of up to 5,000 users.

Why Organizations Should Consider Archiving

There are a variety of reasons that any organization should consider deploying an email archiving system. In some organizations, one reason will suffice; in others, there will need to be a combination of benefits to help sell the notion that email archiving is a best practice and a sound business decision.

Regulatory Compliance

There is a mindset among many messaging managers and other decision makers that there are 'regulated' and 'unregulated' industries. Regulated industries would include broker-dealers and others who deal in securities trading, since these organizations face stringent requirements; while unregulated industries would include virtually everyone else.

That is clearly not the case. In reality, there are heavily regulated industries, such as broker-dealers and investment advisors, and less heavily regulated, which includes just about everyone else. Virtually all employers in all industries face varying degrees of regulation. For example:

There are a variety of reasons that any organization should consider deploying an email archiving system. In some organizations, one reason will suffice; in others, there will need to be a combination of benefits to help sell the notion that email archiving is a best practice and a sound business decision.

- Broker-dealers must comply with a variety of retention and supervisory regulations, including SEC Rules 17a-3 and 17a-4; NASD Rules 2210 and 3110; NYSE Rules 440, 342 and 472; and NFA Rule 2-9.
- Registered investment advisors must comply with new email retention provisions of Rule 204-2 contained in the Investment Advisers Act.
- The Investment Dealers Association of Canada imposes email retention and supervisory requirements on Canadian investment dealers through IDA By-law 29.7.
- Other data retention requirements focused on the financial services space include NCUA Part 749, 12 CFR 226.25, 17 CFR 270, 17 CFR 275 and 17 CFR 240.
- Large, public companies face regulatory requirements from statutes like Sarbanes-Oxley, specifically Sections 404 and 802.
- Organizations that manage healthcare-related information must satisfy statutes like the Health Insurance Portability and Accountability Act (HIPAA), the Medicare Conditions of Participation. Further, Medicare and Medicaid reimbursement to rural health clinics requires that these clinics maintain medical records for six years.
- Contractors to the US federal government must satisfy provisions of the Federal Acquisition Regulation (FAR).
- Almost all organizations, depending on the jurisdiction(s) in which they operate, are subject to regulations like the Gramm-Leach-Bliley Act, California's SB 1386, the Americans with Disabilities Act, the Patriot Act, the Toxic Substances Control Act, the Civil Rights Act of 1964 and the Personal Information Protection and Electronic Documents Act (Canada), to name but a few of the many regulations that include data retention provisions.

The consequences of failing to comply with data retention regulations, as well as legal discovery requirements (as discussed later in this document), can be severe. Consider the following:

- Ronald Perelman sued Morgan Stanley in a case in which Perelman alleged that Morgan Stanley did not uncover fraud at appliance maker Sunbeam. Because Morgan

Ronald Perelman sued Morgan Stanley in a case in which Perelman alleged that Morgan Stanley did not uncover fraud at appliance maker Sunbeam. Because Morgan Stanley did not provide to the court emails that it was ordered to produce, the judge in the case told the jury that Morgan Stanley's failure to produce the emails was 'an act of bad faith' – Perelman won a \$1.7 billion judgment.

Stanley did not provide to the court emails that it was ordered to produce, the judge in the case told the jury that Morgan Stanley's failure to produce the emails was 'an act of bad faith' – Perelman won a \$1.7 billion judgement. Further, in February 2006, the SEC fined Morgan Stanley \$15 million because of their inability to produce the required emails in this case.

- In March of 2004, Bank of America was fined \$10 million by the SEC for failure to a) continue to retain email records regarding a recent merger and b) for taking too long to comply with regulatory requests. The SEC charged that Bank of America misled regulators and took too long to produce evidence in an investigation of improper trading by employees at its securities brokerage. The bank complained that it would be "too much work" to produce certain archived emails – it took the bank nearly two years to produce all of the emails that had been requested.
- In December 2002, Salomon Smith Barney, Morgan Stanley, Piper Jaffrey & Hopwood, Deutsche Bank and Goldman Sachs were fined a total of \$8.25 million because of their failure to adhere to SEC Rule 17a-4 which requires broker-dealers to preserve electronic data on non-rewritable, non-erasable storage.

The increasing proportion of corporate records that are sent through and stored in email necessitates an archival capability that can manage records in this native format – printing copies of email for retention is unwieldy, prone to error and very expensive.

While most of the regulations that include provisions for data retention do not specifically require email retention, there are two important things to consider in this regard. First, the increasing proportion of corporate records that are sent through and stored in email necessitates an archival capability that can manage records in this native format – printing copies of email for retention is unwieldy, prone to error and very expensive. Second, email constitutes a written communication that carries the same formality and weight of a certified letter.

It is important, therefore, that organizations of all sizes and in all industries assess their regulatory requirements with regard to the preservation of email. These requirements exist at the Federal and state levels and, in some cases, at the county or city level. Also, the various countries in which an organization operates typically impose some level of record retention requirements with which organizations must comply.

Legal Discovery and Litigation Support

From a legal standpoint, data retention is an increasingly important component of a good messaging management strategy for one simple reason: email is increasingly included in legal discovery orders. Courts are increasingly finding that email contains valuable content that can be of value in legal discovery proceedings. Further, the case of *Zubulake vs. Warburg* has become the 'gold standard' in legal discovery arguments, since the case makes it more likely that a defendant will have to bear the costs associated with legal discovery if a plaintiff can demonstrate that an email system contains information that is likely to be valuable.

An organization faced with the cost of satisfying a legal discovery order using nothing but backup tapes faces potentially major costs to satisfy the order.

For an organization that must produce information from its email system during legal discovery, the primary value that an archiving system can offer is a dramatic reduction in the cost of this activity. An organization faced with the cost of satisfying a legal discovery order using nothing but backup tapes faces potentially major costs to satisfy the order. Because recovery servers must be set up, the contents of backup tapes read into live storage, and then the requested information must be found, the process of discovery can be time-consuming, extremely expensive and disruptive to IT staff members who typically must stop other activities to perform this work. An email archiving system can dramatically shorten the amount of time required for legal discovery and can cut the costs of discovery to just a fraction of what they would be otherwise.

Another issue to consider is the potentially severe consequence of not being able to produce email in a timely fashion in response to a discovery order. Emails that cannot be produced in response to such an order may be presumed to be incriminating – the Perlman case noted above is an example of the type of inference that may be drawn by a judge and jury from such an inability to satisfy a discovery order.

In addition to legal discovery, an email archiving system can assist an organization in assessing its position at the beginning of a legal action. An organization faced with a wrongful termination lawsuit, for example, can quickly go through an archive for all emails and other information that might be relevant. If the organization finds that its position is untenable, the organization's legal counsel can push for a quick settlement in order to minimize its losses. If, on the other hand, an examination of the archive reveals that the

lawsuit is without merit, it can leverage this knowledge, as well.

From a legal perspective, one of the arguments against email archiving is that it preserves 'smoking guns' that could serve to harm an organization during a regulatory audit or legal discovery. Many believe that deleting all email on a regular basis can insulate an organization from liability by removing potentially incriminating evidence that might be introduced during a legal action, for example. However, there are two arguments against deleting email as a means of protecting an organization:

- Deleted email is never completely deleted. While your organization may delete all copies of email, external recipients of email still likely have copies of it stored in their archives, on backup tapes, or in local .PST files. Employees likely have copies of email on their laptops, PDAs, home computers, USB keychain devices, etc. In short, while email can be deleted from servers and backup tapes, there are many other locations in which copies may be found.
- Deleting email on a regular basis is no guarantee that an organization will not be held liable for producing email during a regulatory audit or during discovery.

An appropriately configured email archiving system can automatically move content from users' mailboxes to the archive while still making it available to users on a long term basis.

Storage Management and Storage Optimization

Most organizations impose mailbox size quotas in order to ensure a good compromise between email server performance and usable mailbox sizes for end users. Osterman Research has found that the median mailbox size among organizations that impose such quotas is 100 megabytes. If mailbox sizes are allowed to grow larger, email server efficiency can suffer, message delivery times can slow and restoration after a server crash can take longer. If quotas are made smaller, users will spend more time cleaning out their mailbox in order to stay within their quota limitation, reducing their productivity.

An appropriately configured email archiving system can automatically move content from users' mailboxes to the archive while still making it available to users on a long term basis. From an operational standpoint, then, an email archive can provide the best of both worlds: IT can impose fairly strict quota limitations in order to maintain optimal email server performance, while users can employ a mailbox

that appears to be infinitely large because content is automatically archived.

Knowledge Management

Osterman Research has found that the typical email user spends about one-third of his or her day using some aspect of an email system: sending and receiving emails, looking for attachments, creating or looking up contacts, managing tasks and so forth. Coupled with the fact that email systems have become the primary file transport mechanism and repository for most organizations, there is, therefore, an enormous quantity of information stored in email systems that users can employ in doing their work. Osterman Research has found that more than 90% of email users refer to old email when composing new email.

An email archiving system can serve as an effective knowledge management tool by making older email content available to users through an easy-to-use search interface. While knowledge management is unlikely to be the primary reason that an organization implements email archiving, it is an important additional benefit that an organization can realize.

Disaster Recovery

It almost goes without saying that disasters happen. Hurricanes, tornadoes, floods, earthquakes – as well as the odd leaky water pipe above a server room – can all render an email system inoperable. While backup tapes are useful in bringing an email system back online, perhaps using a secondary set of servers at another location, there can still be substantial data loss incurred. For example, if an email server goes down due to some sort of serious problem at 4:00pm on a Wednesday afternoon, typically the most recent backup tape that would be available would be one from the night before, resulting in a loss of all email data generated by employees on that Wednesday. An email archiving system, on the other hand, can be configured to archive data in near real-time, resulting in comparatively little data loss.

An email archiving system can serve as an effective knowledge management tool by making older email content available to users through an easy-to-use search interface.

The WaLa Systems Value Proposition

WaLa Systems' Defender is a self-contained appliance that provides a complete archiving solution for organizations of up to 5,000 users. The appliance is easy to deploy and manage, and provides a complete archiving solution that satisfies the requirements discussed above:

- **Compliance**

Defender fulfills the message storage requirements of the various regulations noted above. Data is stored with MD5 identification, an encryption algorithm designed to verify the integrity of data, to guarantee that the data has not been modified.

- **Legal discovery**

Defender can quickly produce all related documents. Often, showing the context in which an email was written can refute a single apparently damaging email taken out of context.

- **Storage management**

With access to an extremely large archive, users no longer need to tie up large amounts of storage on their desktops or the company mail server(s).

- **Knowledge management**

Defender offers an easy-to-use interface that allows users to rapidly identify and recover messages. Users may retrieve their messages from their own archive, reducing the need for IT staff to be involved in recovering deleted or missing emails.

Defender also provides a number of other benefits, including:

- A very affordable archiving capability that can be deployed for as little as \$10 per user.
- Real-time archiving, not batch archiving. This is extremely important in the context of regulatory and legal compliance, since a batch archiving system allows users to delete email between archiving cycles.
- Non-intrusive archiving that imposes no requirement on individual users to identify the records that need to be retained and those that can safely be deleted.

[Defender provides] real-time archiving, not batch archiving. This is extremely important in the context of regulatory and legal compliance, since a batch archiving system allows users to delete email between archiving cycles.

- An 'edge' form factor, completely independent of the email server, so that mail server performance is unaffected by archiving operations.
- The ability to restore email content to a newly created mailbox so that individual users can be investigated independently of their normal day-to-day use of email.
- On-line search capabilities, including email and mailbox restoration, eliminating the need for tape-based systems.
- Protection of intellectual property through both outbound content filtering and supervisory search capabilities.
- Defender serves as the basis for a robust disaster recovery and business continuity solution.

For smaller organizations, an easy-to-deploy email archiving solution is an important tool that can reduce an organization's costs, make it more responsive to information requests during regulatory audits or legal discovery, make its email servers more efficient and make its users more productive.

Summary and Conclusion

Email archiving is a critical component of an overall messaging management capability that can provide a number of important benefits for organizations of all sizes in all industries. Among these benefits are:

- Regulatory compliance
- Legal discovery and litigation support
- Storage management and storage optimization
- Knowledge management
- Disaster recovery

For smaller organizations, an easy-to-deploy email archiving solution is an important tool that can reduce an organization's costs, make it more responsive to information requests during regulatory audits or legal discovery, make its email servers more efficient and make its users more productive.

© 2006 Osterman Research, Inc. All rights reserved.

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

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.