

3 REASONS TO ARCHIVE E-MAIL

Compliance, Capacity, e-Policy

**C2C Systems
November 2003**

November 2003 Copyright C2C Systems

Disclaimer of liability: While every precaution has been taken in the preparation of this document, C2C Systems assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

Introduction

Compliance, capacity and e-policy. Which factors are driving e-mail archiving at your organization? And how do you pick a solution that solves your specific problems without breaking the bank? This white paper:

- Examines some of the drivers for archiving.
- Explores the internal and external influences on e-mail archiving.
- Reveals some ideas to tackle your most important problems.
- Discusses some of the requirements of current legislation.
- Looks at some solutions to the various needs.

Drivers to archive

Three basic requirements are commonly expressed when email administrators are asked about their needs for archiving. These being:

- To aid the organization meet legal requirements (compliance).
- To improve system performance (capacity).
- To manage the retention of corporate information (ePolicy).

When C2C asks administrators for their key requirements within each of these areas, their answers generally cover the following. Your organization is probably no exception.

Compliance

- Assist compliance with legal requirements.
- Reduce the legal risks associated with emails.
- Improve the awareness to the organization of legal exposure.
- Ability to store, search and retrieve emails.

Capacity

- To improve the email system performance.
- Fast implementation without need for complex infrastructure.
- To help improve Service Level Agreements (SLA's).
- Reduce back-up/restore times.

e-Policy

- Enforce company e-Policy.
- Provide retention of emails (corporate information).
- Reduce legal exposure.
- Improve system performance.

Unfortunately, in practice, the solution to one requirement may be in direct conflict to the aims of another. This is because the business requirements often differ hugely from the IT drivers; even the IT infrastructure requirements can conflict with each other.

So let us examine some of these influences.

Compliance

This is driven by various governmental and regulatory demands. The high profile acts of today are SEC and Sarbanes-Oxley, the latter affecting many US companies. The legislation can call for retention periods and demand deletion as well. The requirement is to copy away all emails relating to subjects, departments or individuals.

The need here is to copy away data before a user has a chance to manipulate it or delete it. System performance and selective retention have nothing to do with compliance.

Retention of Information

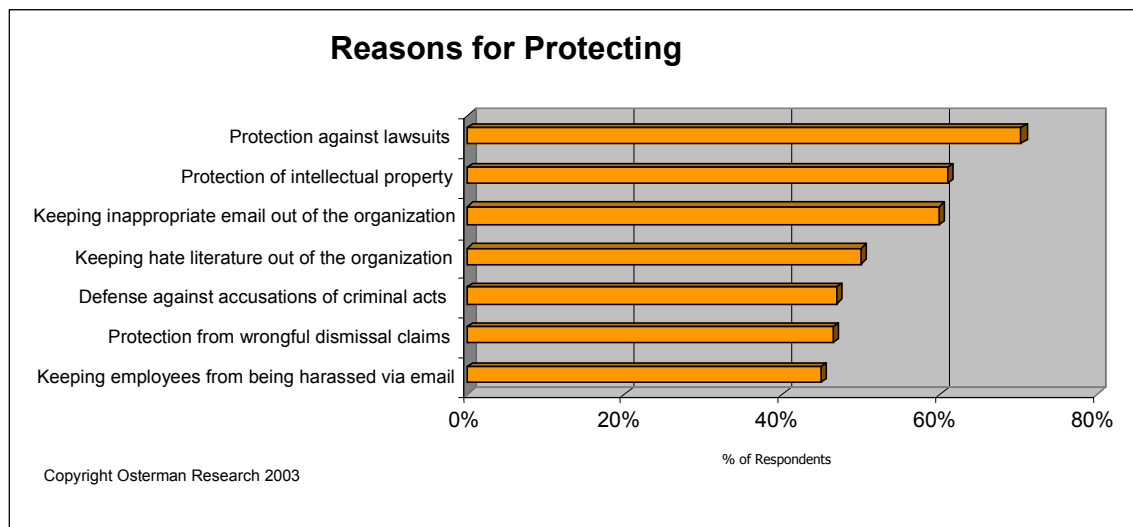
This relates to the use of information in the workplace. There are two primary reasons for retaining emails.

- Emails contain knowledge.
- Emails contain information that can protect the organization.

Surveys have shown that users retain emails seen as relevant to their daily work. They often reference them regularly and therefore need to keep this information accessible.

Management is also aware of the risk involved with email. There has been plenty of publicity of court cases involved with discrimination and inappropriate use of email. The organization must therefore protect itself; the ability to find or remove email is part of that protection. The emails the organization may wish to find or remove could well be different from the emails being used by users in their daily business.

The following chart from a survey by Osterman Research highlights the reasons companies gave for keeping email.



The solution here is to selectively retain and store emails, based on corporate criteria.

Capacity / system performance.

The demand for mailbox space is faced by every organization. The impact of mailbox size on system performance and user productivity is high. Large information stores will impact the back-up/restore times of the system, potentially impacting the business if failures were to occur at key business hours.

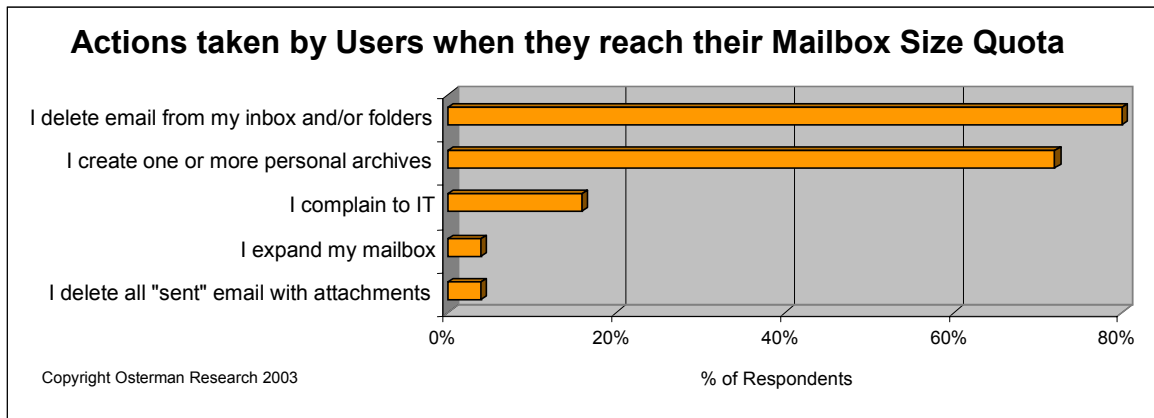
The demand from most Administrators is to reduce the mailbox size or demand for space. Reducing mailbox size can be done by introducing quotas, but this is not necessarily a good thing to do (see below).

Another alternative is to archive, but be aware of the choice of approaches available. If the need is to make drastic reductions to the volume of storage used, then tackle this; don't implement a complex archiving solution when other approaches can be implemented quickly and effectively.

Impact of mailbox quotas

Users' demands to increase their mailbox sizes give IT departments a continual headache of how to provide and manage enough storage. Meeting storage demands are expensive, so IT departments are often driven to introduce mailbox quotas.

Users' reaction to hitting mailbox quotas is alarming. This chart (courtesy Osterman Research) shows how users cope.



If users have to delete email, but they need to retain corporate knowledge to do their job, it follows that they will spend longer and longer trying to find emails that can be deleted without impacting their working life. This time costs money. At 30 minutes per week, this amounts to thousands of dollars of lost productivity per user per year.

The common short-term reaction is to create a personal archive, known as a PST. However the problems of PSTs are now well known, with major issues such as size limitations and invisibility to the Administrator. If PSTs are unknown to the Admin, then they cannot be searched without special software and the ability for a company to limit risk is in jeopardy.

So, the decision needs to be taken as to whether to

- a) allow users to delete emails (losing vital information) or
- b) allow them to create PSTs (creating legal exposure to the company) or
- c) to archive the data in the most suitable way.

The problem of mailbox quotas can be resolved by introducing archive systems that offer different storage media for less critical or older data. This storage can range from a secondary Exchange system (easy to implement, immediate benefit) to off-line or near-line systems where retrieval is likely to be slower, but the storage costs are almost certainly lower.

Looking for answers

These are just some of the internal and external forces driving the need to archive. If you are a registered securities dealer or broker, you have to archive all electronic communications of licensed professionals. If your company has doubled in staff in less than a year, you may be reaching the high end of mailbox storage limits and your Exchange server is no longer at a manageable size. If you are a lawyer in a large firm, it may be company policy to save e-mails that could later be used as evidence in court.

“E-mail archiving is becoming increasingly critical for enterprises of all sizes,” says Michael Osterman, president of Osterman Research. “A properly designed and managed archiving system can significantly improve e-mail system performance, help maintain adherence to corporate policies and help an enterprise meet its regulatory and related requirements for long-term archival of e-mail-based records.”

As you can see, e-mail archiving is being driven by a number of areas: capacity, compliance and policy. Let’s take a look at each one.

Capacity Management

Experience tells us that message volumes and message sizes are rising rapidly. Some types of companies whose focus is sending and receiving large reports (notably marketing, finance type organizations) tend to show high growth in terms of message attachment size, others more simply find that an email based conversation is taking over from the ‘phone as the preferred method of business communication. The resultant increase in traffic and storage volumes can adversely affect email systems and infrastructures that just weren’t built for the increases we’ve all encountered.

“We see 10,000 messages a day, 40,000 messages a week,” says Kenneth Adams, CIO at Miles & Stockbridge, a regional law firm of 160 lawyers in Maryland and Virginia. “We have mailbox management concerns.”

Administrators, charged with providing high availability servers *and* giving users access to their stored data, are turning to archiving solutions. There are a variety of solutions on the market, ranging in terms of cost, complexity, ease of use and manageability. Adams is using Archive One Capacity, C2C’s e-mail archiving and capacity management solution for Microsoft Exchange, as a pre-emptive solution.

“We use it to manage the SENT and DELETED e-mail folders, taking the weight out of the users mailbox and allowing us better controls over recovery and retention,” says Adams who is the administrator for one Exchange 2000 server with 500 mailboxes.

Another archiving requirement is user invisibility. Busy administrators don’t have time to train users on a new system. *“We wanted a solution that was easy to implement and was as good as invisible to our 500 users,” says Paul Cartwright from Macfarlanes, a major UK law firm. “They don’t want to know about the technology and shouldn’t have to. What’s important is providing them with an e-mail system that’s responsive and robust.”*

Archiving for capacity management quite simply uses central rules to keep critical data locally and archive off older data to a secondary store. This means that the performance and availability of email which is critical to the business can be maintained within SLAs, while older (less critical) email may be stored on a second server and have a longer agreed back-up or restore window.

Regulatory Compliance

Regulations are requiring various industries to store electronic information for a period of time. These new standards are pushing the need to archive.

Typical regulations force organizations to

- Keep copies of all e-mails (selected by individual or department).
- Keep copies of all e-mail transactions with third parties.
- Maintain copies of the electronic calendars of key members of staff.
- Save messages in a securely indexed format and be able to be retrieved as and when they are needed.

Non-compliance with regulations is serious. In December 2002, The Securities and Exchange Commission, the New York Stock Exchange and NASD fined five firms a total of \$8.25 million for failure to preserve e-mail communications. Each of the firms — Deutsche Bank Securities Inc.; Goldman, Sachs & Co.; Morgan Stanley & Co. Incorporated; Salomon Smith Barney Inc.; and U.S. Bancorp Piper Jaffray Inc. — consented (without admitting or denying the allegations) to findings that each failed to preserve for a period of three years, and/or preserve in an accessible place for two years, electronic communications relating to the business of the firm, including interoffice memoranda and communications.

To meet regulatory requirements, the key is to find an archiving solution that maintains e-mail integrity. DoD 5015.2-STD, for example, requires that any record (including e-mail), when retrieved, can be reproduced, viewed, and manipulated in the same manner as the original. When it comes time for regulatory audits, you won’t want e-mails challenged for lack of authentication.

This is one of the main reasons **why back-up of email isn’t enough** to meet regulatory requirements. The fast indexing and search for retrieval of email is inherent to true archiving solutions. When you need to track down email, you’ll no doubt need to search millions of messages and their contents in a restricted time-frame. Back-up just doesn’t allow for this to happen – true archiving solutions are built for the writing away and

retrieval of high volumes of email, maintaining full data integrity and audit trails which would stand up in a court of law.

Another point to remember is that searching and retrieving messages within a prescribed time-frame is virtually impossible to do manually; when the requirement is to retrieve an email out of millions within (say) 48 hours, this does not mean “give the request to the IT department and they must present the data within 48 hours”. This almost certainly means “your company has 48 hours in which to present the data”, so you need to get the data to the lawyer who probably needs to set it out in the context of the case and to present that within 48 hours. Realistically, the IT dept probably needs to find the data within an hour! This implies the need for a fully flexible, well managed system.

When you look at compliance you will need to bear in mind

- The regulatory reasons for compliance.
- Other legal factors pertaining to data retention.
- Whether the data is tamper proof.
- Methods of sampling and review.
- The abilities of the company to manage this data.
- You may need to prove that you have undertaken all of these and more.

You will need to involve all aspects of management to ensure that the compliance project is not just left to IT, it is an organization wide activity.

So what do you do if regulations don't yet apply to your organization?

Our experience says ‘be prepared’. It is sensible for any organization to begin to archive emails that may be regarded as company records; whether for employee management or commercial reasons. Common sense says that it is likely that regulation will spread, and it is simply unacceptable in court to say that electronic data cannot be retrieved.

E-Policy

As more business-critical information is sent over e-mail, companies are increasingly aware of the need to ensure that all records and information important to a business, whether in paper or electronic form, is archived. According to The ePolicy Institute, a new survey of 1,100 U.S. companies reveals that 14 percent of respondents have been ordered by a court or regulatory body to produce employee e-mail, up from 9 percent just two years ago.

In response, many companies are creating, implementing and educating employees about e-policy, a corporate statement and set of rules to protect the organization from

- casual or intentional abuse that could result in the release of sensitive information, and
- IT system failures or litigation against the organization by employees or other parties.

An e-policy may specify what can and cannot be sent electronically (such as e-mail jokes with attachments) and what is kept, such as all e-mails to and from the Human Resources department. This provides greater security and minimized liability associated with inappropriate e-mail content. For example, UBS Warburg LLC was sued for sex discrimination and retaliation in June 2003. The plaintiff sought e-mails in discovery to

prove her case. The e-mails were archived and would cost \$175,000 to restore and produce, but a federal judge ordered the employer, at its expense, to turn over all e-mails on optical disk or an active server.

Although internal and content-driven e-policy is a third reason to archive, The ePolicy Institute finds that only 34 percent of employers have a written e-mail retention and deletion policy in place today. "That's the same figure reported in 2001, 12 months before five Wall Street brokerages were fined \$8.3 million for failing to retain e-mail," says Nancy Flynn, executive director of The ePolicy Institute, www.ePolicyInstitute.com.

Where does my company stand on archiving?

An August 2003 Osterman Research study, "Enterprise Email Archiving: Market Problems, Needs and Trends," shows most companies are still in the infancy of addressing archiving:

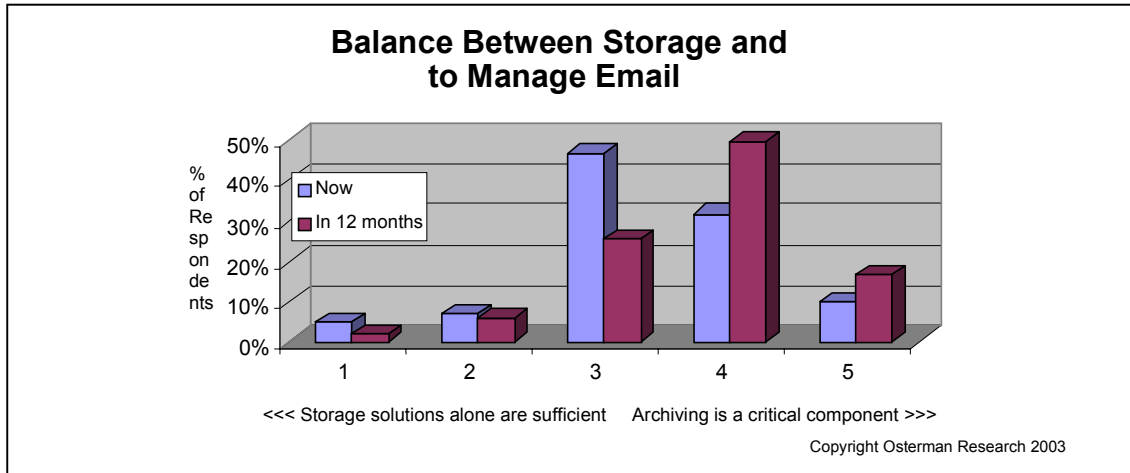
- Only about one-half of organizations have established an e-mail retention policy, and about the same percentage has implemented policies or tools for managing e-mail communication risks.
- This is despite the fact that more than one-half of organizations surveyed have at some point fired an employee for a transgression related to e-mail, and that nearly one-half of organizations have at some point been ordered by a court or regulatory body to produce employee email.
- Only one in seven organizations has implemented any "true" archiving system.
- Nearly three in five organizations have not implemented any policies or systems to ensure that users do not delete important messaging system content.

Despite the lack of progress most companies are now seriously examining archiving and balancing their needs with the organizational requirements.

How does Email Archiving fit with data lifecycle management?

Email archiving is an application that requires managed and controlled storage. Your company has probably invested thousands or even millions of dollars in creating a managed storage system. Email archiving should fit within that strategy to ensure the data is (a) safe, (b) managed and (c) secure within the framework of emerging technologies. The archiving software you choose, must work with storage management applications to give you the best of both worlds, an application from a company that understands the specific demands of a messaging system integrating with a purpose built storage management system.

The following chart (courtesy Osterman Research) shows that there is a balance between storage management and archiving.



This demonstrates that organizations are aware that storage management and archiving are almost equally important. You should be looking at systems that take advantage of or integrate with storage management solutions. Taking on archiving without putting it into context of your corporate storage management ignores all the investment and management time taken in your storage strategy.

By archiving email, companies are able to quickly produce needed evidence in court. But a key feature of any archiving solution will be the architecture of the product — Does it fit in with your messaging strategy? Does it integrate with your storage and data management investment to date? And will the supplier be in business seven years from now? Whatever archiving solution is used, you should ensure that the data will remain accessible for many years.

The C2C Approach

C2C recently announced its strategy to help organizations reduce risk while managing resources better — the **Archive One** family.

Archive One Capacity, the top selling single-technology e-mail archiving and capacity management solution for Exchange. Built in Exchange, this is designed to be up and running in minutes for a quick and effective way to minimize mailbox size.

Key benefits are:

- Improves Exchange system performance
- Fast to implement giving immediate benefits
- Will help improve/achieve SLAs
- Transparent retrieval of archived messages
- Large range of archiving criteria for selective archiving
- Integration with standard anti-virus and back-up solutions

Archive One Compliance, provides archiving, retention and retrieval management for Exchange. Archive One Compliance is designed to provide a full discovery and audit trail to organizations that need to comply with the vast array of country, government, industry and corporate rules and regulations for e-mail retention and retrieval. Built with low Total Cost of Ownership in mind, this solution integrates with investments you have already made in storage management software and storage hardware.

Key benefits are:

- Assist compliance with requirements
- Reduce legal risks
- Improve awareness of legal exposure
- Remove the need for mailbox quotas
- Provide for fast discovery and retrieval of emails
- Work in a secure environment
- Ease of use and installation
- Huge range of storage h/w supported
- Integration with leading storage management software.

Archive One Policy This is the combination of email analysis and selectivity as used in the capacity technology coupled with the archiving management to near-line / off-line storage from the compliance technology.

Key benefits are:

- Ability to enforce corporate ePolicy
- Provides a secure method for long term retention of email
- Reduces legal exposure
- Gives user ability to search and retrieve email
- Large range of archiving criteria for selective archiving
- Ease of use and installation.
- The same approach to storage management and hardware support as for Compliance.

Where can I find out more?

For more information and free evaluation software, visit www.c2c.com

C2C Systems Inc.
1 Federal Street
Springfield Enterprise Center
Springfield, MA 01105 USA
T: 413-739-8575
F: 413-739-4980
info@c2c.com

C2C Systems Ltd.
6 Richfield Place, Richfield Ave
Reading, Berkshire
UK RG1 8EQ
T: +44 (0) 118 951 1211
F: +44 (0) 118 951 1111
info@c2c.com

All Trademarks acknowledged.
Copyright C2C Systems 2003

Reference: Enterprise Email Archiving: Market Problems, Needs and Trends. An Osterman Research Multiclient Study. 2003. www.ostermanresearch.com

Appendix 1

A full spectrum of regulations specifies e-mail archiving and retrieval standards; often email is seen as just another form of electronic data and therefore treated with all other electronic documents. Here are some examples:

SEC Rule 17a-4 requires that all US financial institutions retain electronic documents — including e-mail and instant messaging — for at least six years.

The Sarbanes-Oxley Act creates new disclosure requirements for US public companies as well as new certification responsibilities for CEOs and CFOs.

HIPAA (Healthcare Insurance Portability and Accountability Act) and **Gramm-Leach-Bliley** are US privacy laws that regulate access to personal information. HIPAA, for example, regulates communications between patients, insurers and health care providers.

DoD 5015.2-STD, “Design Criteria Standard for Electronic Records Management Software Applications,” provides implementing and procedural guidance on the management of records in the US Department of Defense. E-mail messages are treated the same as any other record.

NASD (National Association of Securities Dealers) Rules 3010 and 3110 govern archive regulations for brokerages buying and selling stock on the NASDAQ.

The Food and Drug Administration’s Title 21, Part 11, requires the preservation of all electronic records.

U.S. National Archives & Records Administration General Records Schedule 20 (GRS20) manages rules for capturing and storing official government records. Some records need “disposition approval” and can only be authorized for erasure or deletion when an agency authority determines that they are no longer needed for administrative, legal, audit or other operational purposes.

The European Directive on Data Protection provides regional requirements and country-specific implementations by member states. This law means that individuals have entitlements to access their personal data kept on file, within a defined time-scale (either electronically or in hard copy). It also covers use of data including to whom the data can be passed or how it is used.