



3 Reasons to Archive Email

Compliance, Capacity, E-Policy
and more ideas beyond email archiving



Introduction

Compliance, capacity management and e-policy enforcement, which factors are driving email archiving at your organization? How do you pick a solution that solves your specific problems without breaking the bank? This white paper will help you by:

- Examining some of the drivers for archiving
- Exploring the internal and external influences on email archiving
- Revealing ideas on how to tackle your most important problems
- Discussing the requirements of current legislation
- Looking at some solutions to the various needs
- Looking at issues raised by email archiving

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



Drivers to Archive

When email administrators are asked about their archiving needs, they usually express three basic requirements:

- To aid the organization in meeting legal requirements (Compliance)
- To manage the retention of corporate information (e-Policy)
- To improve system performance (Capacity)

When we ask 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 regulatory requirements
- Reduce the legal risks associated with emails
- Improve the awareness to the organization of legal exposure
- Ability to store, search and retrieve emails
- Enable secure and audited trails of email activity

e-Policy

- Enforce company e-Policy to retain and / or delete email
- Reduce legal exposure
- Tailor retention policies to organizational needs
- Analyze email and take centralized decisions and actions

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.

Capacity

- Improve the email system performance
- Reduce mailbox and information store size
- Meet and improve Service Level Agreements (SLAs)
- Reduce back-up/restore times
- Integrate with storage and Information Lifecycle Management (ILM) strategy

Compliance

The need for 'compliance' is driven by various governmental and regulatory demands. The high profile acts of today include SEC, Sarbanes-Oxley and Basel II which were primarily driven by experiences of email mismanagement. The UK and US Freedom of Information Act laws have increased the visibility of email retention and accessibility during 2005. Legislation commonly calls for retention periods but may demand deletion following expiration of the retention period. The requirement is usually to copy away all emails relating to subjects, departments or individuals before a user



has a chance to manipulate or delete the information, providing a fully secure and audited record of email activity. System performance and selective retention have nothing to do with compliance; a solution to aid compliance is generally working behind the scenes, invisible to the end-user and with the archived copies accessible only by certain permitted officers.

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 emails (selected by individual or department)
- Keep copies of all email transactions with third parties
- Maintain copies of the electronic calendars of key members of staff
- Save messages in a secure format, 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 email 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 email integrity. DoD 5015.2-STD, for example, requires that any record (including email), 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 emails 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.

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 “your IT department has 48 hours to find the data”. It 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
- Log & audit trails of archive searches – this may involve a review hierarchy of IT, Security and/or Compliance Officers



- 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.

ePolicy

This relates to the ongoing use of information in the workplace and the appropriate management of this data to accommodate risk and accessibility factors.

As more business-critical information is sent over email, 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 Forrester Consulting over one quarter of surveyed companies were ordered by a court or regulatory body to produce employee email during 2005-2006.

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 email jokes with attachments) and what is kept, such as all emails to and from the Human Resources department. This provides greater security and minimized liability associated with inappropriate email content. For example, UBS Warburg LLC was sued for sex discrimination and retaliation in June 2003. The plaintiff sought emails in discovery to prove her case. The emails 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 emails on optical disk or an active server. Surveys have shown that users retain emails seen as relevant to their daily work, often for long time periods. They may reference them regularly and therefore see the need to keep this information accessible.

Management is well aware of the risk involved with email. As described above, there has been plenty of publicity of court cases involved with discrimination and inappropriate use of email. An organization must therefore protect itself and the ability to find, analyze or remove email is part of that protection.

This list highlights the reasons companies gave for keeping email in a survey by Osterman Research:

- Protecting against lawsuits
- Protection of intellectual property
- Keeping inappropriate email out of the organization
- Keeping hate literature out of the organization
- Defense against accusations of criminal acts
- Protection from wrongful dismissal claims
- Keeping employees from being harassed via email



Policy-driven management is enabled by a detailed and granular engine, which analyses emails by their header, body or attachment content and details and allows the administrator to set appropriate actions for a given set of requirements. In any organization the actions may differ by department, individual or even according to a project or customer. Flexibility of the analysis engine is the key to successfully enacting policy-driven archiving; emails can be managed according to far more criteria than just size or age to reflect the business requirements from the solution.

While analysis by a policy-driven solution allows the selective retention and storage of emails, use of an appropriate engine may equally result in actions such as the deletion of email, the accelerated archival of large attachments from the information store or the isolation of questionable attachments into a separate folder. Policy analysis enables a whole range of email management activities to take place.

Repository-based archiving

A flexible e-policy engine enables the distinct benefits based upon the email data. If we then add the ability to create and manage multiple repositories, then we can be selective where the data is stored and for how long. This creates a unique model which enables:

- Cost-effective use of storage media
- Retrieval times reflect relative frequency of access by users
- Hardware independence of archives
- Migration of repositories across media over time
- Reduced requirement for incremental back-ups
- Disaster Recovery plan integration

Capacity

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.

The impact of mailbox and information store size on system performance and user productivity is high. Large information stores will impact the backup/restore times of the system, potentially impacting the business if failures were to occur at key business hours.

One typical reaction is to reduce mailbox size by introducing quotas, but this is not necessarily a good thing to do in terms of the organization. Therefore 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. User invisibility is often a priority: busy administrators don't have time to train users on a new system.

Archiving for capacity management quite simply uses policy-driven central rules to keep critical data locally and archive off older data to a secondary store or other storage media. 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 externally and may have a longer agreed back-up or restore window.



If the need is to make drastic reductions to the volume or cost of storage used, then it is appropriate to tackle this but keep in mind that the two main factors affecting archiving project's success must be balanced: Cost of the storage media used and accessibility or retrieval time of the email to the user.

Impact of mailbox quotas & PSTs

The demands from users to increase their mailbox size provide IT departments with a continual challenge regarding the provision and management of storage. Meeting storage demands are expensive, so IT departments are often driven to introduce mailbox quotas.

User reaction to hitting mailbox quotas can be alarming. The following list from a survey by Osterman Research shows how users cope:

- I delete email from my inbox and/or folders
- I create one or more personal archives
- I complain to IT
- I expand my mailbox
- I delete all "sent" email with attachments

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 Store file, known as a PST. However the problems of PST files are now well known, with major issues such as size limitations and invisibility to the Administrator. If PST files are unknown to the administrators, 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)
- B. Allow them to create PST files (creating legal exposure to the company)
- C. To archive the data in the most suitable way

The problem of mailbox quotas can be resolved by introducing systems that archive from the information store onto a range of different storage media. This storage can range from a secondary Exchange system (easy to implement with an immediate benefit in performance) to off-line or near-line systems where retrieval is likely to be slower, but the storage costs are almost certainly lower.

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.



There is a balance between storage management and archiving, organizations are aware that storage management and archiving are almost equally important – highly complementary in fact. You should be looking at systems that take advantage of or integrate with storage management solutions, simply because there will be increasing volumes of email stored over time and it makes economical sense to manage the ageing email archives across different storage media, with differing costs and response times.

Issues such as migrating data across storage media, retiring media over time, employing a range of storage as appropriate to many factors: primarily cost and accessibility – cannot be ignored. 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.

This could prove expensive.

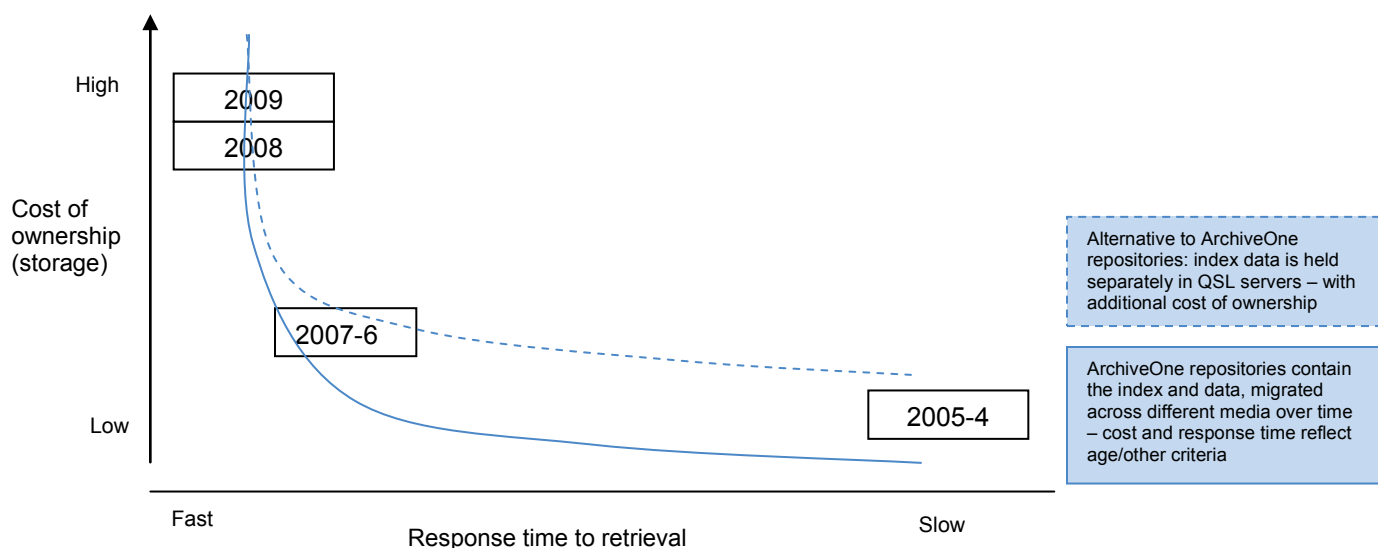
Repository based archiving: a cost effective model

Repository based archiving enables a balance between the issues illustrated above, benefiting the organizational e-policy, user, storage budgets, back-up and restore strategy and disaster recovery to optimal advantage.

A simple approach to use of archive repositories is illustrated here. Repositories are established by year and stored on media appropriate to the probable access requirements of users and the relative storage costs of those media.

For example, year 2005 and 2004 data is on old, slow, and low-cost media. Year 2007 and 2006 data is on medium cost and response media, while 2008 and the new 2009 repositories are on fast, high performance media, which is more expensive but supports the users' access requirements.

At the end of 2009, a 2010 repository will be established and previous years' repositories will be migrated back by one profile of media – so 2008 will go to medium response storage and 2006 will be moved to slower, cheaper media. Note that ArchiveOne® repositories contain the associated index data; alternative SQL based models have directly attributed additional cost of ownership with separate databases for indexes.





Where does my company stand on archiving?

An Osterman Research study with C2C shows most companies are still in the infancy of addressing archiving:

- Only just over one-half of organizations surveyed have established an email retention policy, and about the same percentage has implemented policies or tools for managing email communication risks
- Most organizations (70%) rely on back-up tape for email retention
- Only one in six organizations has implemented any “true” archiving system
- Nearly three in five organizations have not implemented any systems to ensure that users do not delete important messaging system content. One in three has no email retention policy in place at all

Another survey conducted by C2C, which featured hundreds of network administrators, system managers and other IT personnel from organizations of all sizes, found that:

- 37% were under the impression that using PST files is the same as email archiving
- 39 percent confuse backup and email archiving

Other issues

Once you have archived your email we find that administrators often have 2 questions. “How do I search all my archived and non-archived data?” and “How do I ensure the integrity of archived email and keep it secure from non-privileged users?”

These questions are common regardless of whether the client has chosen a C2C solution or an alternative product. At C2C we have addressed these issues with solutions that apply to any Exchange based system.

How do I search all my archived and non-archived data?

eDiscovery is more than a sub-set of a compliance requirement. Many organizations need to find various types of information without being concerned about compliance legislation to drive them. Consider examples of any organization that has to retrieve information related an intellectual property dispute, where dates of actions are a critical, or health sector manager who must find all communications about a certain patient or a specific drug.

Similarly, finding correspondence between suppliers and customers is often very important in maintaining good commercial relationships between organizations, by resolving disputes before they get to any level of legal intervention at all.

In addition there is specific eDiscovery legislation coming into place in some countries. This forces legal professionals to be explicit in their handling and use of electronic evidence. So law firms have to become very clear when advising their clients to be open about how they are able to find email records, both in archived and non-archived systems.

In USA the amendments to the Federal Rules of Civil Procedure (FRCP), which came into effect in December 2006, highlight any firm’s legal duty to include electronically stored emails in initial legal disclosures. This applies to cases for organizations in all markets, industries and sectors.

For all of these reasons commercial and non-commercial organizations alike are being advised by many independent consultants to make sure that they have eDiscovery solutions in place.



eDiscovery solutions require more than Compliance based archiving. It is the need to retrieve all emails that have been stored in the archive plus the ability to search for very old emails that may have not been archived and emails that are perhaps too young to be archived.

How do I ensure the integrity of archived email and keep it secure from non-privileged users?

While security has sometimes been seen as a 'flip side' to easy data sharing; this is not the case for archiving. While email servers are not always set-up with security as the highest priority, it is quite easy to add security verification to make sure that email server settings are correctly configured and so make sure that users do only have rights to see and open records that they should.

Email archiving can add to the security of the complete email system, so long as access rights verification has been added to the core mail server systems. Exact controls are provided to enable and disable access to appropriate archive locations and stores. Further to this: administrator, operator and supervisor roles should be created to allow appropriate levels of secure access to the total archive.

Audit trails are also important e-security measures. A good archive system will monitor operator usage, especially when it comes to general searches and queries. You can be sure that not only users with appropriate authority conduct global searches but also that their motivations for each search are legitimate. This provides more control than is available within a basic email system.

Email Archiving Checklist:

- Archive messages and attachments outside Exchange
- Replace messages and attachments with small message links
- Index email and attachments for fast search/ retrieval
- Wide range of easy to use archiving criteria: flexibility to thousands or policies
- Choice of 'client' or 'no client' software to ease deployment
- Support wide variety of storage media
- Compress archives for maximum efficiency
- PST archiving (automatically locates local PSTs)
- Support local archives on laptops
- Public folder archiving and management
- Multiple archive repositories with independent retention periods
- No requirement for additional software licenses or resourcing e.g. for SQL
- Full audit trails
- Admin and/or User level retrieval from archives
- Discovery within existing 'live' mail stores
- Easy to install, use and maintain



Appendix 1

A full spectrum of regulations specifies email 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 email and instant messaging — for at least six years.

The **Sarbanes-Oxley** ruling creates 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. Gramm-Leach-Bliley legislation applies to the US financial services industry.

MiFID (Markets in Financial Instruments Directive) is a European Union law. The main objectives of the Directive are to increase competition and consumer protection in investment services. Since 6th March 2009 all email records of these services must be retained for a period of at least six months, in a medium that permits access to the records readily and with audit trail.

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. Email 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.

21 CFR Part 11 (The Food and Drug Administration's Title 21, Part 11) requires the preservation of all electronic records.

GRS20 (U.S. National Archives & Records Administration General Records Schedule 20) 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.

The Freedom of Information Act (5 U.S.C. § 552) generally provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions. This right of access is enforceable in court, and it is supported at the administrative agency level by the "citizen-centered and results-oriented approach" of a presidential executive order.

Freedom of Information Act (UK): Since January 1st 2005 members of the UK public have been able to request records from a wide range of public authorities.



Reference:

Enterprise Email Archiving: Market Problems, Needs and Trends. An Osterman Research Multi-client Study, 2003 and survey 2005 www.ostermanresearch.com

E-Policy Institute “2004 Workplace Email and Instant Messaging Survey”

<http://www.epolicyinstitute.com/survey/index.html>

Email Archiving Survey Report, C2C Systems 2007, <http://www.c2c.com>

About C2C

C2C offers automated data archiving and management for email, files and SharePoint content. With over 15 years experience delivering solutions for capacity, e-policy enforcement, compliance and e-discovery, C2C optimizes performance, reduces storage management costs and minimizes risks associated with email - helping you to control your data before it controls you.

The Company, a Microsoft Gold Certified Partner, supports organizations in the government, manufacturing, finance, education and healthcare industries, including Fortune 1000 companies. Established in 1992, C2C is a privately held company with offices in Westborough, Mass. and Reading in the UK.

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.

Trademarks

All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

Where can I find out more?

For more information and free evaluation software, visit www.c2c.com or email info@c2c.com.

C2C Systems, Inc.
134 Flanders Road
Westborough
MA 01581
USA

T: +1 508-870-2205
F: +1 508-870-2250

C2C Systems Ltd
6 Richfield Place, Richfield Ave
Reading
Berkshire RG1 8EQ
UK

T: +44 (0) 118 951 1211
F: +44 (0) 118 951 1111