



Email Archiving, Retrieval and Analysis

The Key Issues

"If you are going to find a smoking gun,
you will find it in email."

Abstract

Organisations are increasingly dependent on email for conducting business, internally and externally. As a result, there are a number of risks associated with email and email management that need to be addressed by the organisation as a whole.

Whether you are a Risk Manager, CIO, Knowledge Manager, IT Manager or End User, there are email-related challenges you need to be aware of, as we all become increasingly dependent on this critical communication system.

The Impact of Email

Email is like an elephant – it never forgets. Its immediacy and ease of use means email messages can be created quickly, but their contents can come back to haunt.

Bill Gates, Alastair Campbell, Kenneth Lay and many others have all found out that emails sent long ago are not lost forever.

Email has increased as an official means of conducting business, and is unlike any other form of business communication. Like other documents, email is created, distributed, filed and destroyed, but

this process typically happens in an ad hoc manner and outside the formal processes used for traditional business documents and information.

Not only are employees and organisations more efficient as a result of using email, it is also the most cost effective means of communication.

Additionally, the transaction rate of email is many times that of other business documents due not only to the frequent use of email as a substitute for phone and written communications, but also because it is a near-instant form of communication that can reach many people simultaneously.

As a result, email has become the single largest business application in use by most corporations. Over 50 per cent of enterprises categorise email as a mission-critical system – something that was traditionally associated with financial and mainframe systems.

The purpose of this whitepaper is to explore some of the key issues facing organisations today, from a variety of perspectives, and to introduce a solution for helping these organisations manage these issues more effectively.

Challenges for All

Due to this impact, email – and the management of email – creates challenges for all parts of an organisation. From the Chief Executive to the Risk Manager, from the IT Manager to the end user, there are issues which we all face.

Many of these issues are shared across the different occupations but the themes are consistent: we all depend on email, but the tools which we are provided to manage email no longer meet an organisation's requirements.

This paper details some of these issues, and how they can be managed.

Key Issues

- Email is critical - an organisation can not live without email in the same way it can not live without telephones or electricity.
- Organisations need to be responsible in how they store and retain information contained in emails – like other documents, message are important records.
- Legal compliance and regulations mean organisations need to find information, and find it quickly.
- Existing messaging systems and tools cannot cater for the needs of the broader organisation; finding content is a challenge.
- Email is considered valuable evidence and is often labelled the “smoking gun” of modern litigation because it preserves conversations, important business decisions and documents.

Risk Manager

For the Risk Manager, managing email is about managing risk.

From simple internal communications to vital sales calls to customers, to invoicing and billing and high-level decision making, email is involved at every level of business life. A company can not live without email in the same way it can not live without telephones or electricity.

And because email is so quick to create and inexpensive to send, the volume of messages has increased exponentially. This creates risks for the organisation, detailed below.

Compliance

Organisations need the ability to comply with legal and regulatory demands when it comes to retaining and finding records.

Like other forms of document, an email is a record; defined as any piece of data, in any form, created or received in connection with the transaction of an organisation's business. Organisations need to ensure they have policies and tools in place that provide for the storage and retrieval of these records, and how long they should be preserved, in order to ensure the organisation is able to comply with regulations.

To ensure this, they need a system that ensures all emails – and their attachments – are captured, that access to these messages is logged, and that these messages cannot be tampered with; in other words, a “flight data recorder” for email. Such a solution should also be able to alert the relevant people, when emails of a particular type, or containing particular content, are processed. Similarly, this system needs to ensure that the transactional act of sending an email, and who sent and received that message – and any attachments – should be identified quickly and with minimal effort.

IT Limitations

With limited IT resources, email messages will not be retained and therefore cannot be located when required.

Most companies do not grant easy access to users, and 81 percent of companies do not allow users to access the archives without IT administrator assistance. Whether a message is purged to make space, accidentally deleted, or gets corrupted, users often find themselves needing to access a backup copy.

This translates to an average of six hours per week of administration time to assist end-users with retrieving older email, and it often takes an average of five hours to complete a system backup—meaning that administrators must plan well ahead when addressing backup procedures, further burdening their valuable time.

Intellectual Property

The organisation's intellectual property is either being deleted, or because personal email stores are required, that it simply isn't known about or being kept. By some estimates, 35-60 percent of business-critical information is stored in personal messaging systems, yet is not effectively managed. These large personal libraries of email messages are of growing interest to top management who wish to leverage this information and are concerned about the company's exposure to costly legal discovery processes.

Where do these messages go? Often they are either deleted or are moved into a local archive file—two apparent solutions that present problems to corporations wishing to leverage the amount of information captured within email messages because the messages are either difficult to access or expunged entirely from the system.

Typical email systems provide archiving capabilities which are inadequate solutions for effective long-term message archiving. The personal archive files create a fragmented corporate record and make 100 percent visibility a near impossibility. And while the message server allows companies to store messages, retrieval without requiring additional effort and expense is next to impossible.

Organisations require a solution that ensures all intellectual property is maintained, that it can be easily located – across the entire organisation – and that both messages and their attachments can be stored efficiently and effectively.

Business Continuity

Should the email server “go down”, there isn't an easy way of accessing your organisation's messages, dramatically reducing your organisation's productivity.

Email has become the lifeblood of most companies, especially ones that are widely distributed geographically. When the email system is down, many companies nearly cease to operate. This is not just a matter of immediate communications; many companies use email as a kind of de facto system for archiving and sharing documents.

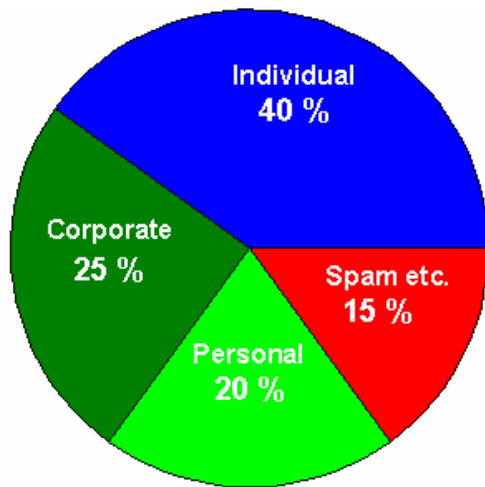
Recent virus outbreaks have highlighted the importance of email and the vulnerable nature of these systems to external threats. Typically, should a virus infiltrate an organisation, the immediate reaction is to shut down the email server, in case more infected messages should find their way into the system. This has an obvious impact on the business, which is unable to access their messages.

Knowledge Manager

Because email – and its associated attachments – are easy to create, receive and distribute, the volumes of information and knowledge that is contained within the organisation grows exponentially from year to year.

As employees increasingly use email as their main tool for business communications, more and more information remains hidden from the organisation. Memos, contracts, complaints and other documents are created and processed within email. No one can remember the details of all messages they have sent and received, so this information may – intentionally or unintentionally – be lost forever.

However, not all email messages are equal. When an email message is sent or received, it can usually be categorised as one of four types:



- **Individual** – Email between one individual and another within an organisation, rather than the organisation at large (i.e. an individual event, rather than a corporate process).
- **Corporate** – Email that is of benefit to the organisation at large, and was either originally intended to be used as a corporate record, or has become a corporate record.
- **Personal** – The individual uses email for personal use, with no corporate benefit.
- **Spam etc.** – Email that is erroneous, unimportant or of nuisance value, which is not stopped by corporate filters.

Of these types, most organisations that maintain a corporate store are only concerned with keeping two types of message: individual and corporate; organisations typically have little requirement to save personal and spam-related emails. As a result, those messages – and attachments – which are able to be deemed of benefit to the organisation need to be retained in the corporate store.

Management of the information that is important to the organisation has become a critical issue, particularly for the Knowledge Manager who needs to ensure that this information is captured, stored and remains accessible to the organisation.

For the Knowledge Manager, there are several key reasons why email is so important:

- **Email is increasingly easy to use and distribute** – In short, there is more of it. Users can easily create and distribute messages more easily than any other form of communication. Management of these messages can prove challenging and platforms such as Microsoft Exchange do not provide the Knowledge Manager the tools to access and manage this information.
- **Email is a valuable asset** – Email messages and, in particular email attachments, contain information which is of value to the organisation. Over time, messages and attachments become lost or difficult to find, yet this valuable knowledge is often left unmanaged by users who either erase email or store them in inaccessible locations.
- **Email is a record** – According to the Association of Records Managers and Administrators (ARMA) email is considered the organisation's property and, as such, is subject to management under the organisation's records management function.
- **Email needs to remain accessible** – Legislation now incorporates electronic means of communication and enforces guidelines around the retention of email and how long it must remain accessible.
- **Employee turnover** – Organisations need to be able to manage their email messages as such messages may influence how liable an organisation may be in many different scenarios, such as lawsuits, investigations, or disputes with employees, partners or customers. Employee turnover can be an issue, particularly in terms of where this knowledge may end up – it will not always remain within the organisation.

- **Email creates technology hurdles** – With the increased use and volume of email, email messaging systems are strained: messages are stored in multiple locations, performance and stability of systems can be affected, storage is rapidly used up, while viruses and other external threats can impact email systems and the broader organisation. These issues have a direct impact on the role of the knowledge manager and how safe the information is.
- **Email impacts the bottom line** – Poor management of email can also impact the bottom line, as information is easily lost and backups remain inaccessible. Management, including the Knowledge Manager, are unaware at what information they have or have missed out on.

While document management systems are effective at managing Office documents, they are perceived by many as not being suitable for emails and their attachments – the overhead of manually profiling of every incoming or outgoing email is considered impractical by critics of document management systems.

By having an automatic, central email repository a solution such as AfterMail is able to complement both the document and records management system as well as provide a single, central store that can be easily searched using a range of search and content analysis technologies. Such a solution can be implemented quickly, with minimal impact and risk on other systems in the organisation – it is a perfect complement to any existing knowledge management systems. The result is a single, central store that captures all knowledge and makes it available to appropriate people within the organisation.

Such an approach is consistent with current trends which favour a more automated approach to meeting the challenges of knowledge management.

IT Manager

IT Managers are under increasing pressure as the use of email grows, and their systems try to cope with greater volumes of messages and ever-larger attachments. Should the email server “go down”, the productivity of the organisation suffers.

While this usage endorses email as a “killer app”, it also has some “killer” side effects: it creates significant storage issues for users and IT administrators, and the disparate repositories makes locating key information both difficult and expensive.

In most organisations, it is the responsibility of the IT department to ensure that the critical email system remains available, and that emails can be stored, yet these increased volumes and usage continually challenge IT, its resources and its ability to deliver a stable and robust environment. As a result, IT needs to take steps to meet these challenges, and ensure it can provide the organisation the services it needs.

Email systems were never intended to support the need to manage and archive large volumes of business data for long term storage. With the increasing volume of email circulating within corporate email systems, combined with user mailbox size limits, administrators are now struggling with the management of email systems space, long-term backup strategies, as well as effective email retrieval.

Bulk storage of information in the message store – using the traditional approach of backup tapes and in local archives – is not an adequate solution to managing this information:

- It does not provide employees across the organisation ready access to corporate information, particularly if the information is old or stored in local archives.

- It does not allow an organisation to mine value from the information that it has paid employees to generate.
- Standard tools do not provide the flexibility for administrators to provide the necessary information to their users in a timely way, without significant time and resources.

There are also external challenges facing email systems; viruses, worms and other threats pose a risk to the email system. Other threats, such as earthquakes or natural disasters, mean that business continuity needs to be considered and email is now a critical service which needs to be restored as soon as possible.

Any solution to these issues needs to be implemented with minimal impact to any existing infrastructure, and enhance the performance of the current systems.

The IT Manager will be able to quickly implement a solution such as AfterMail, which will not only deliver an effective email archiving capability, it will also provide a platform which will support any email requirements – it can be integrated with existing systems, and can provide or be incorporated with other complementary systems already in place. The use of web services technology enables the email-related data within the repository to be accessed and utilised, without impacting the existing email solution.

End Users

While email is a useful tool for end users, who can communicate faster and more cheaply than ever before, there are still some issues concerning how users deal with messages and the limitations which are imposed on them.

As the frequency and size of emails increase, users' inboxes quickly fill, exceeding mailbox quotas, and users end up unable to send mail until the size of the inbox is reduced.

How do users do this? Are the messages deleted, which will potentially remove important corporate information from the system?

Or are the messages archived to some other location? When users archive these files – using, for example, a Microsoft Outlook personal store, or PST file – this creates more disk space, however there are some additional issues:

- Because information is stored inefficiently, the files can grow quickly.
- They are not robust – should the files get corrupted, all of the user's mail could be lost.
- They are not secure – anyone can access the content of a PST file using the right tools.
- Unless the user remembers, PST files don't get backed up. If a user's PC crashes and data is lost, all email messages may be lost.
- Poor search capabilities also mean that any information contained within PST files may not be easy to find.

In short, there are few options for users that enable end users to keep email for long periods of time, and access it again as and when they need it.

Users need a solution that will free them from these burdens: automatically filing all messages, enables them to quickly access any email message, and to do all this easily without impacting their productivity.

Benefits of AfterMail

Email can certainly be regarded as a victim of its own success. Information can be distributed relatively quickly, in a format that can be accessed from a variety of devices, and the functionality allows a single message to be automatically replicated to many people at the same time, and for additional content to be attached. The reality of this functionality is that mailboxes can get very large, very quickly. As a result, emails will increase exponentially and will double every two years. Given this volume, organisations can not know what is valuable and what isn't – they need a 'flight recorder box' to keep it all, just in case.

By implementing an email archiving solution, your organisation will be able to reduce the risks associated with email management, and ensure compliance and discovery requirements are met. By capturing all email messages, your organisation will also ensure corporate knowledge is retained and accessible – to approved personnel – reducing the cost of administration and empowering users throughout the organisation.

Simple in concept, but highly functional in deployment, AfterMail *automatically* captures email messages sent through your email server, and intelligently stores them in a single, centralised email archival and analysis system. Once stored, AfterMail provides easy access to these messages, allowing permitted users to search and retrieve their own messages, or for managers and administrators to search across the entire organisation.

By processing messages in this way, AfterMail gives organisations the assurance that their key needs are being met:

- **Ensuring an archive** – Put simply, all messages are stored. Once a message is processed by the email server, a copy of the message is automatically placed in the AfterMail repository. AfterMail also provides users – security permitting – with the ability to quickly and easily search for messages (and message content) using a standard web browser.
- **Search and Retrieval** – Authorised users can search for archived messages using the built in search tools. Users can search the content of the message, as well as any of its metadata, including To, From, Subject etc. Requests for information can be conducted in minutes, not hours or days.
- **Attachment View** – In addition to being able to search email messages and attachments, AfterMail enables users to locate attachments within the system, and identify who has sent or received these attachments. This enables users and administrators to quickly locate the most recent version of a document, and understand who sent and received the document.
- **Single Instance Store** – Only a *single* copy of any email – and any attachment – is kept, ensuring storage requirements and costs are kept to a minimum. All core aspects of the message are extracted to provide for increased accessibility and reporting, while an identical copy of the original message is also stored.
- **Organisational View of Email** – Rather than focus on email at an individual level, AfterMail enables organisations to search, view and analyse message content at an organisational level. Themes within messages can be identified, as can frequent users and recipients.
- **End User Adoption** – Unlike other document management and classification systems, AfterMail requires no user involvement, resulting in an automatic uptake by the organisation. Users will also benefit by having all of their emails – security permitting – available, and they will no longer have to worry about clearing out their mailboxes or managing multiple personal message store files.

- **Multiple Server and Platform Support** – Unlike its competitors, AfterMail is able to support a broad range of messaging servers and can also work in a mixed platform environment, where two or more of these messaging servers are used.
- **Comprehensive Reporting** - AfterMail provides comprehensive built-in reporting enabling IT and Business Managers to understand their email repository. In addition to messages, AfterMail enables organisations to report on the metadata associated with those messages: by user, recipient, organisation etc.
- **Legal and Auditing Considerations** – Once in the email system, the details of the message as well as the message itself are securely stored - complete records of activity are essential.. Messages can be located easily, including those that involve an individual or a business group, while a record of all messages is stored for auditing purposes.
- **Business Continuity** – AfterMail doesn't rely on the email server for providing access to messages once they have been archived. If the email server goes down, or needs to be disconnected due to a virus outbreak, users can still access their emails from AfterMail.
- **Consistent Security Model** – AfterMail utilises the same security model used within the organisation, enforcing security and reducing the need to administer multiple sets of logins. Users are only able to access those messages – and attachments – to which they are entitled. Any attempt to access messages that the user does not have access to is logged and can be used for auditing purposes at a later date.
- **Web Services** – Based on open technologies, AfterMail can be integrated with existing systems that need to provide access to email communications. Such read only access can be provided without modifying the email store, ensuring messages can not be tampered. EDMS and customer relationship management (CRM) systems can be provided access to email and attachment data and content.

AfterMail has been designed to be implemented quickly, with minimal impact to an organisation's email systems and existing tools. It has minimal overhead, and will work in conjunction with all existing tools and processes – including spam filters and document management systems – but provides an additional level of confidence to organisations that their corporate knowledge is being retained and, once retained, can be found again.

AfterMail is an email archiving, retrieval and analysis solution that enables organisations to capture, store and report on electronic mail messages.

AfterMail enables email knowledge management by transforming individual communication into corporate knowledge.

Legal Notices

The information contained in this document represents the current view of AfterMail Limited on the issues discussed as of the date of publication. Because AfterMail must respond to changing market conditions, it should not be interpreted to be a commitment on the part of AfterMail, and AfterMail cannot guarantee the accuracy of any information presented after the date of publication. The information represents the product at the time this document was printed and should be used for planning purposes only. Information subject to change at any time without prior notice.

This document is for informational purposes only. AfterMail makes no warranties, express or implied, in this document.

The names of actual companies or products mentioned herein may be trademarks of their respective owners.

AfterMail is a registered trademark of AfterMail Limited.

© 2004 AfterMail Limited.



www.aftermail.com