



Supporting Compliance and Discovery with AfterMail

Abstract

Recent corporate and financial reporting scandals have resulted in the need for organisations to effectively protect, monitor, manage and maintain information that could be required for regulatory or compliance purposes.

With the increased usage of electronic messaging as a serious communications and business tool, email is also subject to these laws and regulations, and commercial and public entities need to be able to store and easily retrieve email messages for many years. As email volumes and message sizes have increased, coupled with the weaknesses of many of the leading email platforms, they are struggling to satisfy these requirements.

AfterMail enables organisations to archive, retrieve and analyse email messages, helping them to quickly achieve their compliance and discovery objectives.

Introduction

Email is now an essential business tool, with the content of email regarded as a corporate record. With the growth in the usage of email, the management of email messages has become increasingly challenging; this has become even more complicated with the burgeoning legal and regulatory requirements for record keeping.

Today email contains an increasing amount of corporate knowledge. Financial reports are distributed, discussed and analysed using email; organisations use email to communicate with their customers and to make commitments and resolve complaints; and organisations make promises to other parties – internal and external – using email. Gartner estimates that in excess of 70% of an organisation’s corporate knowledge is contained within their email system.

Recent high profile cases, such as Enron, have been reliant on proving who knew what and when, and have required the examination of email history. An increasing number of everyday court proceedings also rely on email evidence, which can be used for or against an organisation. For instance, when investment banker Frank Quattrone sent an email message urging members of his technology sector banking group at Credit Suisse First Boston to “clean up” their files during a Securities and Exchange Commission investigation, this caused considerable embarrassment to the organisation and led to Quattrone being charged with obstructing federal grand jury and SEC investigations.

Regardless of which industry an organisation is in, or even its location, the management of email is becoming a critical business issue. An ever-growing number of establishments are required by regulations to archive and control access to their communications, and to maintain and store electronic data – including email – in a secure manner.

A ‘keep everything’ regime for email is the most cost effective way to ensure compliance and minimise risk.

Many of these regulations are not yet in place, and there is a limited window of opportunity to satisfy the requirements of the relevant legislation. The repercussions for non-compliance are significant, including expensive fines, and even personal penalties for company executives who do not ensure their organisations are compliant.

While many regulations do not specifically state that email messages need to be archived, the regulatory environment is constantly changing, and the legislation is often subject to many interpretations. This will inevitably affect the long-term operation of email systems. In effect, this situation has been compared to “Y2K, but without an end date.”

In addition to compliance regulations driving companies to understand how records – and email messages – are managed, consideration must also be given to how email messages are accessed, as part of a discovery process.

Email is generally “context poor” – an email message itself usually gives little indication as to its importance. More often than not it is an event or incident that determines the importance of an email; for example, a seemingly benign email can take on a whole new meaning when viewed in the context of a sexual harassment case.

It is for this reason a “keep everything” regime for email is the most cost effective way to ensure compliance and minimise risk. Of course, this can mean storing tens of millions of emails and attachments all of which is pointless unless the content is securely stored and can be easily and exhaustively searched and retrieved. Until recently conventional technology has not supported a ‘keep everything’ approach.

This whitepaper explores how AfterMail can support the requirements of these compliance and discovery issues.

Weaknesses of current systems

Email touches everyone and so regardless of the organisation, it is inevitable that it will need to deliver some form of email capture and archiving, and provide the ability to retrieve such messages at a later date.

Today’s leading email systems have been designed to transact email not manage the information contained within them. Such systems’ effectiveness in transacting email messages has become very apparent from the explosive growth in email.

Until now this has led most organisations to focus on the storage issues of email rather than the regulatory compliance and associated corporate governance issues. A storage focus often results in the management of email being delegated out to the users, with the user being empowered to decide which email messages to keep and which to delete. As a result, this leaves much of the corporate email data residing within insecure personal repositories spread throughout the organisation, which is entirely inappropriate in today’s context of risk management, corporate governance and compliance.

Of course, the rising cost of email storage and management is a real and relevant issue but this needs to be addressed as part of a compliance and governance strategy rather than in isolation. The key weaknesses in current email systems are:

- The mail store is hierarchical rather than relational which means enterprise-wide searching is very difficult.
- Messages and attachments are bound together making single instance storage very ineffective. Also, when emails are “archived” to tape there is no index of the message so searching archives is very time consuming and there is little confidence in the results of such searches.
- The message store is proprietary and so the only access to the data is via the message engine. Therefore if the mail server is unavailable so too is all of the email data.

Furthermore email systems are now mission critical but are also very fragile, in particular because they are under constant threat from viruses and hackers.

AfterMail enables organisations to capture and archive all email messages, and to provide easy and secure search capabilities of this archive completely independent of the email system mail store.

Satisfying Compliance and Discovery Requirements

Because email is so easy to produce and distribute, its value to the organisation can often be underestimated. While email can be used for personal or non-business-related communication, at most other times it is used as a business tool, assisting with the decision-making process or making commitments to customers.

With the dynamic regulatory environment there is now an increasing focus on records retention.

As more and more email is produced, this creates challenges for the organisation in a broad range of areas. Email is no longer an informal communications mechanism; now it is a business tool which can suffer from the same issues of management as any other form of communication: how to keep and file records; how to find these records in the future; and how to understand what these records may mean.

With the dynamic regulatory environment there is now an increasing focus on records retention, especially with regard to email messages and attachments. In the United States, laws such as the Sarbanes-Oxley Act and emerging requirements from the Securities and Exchange Commission (SEC) have companies in a host of vertical industries scrambling to get email archiving systems in place – and this has had repercussions for organisations outside of the US, since multinationals and any company with US-based customers will have to address these requirements.

Specifically, the requirements of these regulations relating to email retention and retrieval include the following criteria:

- Email messages and attachments must be preserved in a non-alterable format.
- An organisation must be able to automatically verify the quality and accuracy of the archiving process.
- Email messages must be fully indexed and searchable.
- All email messages must be preserved for up to six years, and in an accessible place for the first two years.
- When email messages are requested by the regulatory bodies, the stated retrieval time is “immediately.”

For organisations facing regulatory compliance requirements, a well thought-out data management plan is essential. This plan should detail how you use, retain, and retrieve your email messages. Doing so enables you to easily discover and recover pertinent data during litigation, should that occur.

Few companies have clearly defined policies about how messaging may be used, what sorts of data can be transmitted, and what types of protection messaging must have.

Enforcement of such a policy, however, is difficult if the appropriate systems and tools are not available.

Related Legislation

Regulations and legislation have been introduced in numerous countries to ensure that appropriate records – including email – are retained and are accessible. Specialists have estimated that in the United States alone, there are 10,000 laws and regulations that deem that information needs to be protected, monitored, maintained and secured. The following table lists some of these regulations, with which organisations must comply.

United States	United Kingdom	New Zealand
<ul style="list-style-type: none"> • Sarbanes Oxley 2002 • SEC Rule 17A-4 • Healthcare Insurance Portability and Accountability Act (HIPAA) • Patriot Act 	<ul style="list-style-type: none"> • Official Information Act • Public Records Act 1967 • Basel II • Data Protection Act 1998 • Freedom of Information Act 2000 • Electronic Communications Act 2000 • The Privacy and Electronic Communications (EC Directive) Regulations 2003 	<ul style="list-style-type: none"> • Privacy Act 1993 • Crimes Amendment Act 2003 • Companies Act 1993 • Electronic Transactions Act 2003 • Public Records Bill • Official Information Act

It is also worth noting that despite the country of origin of some legislation, it may be applicable in other countries. For example, the Sarbanes Oxley Act is applicable to any organisation which is trading on the US stock exchange, including non-US subsidiaries.

Compliance Issues

Numerous federal regulations affect businesses today. In the United States, financial services organisations now face rules and regulations established by the Securities and Exchange Commission (SEC), while the healthcare industry has rushed to meet the requirements of the HIPAA.

Other broad-reaching regulations, such as Sarbanes Oxley, require businesses in other industries to focus on how they safeguard, disseminate, store, and track financial information.

Outside of the United States, legislation is driving compliance and corporate governance requirements in the financial sector, in particular Basel II in Europe, and the UK's Financial Services and Markets Act 2000. Wider-reaching legislation such as the Data Protection Act also has an impact on the way in which an organisation manages, uses and retains data.

Many of these regulations determine how, where, and how long organisations must maintain electronic records, including email. Regulatory compliance is complex and should be overseen by legal counsel. The following regulations pertain to many organisations and present a simple overview of today's regulatory environment.

Legislation	Overview
United States	
Sarbanes–Oxley Act	<p>The Sarbanes–Oxley Act requires that:</p> <ul style="list-style-type: none"> • Executives of publicly traded companies certify the validity of the company's financial statements. • Section 404 dictates that organisations save all communications, including email, pertaining to certain financial processes. • Financial control and risk mitigation processes are documented and verified by independent auditors. • Companies implement extensive policies, procedures, and tools to prevent fraudulent activities.
SEC Rule 17A-4	<p>SEC Rule 17A-4 requires that:</p> <ul style="list-style-type: none"> • Original copies of all communications, including internal communications, must be preserved for a period of no less than three years, and for the first two years these copies must be in an easily accessible location. • Records are maintained, preserved, and available to be produced or reproduced using either micrographic media (such as microfilm or microfiche) or electronic storage media (any digital storage medium or system).
Europe	
Basel II Capital Accord	<p>Basel II requires that banks focus in a formalised, comprehensive manner on the operational risks that can result from external influences.</p> <p>Operational risk is defined by the Basel Committee as “the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events” including legal risk. Examples include the risks of compliance issues, inadequate record keeping, fraud, insider dealing and a variety of other potential risks.</p>
United Kingdom	
Data Protection Act 1998	<p>The Information Commission provides guidance that the subjects of email have the right to access information about the processing of their personal data and to request accurate copies of information held on them. At any time, any employee, ex-employee or customer may have the right to request a copy of all emails held by your organisation relating to their personal information.</p>

Discovery Issues

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. Not only do organisations need to ensure they have policies and tools in place that provide for the storage of these records, they need to ensure the records can be retrieved.

A company must be able to either find a relevant email or give a defensible reason why it cannot. This means storing all email and ensuring it can be found again. And if it's media-related, it needs to be found quickly; if legal-related, it needs to be accurate.

In the case of an investigation or lawsuit, typically any case-related email messages need to be made available within a specific timeframe. Email is considered valuable evidence and is often labelled the "smoking gun" of modern litigation because it preserves conversations, important business decisions and documents.

Some of the greatest challenges faced by organisations involved in such a process include:

- Determining which email messages residing within the organisation meet the discovery request;
- Ensuring that the messages that are discovered are a *true representation* of the communication that has taken place, and that nothing is missing or has been deleted;
- Absorbing the potentially high cost of discovery.

Traditional email systems make complying with such processes difficult and expensive – organisations need to be able to find information quickly and be assured it has not been tampered with. They need a "flight data recorder" for email.

By capturing all messages that are sent or received, an organisation is provided with both proactive and reactive ways of responding to discovery requests. The systems and processes that are seen to be used by an organisation can assist it when being pressured by outside forces; if the systems are perceived to be effective, then other parties may be less encouraged to pressure you.

Similarly, if an organisation can quickly provide access to all information can ensure other requests can be responded to, then it is much better positioned than if it cannot do this. In a legal situation, you hand the advantage to the other party if they have something – such as an email message – that you don't.

Discovery Costs

The discovery process can be so onerous that it becomes a negotiating tool for settlements. Some of the reasons why this process is so expensive include:

- The sheer volume of email sometimes numbers into the millions of messages.
- Specialised consultants and technicians are often contracted to extract the relevant messages from storage sources.
- Neutral third parties are often assigned to sift through email to qualify them and determine if they should be included for discovery.

Benefits of AfterMail

AfterMail provides an organisation a single, central content archiving solution for all email messages and their attachments. The solution solves the existing problems of archiving and compliance while also delivering a platform for email-enabling line of business applications.

Working with any mainstream email system, AfterMail will automatically archive and index all messages that are sent to, or received by, the email server, and then store these messages centrally. Archiving all messages in this way is the easiest and lowest route to ensuring compliance, but also enables organisations to confirm not only that they have sent or received a message, but whether a message *was not* sent or received.

In addition to archiving all current and future email messages, messages that have been sent in the past can also be migrated into the archive.

Once captured in the AfterMail system, AfterMail provides a full range of capabilities to search across messages and their attachments, according to specific criteria. AfterMail also mirrors the security permissions of your organisation, ensuring users cannot see messages they should not be able to see.

These capabilities provide a robust technology platform which organisations can use to support their compliance and discovery requirements, coupling the technology with relevant policies and procedures.

Some of the core features of AfterMail are outlined below.

Flight Data Recorder

AfterMail captures all messages sent and received – both external and internal – enabling organisations to have a complete, verifiable record of all email communications. Similar in concept to a “flight data recorder”, this ensures organisations capture all messages, ensuring they can prove whether a message has or has not been sent or received. It also ensures a definitive record of all messages and avoids subjectivity – a message that may be considered unimportant to one person, and is deleted, may be critical to the organisation.

Comprehensive Search Capabilities

Once a message is captured in the AfterMail repository, the content of the message, as well as any attachments, can be searched.

Standard email metadata can be searched, including the To:, From: and Subject fields. Message content and attachments can be also searched using a standard full-text search. Users can enter a keyword or combination of words, and the message and the attachment will be searched.

Searches can be saved, so that users can reuse frequent searches without having to enter the same criteria each time. For investigators, this means that commonly-used search criteria can be stored, and a search using those criteria can be initiated at the click of a mouse button.

AfterMail extends this functionality by also making use of RSS (Rich Site Summary) standards. A saved search can output RSS-compliant data, so that an RSS-compliant client application can be used to regularly run this saved search and then notify the user when there have been any updates to the messages found using the saved search. This provides for ongoing, proactive monitoring of the AfterMail repository.

Due to its use of standard technologies, AfterMail is also compatible with complementary and specialised search solutions provided by third parties. More advanced search capabilities can be delivered using products from organisations such as 80/20 Software, while content analysis capabilities can be provided using tools such as The Mole.

Attachment View

Particular types of attachments can also be identified and searched. For example, an organisation may want to know who first received, and then who forwarded, a proposal document or a questionable image file. AfterMail enables this type of activity to be identified and analysed.

Easy, secure access

Access to the AfterMail system and its repository is governed by the same access mechanisms that are used elsewhere in the organisation.

Logins and user permissions used by AfterMail are the same as those managed by an organisation's corporate directory service, such as Microsoft Active Directory, Windows NT 4.0 domain or any other standard LDAP directory service, enabling simpler administration and management, and ensuring that access is controlled in a consistent way. For those organisations without a central directory service, AfterMail itself can manage user login and permission details.

Tamper-proof store

When a message has been captured into the AfterMail repository, the message, and each of its attachments, is given a unique checksum identifier. Should the content of the message change, or should an attachment be modified, the checksum of that item will change, indicating it has been tampered with. This feature ensures the sanctity of the AfterMail repository, and enables any tampered information to be identified.

Auditing Capabilities

In addition to providing a tamper-proof repository, AfterMail also provides comprehensive auditing capabilities.

All searches that are performed using AfterMail are logged: the details of the search, including the keyword(s) that were searched, and the details of the person performing the search, as well as the date and time of the search are all stored in the AfterMail system.

The details of the messages that are viewed are also logged, so that in addition to determining who has searched for a message, it is possible to track who has opened any of the messages that were found. Again, this ensures the AfterMail system is being used appropriately and that the privacy of the organisation and its staff is maintained.

Ability to import past messages

Messages can be loaded into AfterMail from prior backups, or from PST files, enabling the active AfterMail content to be complemented by older content, providing a comprehensive view of email communication over a longer period of time.

Minimal Impact

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 and helps to solve the existing challenges of supporting compliance and discovery.

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. This information does not constitute legal advice and AfterMail accepts no liability for anything you may do or refrain from doing after reading this information. 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.