GFI White Paper

Why organizations need to archive email

The underlying reasons why corporate email archiving is important

Over the past few years, email has become an integral part of the business workflow. This white paper explains why email archiving must be an integral part of every organization. It also examines the different methods for deploying and managing email archive solutions in an organization as well as specifying the key requirements that a fully featured email archiving system should include.

GFI®

Contents

Introduction

Email has become one of, if not the most important communication and business tool in use by organizations worldwide. The growth of email use has not only created security and storage issues but more and more organizations are finding themselves obliged to maintain records of all emails for a number of years. Email archiving has proved to be the way forward for businesses. But why is email archiving so important for organizations?

The corporate value of email

Over the past years, email has become a primary channel of business communication. It provides organizations with a fast medium of conveying business correspondence such as purchase orders, quotations and sales transactions, in virtually any geographical area with the least physical effort possible. Research by Osterman found that 46% of email users spend more than two hours each day doing something in their mailbox while as much as 75% of a company's intellectual property is contained within email and messaging systems.

Since emails have become the electronic substitutes of legal business documentation, the information being passed on through this electronic correspondence constitutes a record. Consequently, such correspondence must be retained for a minimum period of time, often established by statutes. Due to email predominance in the business industry, various pieces of legislations have been enacted to protect personal privacy, enforce corporate governance standards and maintain ethical conduct. The Sarbanes-Oxley Act (SOX), Gramm-Leach Bliley Act (GLBA) and the Freedom of Information Act (FOIA) are some examples of such regulations.

What is the 'true' meaning of email archiving?

An email archive is a repository generally kept in a non-productive environment to provide secure preservation of email for compliance and operational purposes. A 'true' email archiving system automatically extracts message contents and attachments from incoming/outgoing emails and after indexing, it stores them in read-only format. This ensures that archived records are maintained in their original state.

Email archiving moderates the demand for storage space by reducing the amount of online emails on the mail server. Moreover email archives consume less physical storage space than other email storage methods.

The active approach adopted by email archiving solutions ensures that the company has a centralized and accessible copy of all its email. This provides additional protection against accidental or intentional deletion of emails by end-users. Email archiving also eliminates the need to search for personal archives on each and every local machine whenever litigation support is requested.

It must be noted that 'backup' and 'archival' storage serve two different purposes. Backups are intended to save current data against the event of failure or disaster whilst archives protect data so that it can be accessed when needed. The cost of finding the electronic records for a discovery process can be astronomical, requiring months of IT manpower to wade through backup tapes. Analyst firm AMR Research estimates that in 2010, compliance spending in North America will exceed $80 billion. Email archiving systems provide advanced search and retrieval functions. These allow users to track down email messages in a timely and cost effective manner. Without an effective email archiving system, finding an email record is worse than trying to find a needle in a haystack. In Murphy Oil USA vs. Flour Daniel, the defendant was ordered to restore and print the emails contained in 93 tape backups and to absorb the total costs involved to perform this operation which amount to $6.2 million.

Email archiving solutions allow administrators to setup access restrictions. These restrictions secure and protect intellectual property rights as well as ensure data integrity and confidentiality in compliance to the statutes.

What are the primary reasons to archive email?

There are four predominant reasons for an organization to archive its email. These are: Compliance, litigation support, storage management and knowledge management.

Compliance

The new regulatory environment is one of the major drivers behind the increase in demand for email archiving solutions. It is estimated that over 10,000 compliance regulations have been enacted around the world. More stringent controls and severe penalties are forcing organizations to address regulatory compliance more seriously. Morgan Stanley were fined $15 million to the Securities and Exchange Commission in 2006. According to the Washington Post, "… the SEC alleges that Morgan Stanley delayed handing over emails, destroyed others and misled SEC investigators about the efforts the firm was making to comply with the government's request for documents." A $1.57 billion judgment against Morgan Stanley was also issued in 2005 in a case where the firm failed to produce emails. The decision was overturned on appeal but the case highlights the tough stand that the courts will take if companies fail to produce email evidence when required.

Although the data subject to regulatory statutes varies by industry, all records that pertain to the organization's business activity are subject to compliance regulations. These include employee and client records, correspondence between organizations and financial documentation. For example, the Sarbanes-Oxley Act (SOX), affects all industries and imposes severe penalties on anyone who deliberately alters or deletes documents with the intent to defraud third parties. This act necessitates auditors to retain audit papers for a minimum of five years from the end of the fiscal year. Even though it is a US law, SOX is also applicable to European companies with US listings as well as to companies which do business with the US. For more information on Sarbanes-Oxley please visit http://www.s-ox.com.

Other legislations define requirements for specific regulated industries. For instance the Securities and Exchange Commission (SEC) and National Association of Securities Dealers (NASD) are two of the regulators which govern the financial community. SEC Rules 17a-3/a-4 and NASD Rules 3010/3110 oblige broker/dealer organizations to maintain and store all emails pertaining to their trading activity for a minimum period of six years. These rules also impose that for the first two years, this documentation must be kept in an indexed and easily accessible storage. Investment firms Deutsche Bank Securities Inc., Goldman Sachs & Co., Morgan Stanley, Solomon Smith Barney Inc. and U.S. Bancorp Piper Jaffray Inc. were all fined $1.65 million each for not complying with SEC Rule 17a-4 and for failing to produce emails requested during the course of an investigation. For more information on SEC and NASD please visit http://www.sec.gov and http://www.nasd.com.

Healthcare is another heavily regulated industry. The Health Insurance Portability Accountability Act (HIPAA) covers any type of records in both paper and electronic form that contains personal information and details relevant to the medical history of an individual. This information is known as Protected Health Information (PHI). Although present in probably few email messages, all organizations are bound to manage this information according to HIPAA regulations. Firms that are subject to HIPAA regulations include healthcare providers, health insurance firms, healthcare clearing houses and employers that provide health services. The preservation period for medical records varies between five to six years. However, certain statutes oblige the retention of such documentation throughout the whole life of the patient and even for two years after the patient's death. For more information on HIPAA, please visit http://www.hipaa.com.

The Food and Drug Administration (FDA) is the regulatory board which controls firms that make drugs, medical devices, cosmetics and edible goods. The set of regulations which governs record management in these industries is known as GxP. For more information on FDA and its regulations please visit http://www.fda.gov.

Government agencies too must archive email messages. These must comply with the regulations set by the Freedom of Information Act (FOIA), the Patriot Act, National Archive Records Administration (NARA) and other legislative entities. For more information, please visit http://www.usgs.gov/foia, http://www.archives.gov.

Although many regulations exist and each seems to have its own requirements, compliance is based on three main concepts:

- **Data permanence** – The notion that data must be retained in its original state without being altered or deleted.
- **Data security** – Information that is retained must be safeguarded against all security threats which include access by unauthorized persons as well as anything which could physically damage or endanger the availability of the information.

» **Auditability** – The concept of having information duly protected but easily accessible in a timely manner by authorized personnel whenever required.

Not all email is covered under compliance regulations. Some exemptions include spam that clearly does not need to be saved and personal emails, although the latter can be requested as litigation support during an investigation.

Litigation support

Nearly all companies in the course of regular business activities become implicated in lawsuits. Litigation discovery is the process in which parties involved in a lawsuit are requested by the court of law to submit information which is relevant to the case. The company which receives the discovery request is obliged to search its records and to submit all the relevant/requested information in a timely manner. The cost of producing the information for litigation can be colossal and can often outweigh the damages sought in the suit. This is most common in organizations which do not have an adequate email archiving solution in place. For example, the cost for restoring 77 tape backups in the case Zubulake vs. Warbung (UBS Bank) amounted to $165,954 and the relative review costs totaled to $107,694.

One issue with discovery requests is that there is no specific time limit which defines how far back a company must search. Organizations are required to provide all copies of email relevant to the request, regardless how backdated this may be. The completeness and availability of all the requested records and the time required to extract this information depends very much on the organization's email storage management and employee behavior. Electronic documentation can be located in every reasonable place and media. This includes email servers, PST files on desktops, laptops, PDAs, backup tapes and other removable media. Emails stored in a local message store such as an individual's hard disk or often other removable media is rarely beneficial to an employer. Apart from the high cost involved to search every single machine in an organization during a discovery request, it represents a security and intellectual property risk for the company. Furthermore, the existence of this end-user information storage is generally unknown to the IT staff members and can go unnoticed during the course of a discovery search. When email is not stored in a true (and centralized) archive, restoring it consumes a huge amount of time and money, often upwards of $25,000. Recent rulings have acknowledged that the company providing the information must endure the discovery cost, without reimbursement.

Litigation support information must be accurate, complete and possibly in its original state. Since backup systems are prone to error, loss or destruction of data may occur. An organization that fails to submit the information requested in a legal discovery can be found guilty of 'spoliation'. This is a legal term used to describe the improper destruction of evidence (for example, deletion of company email). Such circumstances can lead to a court ordered verdict for the other party or can lead the court to assume that the lost information was harmful to the party that failed to produce it. This occurred in the case Zubulake vs UBS AG Bank where due to the bank's failure to deliver the requested email evidence, district judge Shira Scheindlin instructed the jury to infer that the undelivered evidence was harmful to the bank. Other consequences for spoliation are hefty fines. Philip Morris International, one of the largest tobacco companies in the world was fined $2.75 million dollars for destroying emails in violation of a 1999 order.

Storage management

It is estimated that, one in every four organizations experiences a storage management growth in excess of 25% per year. This drastic escalation in storage requirements is mainly attributed to the increase in use of email in general, added to the upsurge of attachments, which increased the size of the average email from 22 KB to 350 KB. In fact, it is estimated that nearly 50% of organizations are providing more than 150 MB of storage per user. Organizations often make use of email storage quotas to prevent message stores from growing and degrading server performance. The downside of quotas is the effect they have on end-user productivity. Apart from stopping users from using their email whenever their storage allowance is exceeded, quotas can have more serious implications. For instance, quotas and subsequent blockages might drive users to delete important messages from their mailbox in order to make room for new email.

The increase in email usage as well as the relative growth in email size has also affected the efficiency, reliability and speed of message servers. A study by Osterman Research affirms that email stores are growing

at 37% annually. Consequently keeping email in a 'live' (online) storage format will necessitate more physical storage space as well as increasingly powerful hardware to handle these loads.

Compliance regulations have further contributed to the increased demand for storage by obliging organizations to preserve old email for predefined periods.

While storage solutions can be used to deal with the problem of message storage growth, an email archiving solution provides a more versatile way of handling this problem. Apart from centralizing your email records, an efficient archiving solution will store the emails in a compressed format, resulting in considerable disk space savings when compared to a traditional mail store. Furthermore, the emails will be automatically archived as soon as they pass through the message store, thus users can clean up their mailboxes without the worry of losing important emails. Additionally, an email archiving solution that allows authorized users to view emails from a central repository will encourage them to do without having bulky PST files stored locally. Considering the fact that PST files usually take 2 to 5 times more physical storage than an email archive, this would add up to considerable disk space savings.

Knowledge management

An organization's email system is a corporate knowledge repository. It can contain vast quantities of useful email information which is often vital to a business and allowing access to this corporate asset can make users more productive.

An email archiving system can provide appropriate knowledge management tools (for example, email records sorting, advanced search and retrieval functions) that enable IT and end-users to better manage the knowledge base contained in the company's email archive.

Deploying and managing email archive solutions

There are two main methods for deploying and managing email archive solutions:

- A completely in-house solution
- A hosted solution in which the archive is maintained at a third party's data center.

An in-house email archiving solution involves having your email repository on a server within the corporate building. Perhaps the main advantage of in-house archiving is that the organization's sensitive information is stored behind the corporate firewall and is handled by its own internal staff. This ensures better control over data integrity and confidentiality. The organization relies entirely and independently on its own resources and can therefore assess its compliance status at any time. The main disadvantage is the upfront costs involved and the sudden impact which the system might have on the company's IT department. In order to deploy an internal email archive, the company must purchase an adequate email archiving program as well as the hardware (server) which will host the archive.

Hosted solutions require lower up-front cost than in-house solutions. Customers can get up and running pretty quickly without the investment in hardware and IT staff. Running costs are also low since new capabilities and software/hardware upgrades are generally implemented by the provider. In hosted solutions, a software application located on the corporate email server captures email and migrates it offsite via the Internet to a third party data warehouse for archiving. Authorized users can subsequently access the data stored offsite using a web browser or compatible email client.

What features should an email archiving solution have?

- **Minimal user intervention/automation** – Company emails have to be archived automatically and with the minimal human intervention possible.
- **Indexing of records and search capabilities** – Archived emails should be indexed, especially the text content, so that search facilities will enable the quick extraction of records to support regulatory audit requests and legal discovery.

- **Data retention policy control** – The system must include configuration features through which the company can define its archiving criteria. These features should at least allow archiving of specific mailboxes and messages from specific domains or email addresses. In such a way, unnecessary contents such as spam and other informal correspondence is automatically excluded from the archive.
- **Security/tamper-proofing** – An email archiving system must be capable of protecting records from loss, damage or misuse. Record authenticity (i.e. preservation of a record in its original state) is one of the key requirements in many of the content regulations imposed by the laws. In addition, archiving programs must include access restriction features.
- **End-user and management access to archives** – This feature allows a company to use its email archive as a central knowledge repository from where authorized users can extract information required during productivity. One further benefit is that it enables authorized users, such as compliance officers, to access the information contained in the archive without the need for support by IT staff.
- **Support for multiple messaging platforms** – The archiving system should support all major messaging platforms to ensure standards compatibility.

About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized enterprises (SMEs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy and a strong focus on the unique requirements of SMEs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at http://www.gfi.com.

References

Osterman Research – http://www.ostermanresearch.com.

Messaging archiving Market Trends, 2005-2008.

Sarbanes-Oxley Compliance Journal – http://www.s-ox.com.

Compliance Pipeline – http://www.compliancepipeline.com.

Transform Magazine – http://www.transformmag.com/compliance.

U.S. Securities and Exchange Commission – http://www.sec.gov.

National Association of Securities Dealers (NASD) – http://www.nasd.com.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

GFI 1038 may11

GFI®