Using Email Archiving to Protect your Business

Data Storage Corporation
Excellence in Data Protection and Recovery

Message Logic is a business unit of
Data Storage Corporation. 212-564-4922
www.messagelogic.net or www.datastoragecorp.com

Protect Your Company with Email Archiving

Introduction

The U.S. Supreme Court has declared that electronic messages are corporate records and must be preserved and produced when requested. Regulatory bodies such as the SEC, FINRA, FASB, and the FDA along with federal regulations such as the Freedom of Information Act and Sarbanes-Oxley are all enforcing this requirement. These regulations are also being extended to countries worldwide. Yet without automation, it is nearly impossible to meet these regulations, stay in compliance, and produce requested information when necessary while protecting what's important and confidential to the organization.

Consider:

- More than 84 billion emails are sent every year
- Email is evidence in 8 out of 10 court cases
- More than 150,000 requests for information under the Freedom of Information Act have been made
- If done right, Email Archiving can be an effective tool to protect one of your organization's most valuable assets and meet the above regulations.

The Requirements for Email Archiving

Email Archiving started with rules imposed by the SEC and FINRA on financial firms. They realized that many brokers were communicating by email with clients about financial transactions. They had clear rules about the language that could be used in written communications, but the rules didn't explicitly include email or other electronic communications such as Instant Messages.

Today the SEC requires that any documents pertaining to the "business as such" must be retained for a minimum of three years and for the first two years they must be readily accessible. Emails are now defined as business records and are subject to business record retention requirements. Also, in numerous cases, firms using a tape backup solution were unable to recover all of the saved files. They found that data integrity cannot be ensured when using tapes. In many cases, up to 20% of the data is likely to be lost over time due to failure of the media alone. Similar rules to those imposed by the SEC have now been adopted by regulatory bodies in virtually every industry. You can summarize all of the requirements as follows:

- Companies must have a reliable capture of email (email archiving) and in some cases Instant Messages.
- A "Reasonable Retention Policy" must be enforced by the company
- Fast search and retrieval (discovery) is required when the information is summoned
- The company must assure that evidence is not deleted (litigation hold)

And one that is not required today, but we believe is prudent and most likely will be required in the near future:

- Companies will need an on-going policy management (monitoring) to gain control of what is being sent and archived.

The requirements, which make these issues a priority for legal departments, HR, and IT include the following:

- Federal Rules of Civil Procedure (FRCP)
- Freedom of Information Act (FOI or FOIA)
- State adopted Freedom of Information Act's (state given name)
- State Open Meetings Laws
- PCI Compliance
- HIPPA
- SEC, FINRA requirements
- Patriot Act
- Sarbanes-Oxley
- Early Case Assessment
- Corporate Policies — (Acceptable use policy, HR policies, trade practices, protection of corporate intellectual property)

Given the above regulations and requirements, everyone needs to archive email. To summarize:

1) Every organization needs to maintain emails as corporate records.
2) Periodically the messages may need to be produced if requested by a regulatory body, Freedom of Information request or through the Federal Rules of Civil Procedure or courts during a discovery process.

Keep Your Company Safe: Know What You Are Archiving

If the proper steps are taken, then you will be keeping all of the required records and have a system in place to produce them when requested. ***But do you really know what's in your archive?*** At any moment you may be required to perform a search of your records and present them to a regulatory body, court or for internal use such as an employee concern, product issue, or financial due diligence.

I'm sure the executives at Goldman Sachs had no idea that they would be brought before a Senate hearing and be embarrassed by the statements, profanity and attitude contained in their corporate records pertaining to the mortgage crisis.

Recently, Goldman Sachs mandated its employees to refrain from using profanity in any electronic messages. "During a Senate hearing in April, an email with profane language sent by an executive in the company's securities business sector came to light and embarrassed the organization. This led to the institution's new communications policy, which will be enforced. The company's policy will not allow any profanity or even hints at it, meaning any words with asterisks acting as guards are illegal".

Keep Your Company Safe: Retention Management

The importance of having a retention policy is that it allows the organization to delete messages at the end of the policy as long as they continue to maintain any records which are involved in a litigation or regulatory matter. This also may reduce the scope of any potential discovery re-

quest to the retention period and reduces long term storage costs. The Federal Rules of Civil Procedure (FRCP) along with more specific industry regulations all have a provision to define a retention policy. The FRCP state that corporate records such as email must be maintained for a "reasonable" about of time. Reasonable is different in every industry.

For example, certain types of medical records need to be maintained for the life of a patient. Similarly, Pharmaceutical companies need to keep specific records from the trial phase to the life of the drug. However, for both medical and pharmaceutical companies, along with most organizations, normal business communications tend to have a retention requirement of 3–7 years. The key is to make sure the organization adheres to the policy. In the case of AMD vs. Intel, Intel's retention policy was called into question after finding that employees were keeping emails longer than the corporate retention policy.

Keep Your Company Safe: Proactive Monitoring

If we assume that your archive is going to hold all the emails (and possibly IMs) from your company, and then within them lays valuable information as well as possible "issues." It is those issues that may be questioned in the future and then will need to be defended by the organization.

In most cases regulators require that you maintain "business records" and be prepared to produce them. However, if you try "selective" archiving you had better be prepared to have strong, enforceable policies and a process that will stand up in court defining why you delete some messages and not others. In nearly all situations, the best practice has been to archive all inbound, outbound and internal messages that go through your corporate email systems. And if required the same applies to Instant Messages.

Proactive monitoring and alerting senders of policies will reduce the number of possible future issues. In addition to litigation, and compliance requirements, nearly all organizations have an "email use policy" or similar document with strict guidelines on message content and appropriate behavior. However, very few organizations have a tool in place to monitor and enforce these policies. With so much valuable information contained in email, it's important to know exactly what you're archiving. Otherwise, you are waiting for a lawsuit or information request that could potentially damage your organization financially, not to mention its reputation.

This may sound difficult, but it really isn't with the right tools. By actively monitoring your email, you can set up alerts and reports that let you know if potentially damaging emails are going into your archive and who is sending them. This will help your organization reduce or eliminate issues before they become huge problems in the future. It is always better to know about possible violations in corporate policy right away so you can address them and prevent more problems in the future. For example, if your policy is that employees cannot send messages that contain personal information such as social security numbers, then any employee that does can be immediately notified when they mistakenly send out a policy breaking message. If the behavior continues, management can be notified. It's amazing how behavior can change when someone is alerted to issues or mistakes. The organization should not need to find out at the time of a regulatory or legal inquiry that they have been breaking PCI policies for years and

could be held liable. Knowledge is the key. Any executive should be able to look into their archive and get a good understanding of what's going on in the business and have the tools at their disposal to modify policies. Email is a corporate record, just like any document. No one would ever use profanity, harassing language, or personal information in a corporate document, but you would be surprised what you find in email.

Good email archiving tools should include a monitoring function that gives management the ability to identify and alert the sender as well as management if bad behavior continues on issues such as:

- Use of profanity
- Potential harassment or inappropriate content
- Presence of social security numbers or credit card information in violation of PCI compliance
- Inappropriate trading terms not permitted by the SEC or FINRA
- Monitoring for data leaks
- Specific industry issues

All of these items, when found in emails during a regulatory inquiry or legal action, will cause issues.

Keep Your Company Safe: Index the Archive

Another important aspect of an email archiving system is to make sure that the system effectively indexes the archive. Automating this process has proven to be a big benefit to IT. Today, IT is typically responsible for finding the information needed by Legal, Compliance, HR, Finance and other organizations. Having a system in place which has indexing of all of the information can make it as easy as running a query against the archive to quickly produce the requested information. In many cases the mandated time frame to respond is just days and without such a tool, this would be a very expensive process. Another big advantage of a good indexed system is the ability to perform periodic "early case assessments."

Having the information categorized and indexed allows the company to assess a situation quickly.

What if an employee was to make a claim and threatening legal action for being unfairly treated by other employees or management? A quick assessment of all the email communications between the parties could determine if this claim is valid and the organization can decide the correct course of action.

Rules You Should Know

The following regulations are being regularly enforced today. Your obligation to understand these and comply with them is important if you are to avoid excessive litigation and cost.

Freedom of Information Act

On January 21, 2009, President Barack Obama issued Executive Order 13489 that encourages openness, transparency and accountability in government records. In addition, he is promising to reinvigorate the Freedom of Information Act by opening more of the government's filing cabinets to the public without a fight. It can't happen soon enough for the people awaiting replies to more than 150,000 requests for information.

Schools, local government, state government, municipalities, government contractors, consultants, branches of federal government, senators, and congressmen to name a few, are all subject to these requirements. Email communications can be requested by the public or courts and may need to be produced.

Federal Rules of Civil Procedure

The new Federal Rules of Civil Procedure, during the Meet and Confer stage of a lawsuit (first 120days), allows either party to request information which must be produced by the other party at their cost. The courts have little patience with organizations who claim they are unable to comply with broad e-mail discovery orders because of information system design flaws. The bottom line is that e-mail discovery can burden organizations that have not implemented rules and invested in technology to retain and access the required e-mail.

FRCP Rule 37(f) protects organizations from sanctions for deleting email as part of "routine, good-faith operation." This so-called safe harbor provision protects organizations that delete documents as part of ordinary business activities. Unfortunately, "routine, good-faith operation" is not defined. The authoritative Advisory Committee on Civil Rules said that an entity would usually be protected if it took "reasonable steps to preserve the information after it knew or should have known the information was discoverable".

FINRA (Financial Industry Regulatory Authority)

The Financial Industry Regulatory Authority recently announced it has handed out more than $20 million in fines in 2010. FINRA's fines are in response to various violations committed by the brokerage firms it governs, ranging from misleading advertising to licensing violations. However, one major trend Washington-based lawyer Brian Rubin noted is the authority's increased devotion to email retention policies. Any firms without sufficient retention or email archiving policies in place could face fines for failure to produce messages.

Investment bank Piper Jaffray received such a fine in May when it failed to produce 4.3 million sent and received emails between 2002 and 2008. FINRA issued a $700,000 penalty for this violation.

PCI Compliance

The Federal Trade Commission is educating consumers and businesses about the importance of personal and confidential information (PCI) privacy. Under the FTC Act, the Commission guards against unfairness and deception by enforcing companies' privacy promises about how they collect, use and secure consumers' personal information. Under the Gramm-Leach-Bliley Act, the Commission has implemented rules concerning financial privacy notices and the administrative, technical and physical safeguarding of personal information, and it aggressively enforces these rules against pretexting (using false information to obtain personal information).

The Commission also protects consumer privacy under the Fair Credit Reporting Act and the Children's Online Privacy Protection Act. Personal,
Confidential Information such as social security numbers, credit card information, birth dates or other information of a personal nature can not be transmitted to a third party and must be kept confidential and secure to preserve an individual's privacy.

HIPAA

HIPAA covered entities are also required to retain a wide range of documentation regarding their compliance with the regulation. In general, documentation must be retained for six years from the date of its creation, or the date of last effect, whichever is later (though some states mandate longer retention periods).

Documentation that must be retained includes:

- Policy or procedural documentation: Including notices of privacy practices, consents, authorizations and other standard forms
- Patient requests: Such as requests for access, amendment or accountings of PHI disclosures
- Complaints: Documentation related to the handling of patient and/or HCO employee complaints
- Training: Including processes for and content of workforce training.

An increasing number of email messages sent or received by HCOs could fall into these categories, and in some cases, may only exist in email. HIPAA does not explicitly state that emails must be maintained, but evidence suggests that many records that must be maintained are in emails.

Securities Exchange Commission

According to SEC Rule 204-2 all books and records (including emails) required to be made… shall be maintained and preserved in an easily accessible place for a period of not less than five years from the end of the fiscal year during which the last entry was made on such record, the first two years in an appropriate office of the investment adviser.

In addition, SEC Rule 31 states that records to be preserved by Registered Investment Companies, Certain Majority-Owned Subsidiaries Thereof, and Other Persons Having Transactions with Registered Investment Companies must be Preserved for a period not less than six years from the end of the fiscal year in which any transactions occurred, the first two years in an easily accessible place, all books and records required to be made pursuant to paragraphs 5 through

12 or Rule 31a-1(b) and all vouchers, memoranda, correspondence…

And, Rule 17a-4 states that every member, broker and dealer shall preserve for a period of not less than 6 years, the first 2 years in an easily accessible place, all records required to be made pursuant to Rule 17a-3(a) which includes all originals of all communications received and copies of all communications sent by such member, broker or dealer (including inter-office memoranda and communications) relating to his business as such.

Patriot Act

Section 215 of the Act allows the Director of the FBI to get some types of business records if these records are believed necessary to investigate terrorism. In the beginning, a court order was necessary, but this was changed so that a court order was no longer a requirement. Arising from the Patriot Act, the development of not only retention schedules, but destruction schedules for all categories of records including electronic records and email became top priority in many institutions. In essence, a formal records management policies and procedures manual became necessary.

Sarbanes-Oxley

SOX 802 imposes criminal liabilities on the improper destruction of business documents, including e-mail. When Congress passed SOX in July 2002, it imposed new accounting and financial reporting requirements on publicly traded companies. These impacts all companies traded on US exchanges with revenues in excess of $75 million and also apply to private companies to some degree Section 802 addresses the retention and destruction of records, with implied penalties. Under Section 802 it is a crime for anyone to intentionally destroy, alter, mutilate, conceal, cover up, or falsify any records, documents, or tangible objects that are involved in or could be involved in, a US government investigation or prosecution of any matter, or in a Chapter 11 bankruptcy filing. Section 802 stresses the importance of record retention and destruction policies that affect all of a company's e-mail, e-mail attachments, and documents retained on computers, servers, auxiliary drives, e-data, web-sites, as well as hard copies of all company records. The rules state that any employee who knows their company is under investigation, or suspects that it might be, must stop all document destruction and alteration immediately. And, the employee must create a company record showing that they have ordered a halt to all automatic e-data destruction practices.

Private companies are also expected to comply with SOX 802. Private companies now face fines plus up to twenty years imprisonment for knowingly destroying, altering or falsifying records with the intent to impede or influence a federal investigation

Message Logic — A Solution For Even The Most Demanding Email Archiving Challenges

The Message Logic email archiving product is a sophisticated archiving, monitoring, and indexing product that is specifically designed to meet the requirements outlined above. Message Logic intelligently processes the content of electronic communications based on its unique PreSearch™ technology which looks at every message, including the body text, headers, hidden text,

and any attachment text to including the body text, headers, hidden text, and any attachment text to categorize and index the message. The result is a sophisticated and powerful email archiving, electronic discovery, and content monitoring tool with real-time notifications for compliance and email archiving management. The Message Logic solution is available as a hardware appliance, VMware software or SaaS hosted service.

Message Analytics

Message Logic's unique Analytic technology looks at every message, including the body text, headers, hidden text, and any attachment text. Analytics uses three techniques to categorize the message:

- Sophisticated proprietary language models
- Power Search with word lists
- Pattern matching

To develop the sophisticated, statistical "language models," Message Logic assembled tens of thousands of messages from many organizations. Message Logic then built statistical models of these messages to create 80 distinct categories and measures.

When the Message Logic Appliance processes a message, it compares the message to the language models and performs a complex analysis to see if it falls into any of the 80 different categories and measures. Each message is analyzed in its entirety, not just for individual word matches. The analysis includes the message body text, headers, attachments, and hidden text. Message Logic augments this process with additional methods. Message Logic created word lists and customer generated word lists to quickly find some more obvious problems. Sophisticated pattern matching finds privacy and several other violations, such as credit card number leaks.

The result is a highly effective solution that finds messages that other systems miss.
Once the analysis is complete, the message is scored for each of the 80 categories and measures, including privacy, the presence of likely social security numbers, trading terms, confidential information, user defined categories, and potential harassment (offensive content). The relevant score for each message is compared to the threshold score for each category. When a message's score exceeds the threshold, it is then placed into that category.

Real-Time Alerts and Scheduled Reports

Message Logic's real-time alerts and scheduled reports provide an early warning system for potential problems. Once the message is categorized and within seconds of when a message was sent or received, Message Logic can send a custom email to the sender, recipient, administrators, the human resources department, security personnel, and/or a third party. As a result of this approach, urgent matters can be attended to, even if the email recipient is not present to receive the message. If immediate notification is not required, the Message Logic system can be set-up by any user to send a scheduled report on a daily, weekly, or monthly basis. Any search, including those that use a single word or those that use a complex Boolean expression, can be saved and scheduled.

The Message Logic Track Record

Message Logic email archive solutions are being used by companies located around the world. Message Logic customers are in every industry and include financial services firms, health care organizations, K-12 schools, state and local governments, life sciences companies, transportation companies, and manufacturing companies. All of these businesses have regulatory, legal, IT or policy requirements they needed to meet.

Summary

People, especially in the business world, communicate through email now more than ever. Now that everyone is required to treat email as a corporate record and retain and produce email when requested, it is critical to "know what you are archiving" and start enforcing good corporate policy.

An email archive with monitoring and alerting capabilities as well as a strong indexing capability presents a unique ability to enforce corporate policies, regulatory requirements, and best practices while keeping you informed of potentially dangerous information that may become future evidence. The regulations are not going away and daily you hear about more people and companies getting in trouble due to how they communicated by email. Good archiving practices will save time, money and protect one of your organizations biggest assets.