

Realtime
publishers

The Essentials Series:
Operations Benefits of Email Archiving

The Benefits of Meeting eDiscovery Requirements

sponsored by



by Jim McBee

The Benefits of Meeting eDiscovery Requirements1
 Understanding eDiscovery Requirements.....1
 Getting a Handle on Compliance.....3
 Legal Compliance3
 Internal Policy Compliance.....4
 Executive and Legal Buy-In5
 Data Integrity and Chain of Custody5
 What Should You Retain?5
 Meeting eDiscovery Requirements Through Email Archiving6

Copyright Statement

© 2008 Realtime Publishers, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers, Inc or its web site sponsors. In no event shall Realtime Publishers, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

The Benefits of Meeting eDiscovery Requirements

When email administrators and Information Technology (IT) management meet to discuss their future plans, the subjects of eDiscovery and email archiving are common topics. eDiscovery introduces new challenges that IT organizations may have never faced in the past. Providing current and historical email data may be time consuming or, depending on an organization's retention policies, historical email data might not even be available.

Email archiving is the best way to meet eDiscovery requirements as well as ensure that the organization remains compliant with applicable laws and regulations. Although email archiving projects are frequently managed by the Exchange Server administrator, the choice of email archiving software must be carefully evaluated by management. Archiving software must provide the necessary functionality to not only archive email but also meet legal and organizational requirements. This article will explore some of the basics of eDiscovery, legal compliance, and how an email archiving system can help an organization to meet eDiscovery requirements.

Understanding eDiscovery Requirements

If a law requires you to retain information for a period of time, any type of litigation or civil action that uses that law as a basis will require you to produce that information. eDiscovery of such information can prove both time consuming and extremely expensive.

The Traditional Discovery Process

To appreciate the benefits of eDiscovery, consider a situation encountered early in my career. I worked providing IT support for a law firm; one of our clients (a large chemical company) was being sued to clean up ground waste left at several of their sites. The plaintiff in the suit was requiring the firm to produce any records that mentioned a particular chemical, including scientific documents, letters, and memorandums over a 5-year period. Naturally, our attorneys required access to this information as well.

Our firm took delivery of approximately 700,000 documents from the client's warehouse. Our litigation support team's job was to review each of these documents for chemical names, site names, and names of executives/management. Each document was numbered and an index sheet was created by the document reviewers. Paralegals then reviewed the documents that were of value.

The document reviewers then passed the documents to a data entry team that entered the key terms and document number into a database (this was before document scanning and online reviewing). My job was to maintain the system. Once the documents were indexed, the attorneys could quickly locate specific documents they required and have the documents pulled from their respective boxes. During the 6-month process necessary to index and enter this data, the firm sent a customer a litigation support bill of nearly \$500,000 per month to pay for the 25 full-time employees required simply to prepare information for the attorneys.

A modern email archiving system with appropriate eDiscovery components would completely eliminate this entire process except for the final piece—the search.

Usually in a civil or criminal lawsuit, an organization is asked to produce all records relating to the suit. For example, the organization's email administrator would then be responsible for providing all information related to a topic over some period. Even if the administrator had maintained backup tapes for the past several years, how long will it take them to comply with a court order that requires the organization to

- Produce all email conversations relevant to a particular topic over a 5-year period
- Provide a guarantee that the data is complete
- Provide a guarantee that this information has not been altered
- Provide this information in a "reasonable" amount of time

Organizations that are not able to provide this information can be fined millions of dollars. For example, shareholders of PriceWaterhouseCoopers (PWC) were awarded \$139 million in damages because PWC failed to comply with discovery rules. In the case, the judge ruled in favor of the plaintiff after determining that PWC had acted in bad faith when producing email, metadata, documents, and databases and that PWC had failed to protect data from alteration (Sources: <http://www.nytimes.com/2005/01/12/business/12account.html> and <http://my.advisor.com/doc/17382>).

eDiscovery from the Archive: A Practical Example

Consider the following example, which illustrates a practical benefit of a mail archive system. A situation occurred in an organization in which management learned that several employees were engaging in activity that was an extremely gross violation of the employees' acceptable use policy and could result in lawsuits against the organization if left unchecked.

The "leak" that tipped off management also quickly worked its way back to some of the employees in question. One of the ring leaders sent an email to his fellow miscreants instructing them to delete all emails relating to their activity, empty their deleted item folders, and then delete all mail from the deleted item cache.

Naturally, management was a day slower in reacting to this crisis, but authorized the review of two of the employees' mailboxes. Nothing was found until the email archive was searched. The archive kept a complete copy of all emails sent and received; thus, all the offending information was found. A complete picture of these employees' activities was produced, and the chain of custody was documented and preserved. During this internal eDiscovery, the email conversation with other offenders and minor players was uncovered.

The company's Human Resources department quickly fired the ring leaders in this activity and disciplined several minor players. The company's legal council believes that by acting quickly and decisively, they were able to avoid any potential liability. The company's legal council and Human Resources departments credit the ability to quickly produce the necessary evidence against the employees.

Incidentally, the ring leader of the group, upon being notified he was being terminated from his job, claimed there was no evidence that he had done anything wrong and that he would sue them for wrongful termination. The Human Resources department and his manager then produced a stack of email and the audit logs from the email archiving system, including his "delete all the evidence" email from 3 days prior. The employee then left quietly.

Getting a Handle on Compliance

When an organization starts to address compliance requirements, the first question that should be answered is “With whom or what are you trying to comply?” Compliance is usually thought of in terms of conforming to legal restrictions placed by an outside entity.

In the past, retention and records management consisted of boxing up memos, letters, proposals, invoices, purchase orders, meeting minutes, and so on. These boxes were then shipped to an environmentally controlled and guarded warehouse. This information was kept for some period of time based on internal or external policies; though sometimes the information was stored but never purged after its retention period had expired, thus increasing the business’ warehousing costs. Nonetheless, official business communications were retained.

A 2007 study published by the American Bar Association (ABA) estimates that more than 90 percent of all information is now electronic and that more than 80 percent of all company communication is now sent via email (Source: *The Electronic Evidence and Discovery Handbook: Forms, Checklists, and Guidelines*, written by Sharon D. Nelson, Esq. and John Simek, published by the American Bar Association, and available at http://www.abanet.org/media/youraba/200709/electronicInfo_07.html). Email is considered an official mechanism for business communication that may be subject to internal retention policies. However, too frequently, electronic record retention and long-term storage is ignored completely (or at the very least, not well planned) until there is a requirement to retrieve an important piece of information. The ABA study estimates that only about 35 percent of organizations have email retention policies.



Not all email archiving systems retain all data necessary for compliance (with internal policy and/or external regulation). An archiving system that periodically “harvests” email from the mail server will not have all information that passed through a user’s mailbox. Enabling Exchange Server journaling may help ensure the retention of necessary information but will not record all transactions that occur in each user’s mailbox. In addition, enabling mailbox journaling places tremendous additional overhead on the system. When considering an archival implementation, have a clear idea of your compliance requirements in order to find a solution that retains all necessary data.

Legal Compliance

It is likely that at least one of the many existing laws and regulations that require the retention of data for a set period applies to your organization. In addition, that data must be recoverable in a reasonable period of time. For example, the U.S. Sarbanes-Oxley Act (SOX) requires that certain data relating to accounting and finance be retained for 7 years. The U.S. Title 21 CFR Part 11 law requires that records be maintained for up to 5 years. The European Union (EU) requires member states to enact similar data retention and protection laws.

Although such laws and regulations state the need for records retention for a period of time, they do not specifically define a technical vehicle for compliance. Thus, each organization must determine a reasonable approach for complying with the law.



If your organization was required by court order to produce all financial information that was distributed via email, would you be able to do so? Morgan Stanley paid \$15 million dollars because the company could not produce requested emails (Source: <http://www.computerworld.com/hardwaretopics/storage/story/0,10801,108687,00.html>). The government fines and legal costs were far more than the cost of an email archival system that could have immediately produced the necessary data.

Internal Policy Compliance

Records retention policies are nothing new for most organizations. The challenge now is to extend these policies to include electronic records. Internal records policies may exactly match retention policies placed on an organization by a government entity (internal retention should, at minimum, meet the government-required retention levels) or might include additional data that is of use only internally.


The U.S. amended the Federal Rules of Civil Procedures in 2006 such that companies are now required to document and retain email as part of their standard operating procedures. If requested, organizations must also provide requested emails within a reasonable amount of time. Requested data must be provided in its native format with metadata intact. For email data, this includes information such as whether a message was read, replied to, forwarded, flagged, and so on.

U.S. federal government agencies are required by the U.S. Freedom of Information Act (FOIA) to partially or fully disclose government information. FOIA defines the types of information that must be disclosed upon request and the timeframes under which the agency must provide a response. Countries such as the United Kingdom have similar laws, such as the U.K. Freedom of Information Act 2000. Within the U.S., many state and local governments also have laws that require disclosure of government data within a reasonable amount of time.

Additional U.S. laws affect organizations that handle financial and securities transactions and those that do business with the government. These laws also require specific retention periods for some types of data. For example, a privately held civil engineering firm that does business with the U.S. government is required by U.S. Federal Acquisition Regulations (FAR) Subpart 4.7 to retain all records relating to their government contracts and be able to provide that data for review. Per internal retention policies, the engineering firm might want to also retain non-government-related electronic records such as designs, technical discussions, accounting records, and proposals.

Executive and Legal Buy-In

Who is culpable if your organization is not meeting a legal requirement? Ultimately, the company executives are responsible; thus, any project that will help bring your company into legal compliance must include executive-level sponsorship as well as oversight by your legal department. It is unnecessary for executives and legal council to attend every feature, configuration, and server installation meeting, but they should be fully briefed on the capabilities, auditing measures, initial costs, and long-term costs of an email archival solution implementation project.

 When properly briefed on your organization's requirements to be legally compliant, executives and legal counsel will better help you fund a system that will completely meet your needs. Be prepared to present your case for the solutions you are considering in terms of business and legal value.

Data Integrity and Chain of Custody

When information is requested during the eDiscovery process and must be passed on to either an organization's own counsel or opposing council, preserving chain of custody becomes very important. The controls placed on information, who has access to information, and whether information is protected must all be considered. An inability to document these considerations might make the data tainted and inadmissible in court; further, you might be found in violation of the law and subject to fines. Part 34(b) of the U.S. Federal Rules of Civil Procedures requires that electronically stored information be produced with its metadata intact and that the organization be able to provide a documented chain of custody. U.S. Title 21 CFR Part 11 requires that the original content and meaning of preserved records is accurate.

Any type of data retention mechanism or retention policy that is required by law should also provide stipulations to ensure the data has not been spoiled. Spoliation may occur either when the system or an authorized user alters data (either intentionally or unintentionally.). As information is turned over to opposing council in litigation, the organization must be able to preserve chain of custody. Technologies such as MD5 or SHA-1 hashing can be used to create digital signatures that will verify that data has not been changed.

What Should You Retain?


The best time to determine what data your organization needs to retain is during the process of selecting and evaluating an email archival system. At this time, you will better be able to compare the feature sets offered by different vendors and select a solution that meets your organization's specific compliance and eDiscovery requirements.

Although a review of your organization's paper records retention policies might seem like a logical starting point, this approach might not adequately define a policy for email retention. Instead, consider your organization's organizational structure and the roles that individuals fill. Email retention should at least partially be based on an individual's roles or job responsibilities. For example, executives' email data might be retained for 7 years while an account clerk's messages might be retained for 3 years.

Each organization and industry will have different requirements, and those affected by more stringent local, state, federal, and international regulations will face much more strict requirements. The following list highlights additional questions that should be reviewed by not only the IT department but also management and legal council:

- What local, state, federal, and international laws affect our industry and place a records retention or eDiscovery burden on us?
- Should records be archived at some point in time in the future or should information be retained immediately upon transmission or delivery?
- Do we produce any type of intellectual property that should be retained, such as legal documents, engineering drawings, computer code, formulas, and so on? Should we retain email discussions relevant to that intellectual property?
- How do we handle email that does not fall into any specific category?
- Whose email should be archived and how do we stay on top of the requirement to archive or retain an individual's mail as they move between job functions within the organization?
- What are the different job functions or organizational roles within the organization and how will email retention policies differ between these roles?
- What types of data should be retained? Should this include calendar items, contact information, tasks, and personal journals? Should email message metadata be retained for each message that is archived?

As you move forward with email archiving plans, ensure that you address these questions and that you are moving necessary data to the archive and retaining it for the required period of time—not only for your internal usage but also to comply with laws that affect your organization.

 Exchange Server 2007's messaging records management feature allows an email administrator to create folder structures that users can employ for information that must be retained for long-term use. A MAPI-based email harvesting system then moves that data to the email archive. A weakness to this strategy is that the user **MUST** participate in the retention; if the user inadvertently or intentionally ignores this process, the required data is never archived.

Meeting eDiscovery Requirements Through Email Archiving

By some estimates, implementing an email archival system can immediately help reduce your Exchange Server's storage requirements by a significant amount. Reducing the total size of Exchange Server databases will improve database engine performance, reduce the time necessary for backups, and reduce the time that nightly online maintenance takes to complete.

At the same time, the archive system is providing end users with fully indexed data and nearly limitless mail storage options. This seems like all the justification that most organizations would need to move ahead with email archiving plans.

The real value in an email archival system may only begin to manifest itself when IT begins to investigate their organization's records retention policies and how the retention policy affects electronic data. Courts are now treating electronic data the same way they treat printed and physical business records: as official business communications. For this reason, it is imperative that any type of official business communication be retained for legally required periods of time. Many businesses are now affected by local, state, federal, and international laws that govern information retention—and that includes electronic information.

However, simply moving terabytes of data into an archive may not ensure complete compliance. Some laws include the stipulation that, upon demand, these records can be produced in a reasonable amount of time; this may even mean within 48 hours of the request. Email archival systems continue to add value by providing authorized users the ability to search and discover requested content across the entire archive.