



MIMOSA
SYSTEMS

A White Paper

By Bob Spurzem
Mimosa Systems, Inc.

August 2006

■ Electronic Discovery for Email

CONTENTS

Are you Ready for Electronic
Email Discovery.....3

Electronic Discovery on
Microsoft Exchange Server5

Email Discovery for Exchange without
Journaling.....7

Conclusion.....8

Are You Prepared for Electronic Email Discovery?

Recent surveys reveal that half of organizations have performed electronic discovery for one reason or another. So if you have not been asked to search your electronic records, count yourself as one of the lucky ones. But be prepared, because you are likely to be asked in the near future. Over 80% of organization records exist in electronic form, so it stands to reason that to perform even the most basic search, proper preparation is necessary. Electronic search is no simple matter when you consider that the data exists anywhere in the organization from servers to desktops and it exists in multiple, non-compatible formats.

One category of electronic information that requires immediate attention is your organization's email. The reason email is so important for electronic discovery is that email is the most important form of business communication in your organization. It contains vast amounts of very important information and perhaps is the only source of business transaction information. For example, your sales force is likely to use email for its customer communication. They email pricing quotes, enter into negotiations and close deals all by email. And just like traditional paper communication, this important information must be preserved as a business record.

Email is a challenging electronic store of information to search for two major reasons. First, email is an unreliable information store because users can delete email and attachments at will. You have no guarantee that the messages that enter your email system will be available at a future time for discovery. Second, email is highly mobile and can exist in multiple locations simultaneously. Users can create, send and forward email items completely at will. This makes it for all practical purposes impossible to perform a deterministic search when you cannot be sure if you have completely searched all locations where email can exist. When you search the email servers, do you need to search all desktops? What happens when users send email to home PCs, how do you search this information?

Many active forces are driving the need for better email data management for electronic discovery. A watershed event occurred in early 2003 when the SEC fined five major Wall Street firms a total of \$8.25M for not keeping certain e-mails for the required period of time. While the financial services industry was directly impacted by this event, the chips began to fall for other major industries. In addition to financial services, important regulations that mandate preservation and protection of electronic information exist for healthcare, education, government, consumer financial services and all public corporations. The SEC rules are the most widely quoted and the most precise – they specify requirements for data type, retention time period, accessibility, preservation and protection. The Sarbanes-Oxley Act of 2002 similarly mandates the preservation of financial records and audit papers for specific periods of time and authorizes severe penalties for non-compliance.

“Email has become an important source of information in a lawsuit...As a result a well managed email archiving system is vital to an organization's ability to mitigate legal risks from a lawsuit.”

Michael Osterman
Osterman Consulting

Without overlooking the importance of compliance, a second driving force for electronic discovery is the day-to-day demands to search company records. Let's create a simple example. How would you produce all the email that "Employee A" sent to "Employee B" on a specific date? If you are Microsoft Exchange shop, an approach would be to logon to the mailbox of Employee A and perform an "Advanced Find" specifying the "Sent To" and "Time" parameters to match the search. The major flaw in this approach is that you have no assurance that your results are complete. Employee A could have deleted email after sending, so that it is not available. Employee B may have a copy of the email, or perhaps forwarded it to someone else; so again you must follow an unreliable path in search of potential information.

Organizations that have had to perform electronic discovery know first hand the pain and expense involved. Costs can quickly run into the thousands (and millions) of dollars to perform even a basic search of email records. In our previous example, it is very costly to have to search and find email when you consider the necessary steps to perform a complete search. Email servers themselves are straight forward enough to search, but searching all desktops and laptops is almost mind boggling if thousands of machines are involved and not to mention highly disruptive to the organization. An email search does not stop there. Any thorough email search must also include backup tapes that contain copies of email and potentially email that was deleted. Backup tapes are time consuming to search and require dedicated server and tape resources. When tape backups are old and out-of-date, matching email server versions must be restored – adding expense to the total cost of discovery.

It is no easy task to prepare 100% for electronic discovery, but the fact is if you are not prepared, you will someday face the uncomfortable task of searching your organization's electronic records and it will be very costly. In part two of our series we will examine how to meet the challenges of managing email for electronic discovery using the leading enterprise messaging application, Microsoft Exchange Server.

Electronic Discovery on Microsoft Exchange Server

In this section, we will examine the challenges for managing the popular Microsoft Exchange Server for electronic discovery. Microsoft Exchange is the leading enterprise messaging application and presents some unique challenges for electronic discovery.

Microsoft® Exchange Server is a powerful messaging collaboration application that can support thousands of users simultaneously. To preserve Exchange email for compliance and legal discovery, Exchange Server uses a feature called “journaling”. Exchange journaling was introduced in Exchange Server v5.5 as a means to preserve Exchange email data. Journaling is enabled per Mailbox Store and it records all email sent and received for the Mailbox Store in a tamperproof mailbox. This journal mailbox is allocated by the Administrator and is not accessible by normal users. Third party legal discovery and email archiving applications access this journal mailbox and copy the data to a second host where it is indexed and searchable for discovery.

Email archive solutions benefit electronic discovery in two key ways. First, they create a central repository of email information that is indexed and easily accessible for search and discovery. The search tools that email archive solutions offer are superior to the native email server search tools and perform more efficiently with all the email centrally located and indexed. Second, email archive solutions preserve all information in an untamperable archive – no matter if email is deleted on the email server, the same email is preserved in the archive. This circumvents the major flaw of email servers which do not prevent individual users from deleting email. When properly installed and maintained, email archive solutions create an indexed archive of all mailbox information that is available at anytime for electronic discovery.

Journaling presents some major challenges in a production Exchange environment. The first is the performance impact on Exchange Server, which can be 15 to 35 percent performance degradation. The Microsoft TechNet article¹ describes the necessary steps for implementing journaling. The basic premise is that journaling effectively doubles the email traffic for the Mailbox Store. To keep Exchange overall performance equivalent to its performance before journaling is enabled; Exchange resources (e.g. memory, storage, and bandwidth) must be doubled.

Journaling presents some major challenges in a production Exchange environment.

¹ Journaling with Exchange Server 2003. Microsoft TechNet. 2005. Chapter 6.

Depending on the number of Mailbox Stores enabled, it is recommended that journaling be located on a dedicated Exchange Server. For many Exchange environments it is too disruptive and costly to add additional journaling servers and resources. In organizations that have deployed journaling, the implementation has been selective, deployed only for mailboxes that absolutely require it. For the financial services industry, it is the broker-dealers. In public corporations, adhering to the Sarbanes-Oxley Act, it is those who are responsible for financial results, financial auditors and executive officers.

A second major challenge of journaling is the mailbox information it does not record. An example is calendar items. Journaling does not capture when calendar items are created, modified or deleted. The well known case against Martha Stewart is an example where the data contained in a personal calendar appointment was crucial to the case. Another example is the history of a message item. Journaling does not capture when a message was created, when it was moved to a subfolder or when it was deleted. This data is crucial to understanding the intent of the user under investigation. When you consider that the user being investigated will try to cover his tracks by moving or deleting message data, it is critical to have access to the complete history of each message item.

Microsoft Exchange Server presents many challenges for legal discovery. The mailbox information that Exchange manages is highly diverse and is changing constantly. Exchange journaling is the current state-of-the-art for recording email records on Exchange Server. There is growing evidence from users and legal experts who are experienced with journaling that the mailbox information journaling does not capture like calendar items and folder information is very crucial for complete and accurate legal discovery. In our next and final segment, we will examine a new approach to managing email for electronic discovery on Microsoft Exchange that does not rely on journaling.

Email Discovery for Exchange without Journaling

In the second segment of our series, we examined some of the unique challenges that Microsoft Exchange journaling creates for email discovery. We learned that journaling impacts your existing Exchange server performance by as much as 35% and it is not a complete record of all historical mailbox information. In this third and final segment of our series, we will learn about a new method of managing email for electronic discovery that does not impede Exchange Server performance.

Mimosa Systems, Inc. recently launched a new email archive solution, Mimosa NearPoint™ for Microsoft Exchange Server that manages Exchange for email discovery and does not impact Exchange Server performance. NearPoint does not use Exchange journaling; rather it uses a new method that Mimosa calls One Pass Protection™. One Pass Protection is a new process that first copies all Exchange data using the standard Microsoft ESE Backup API to a secondary server (the NearPoint server). After the full copy completes, NearPoint parses all individual mailbox and message data; performs full-text indexing of message header, body and attachment; processes for global single-instance storage; and stores all message data in an archive managed by Microsoft SQL Server.

To meet compliance needs, One Pass Protection continuously reads Exchange log files and copies them to the NearPoint server. Exchange log files are small 5 MB files that contain 100% of Exchange transaction data. All incoming and outgoing messages are contained in the log files and hence captured by One Pass Protection. In fact, every change to Exchange data, no matter how small, is captured in the logs. For example, One Pass Protection captures full folder information and all messages types such as contacts and calendar items that are not captured by Journaling. As new log files are received on NearPoint, they are continuously processed and added to the archive. By reading Exchange log files continuously, NearPoint captures 100% of Exchange data meeting regulatory requirements for email archival and does so without effecting Exchange performance.

For email discovery on Exchange, Mimosa NearPoint has two major advantages over traditional email archiving solutions that rely on journaling. First of all, its unique One Pass Protection methods operate “off-host” and do not impact Exchange Server performance. By copying the Exchange transaction log files, it gains access to 100% new Exchange information without impeding Exchange performance. Secondly, NearPoint creates an indexed archive that contains a complete record of all mailbox information, including email, folders, calendars and contacts. Search and discovery of the NearPoint archive can be performed quickly and with high confidence because the results are very complete.

Mimosa NearPoint™ for Microsoft Exchange Server manages Exchange for email discovery and does not impact Exchange Server performance.

Conclusion

This paper has introduced the forces driving the need to manage email for electronic discovery. We discussed several unique challenges that Microsoft Exchange, the leading enterprise messaging application, presents to the user. And, in the final section introduced a unified email archiving solution from Mimoso Systems that performs email discovery on Exchange and avoids some of the common problems of traditional email archiving solutions that rely on journaling.

Find out More

For more information about Mimoso Systems and how NearPoint can help solve your archiving, eDiscovery, recovery and storage management issues contact a Mimoso Sales Representative at 408.970.9070 or visit our web site at www.MimosoSystems.com.