Compliance Readiness – Legal Service Providers

Important Considerations For Implementing An Email Archiving Solution

*The Editor interviews **Bill Tolson**, Director of Product Marketing, Mimosa Systems.*

Editor: Please tell our readers about Mimosa Systems and your background and professional experience.

Tolson: Mimosa Systems was founded in 2003 and currently offers software based solutions for archiving Microsoft Exchange data. We will also offer archiving of Microsoft Windows based file systems and Microsoft SharePoint applications. Our clientele includes a full range of customers. We have worked with small companies with 100 email boxes all the way up to *Fortune* 100 companies with diverse data centers around the world.

I came to Mimosa Systems after spending approximately 15 years in the mass storage industry with companies like Hewlett Packard, Iomega, StorageTech and Hitachi Data Systems. I also spent several years with a consulting company serving as a principal consultant helping *Fortune* 1000 companies analyze their needs for records retention policies and archiving solutions.

Editor: What factors should a company consider when developing an email archiving policy?

Tolson: When developing an email archiving policy, it is always a good idea to have the IT department and legal department sit down together to get an idea of which emails should be stored and the length of time they should be kept. As a consultant, I regularly recommended that companies create “high water marks” to make the retention process more expedient and to reduce costs. For example, it would be near impossible for an organization to try to automate email retention based on their current hardcopy retention schedule. Many hardcopy retention schedules have tens to hundreds of differing retention periods based on very specific document formats. Choosing one or two general retention policies for email makes more sense and is much easier to automate. The idea is to create an email retention policy that retains email for the necessary period of time.

Editor: Are there specific regulatory requirements that companies need to take into account during this process?

Tolson: Most regulatory requirements are government driven by industry. The biggest concern for companies is the Sarbanes-Oxley requirements which require companies to retain specific business documents including some emails. Any company that is publicly traded should have a record retention policy addressing Sarbanes-Oxley’s requirements.

If you are in the brokerage industry, SEC Rule 17 will drive your retention policy. In the Healthcare industry, it is HIPAA. Other industries which have records retention requirements include energy companies, drug and food companies, transportation and shipping companies. Many companies have employment records requirements. Also, any companies that work with the U.S. government have records retention requirements under the Federal Acquisition Regulations. Depending on the industry you are in, you probably have some type of government regulation that specifies what needs to be kept and the time period it must be stored.

MIMOSA SYSTEMS

Editor: What are the biggest mistakes you have seen companies make with email systems when faced with a potential discovery of their email system?

Tolson: There are two major mistakes I have encountered. First, companies do not have the proper procedures for ensuring that an effective litigation hold on data, including email, can be put in place quickly. Many companies rely on sending out a mass email message to all of their employees telling them not to delete any email messages until further notice. This practice does not guarantee all employees understood or even received the hold notice. To reduce risk of inadvertent destruction of email, they should have an automated email archiving solution that can apply a litigation hold centrally across the entire enterprise in an expedient manner so employees can’t delete their email until the litigation hold policy is released. There are many examples where companies have lost cases or been fined heavily for not stopping the deletion of email when they had notice of pending litigation.

Second, I have frequently encountered companies that have not taken into consideration the burdens and costs associated with searching through employee computers, handheld devices and removable media for employee personal email archives. This is both costly and very disruptive to the company. Companies need to set up detailed email use policies outlining whether employees can create personal archives, where the information should be stored and how long it should be kept. A centrally managed and stored email archive system that automatically indexes and stores messages will reduce those costs and provide the company with greater assurance that it will be able to quickly apply a litigation hold and centrally manage, search and retrieve the emails in the event of discovery.

Editor: How can the general counsel or CIO convince management of the need for an email archiving system?

Tolson: Not too long ago most CEOs viewed archived emails as potential “smoking guns.” The company management would adopt 30 to 90 day deletion policies with the intention of removing potentially bad emails from the system thereby reducing their risk. In reality there are many places where emails can be stored so it is impossible to ensure that all instances of a message have been deleted. To manage the risk, you have to assume that copies of potentially damaging email will float to the surface during a case. Another way to look at keeping emails for a longer period of time is having those emails archived and available because those emails could help your company’s case. There have been many cases where companies have lost lawsuits because they did not have the records that would have proven their case.

Editor: How does Mimosa’s NearPoint solution ensure that clients can implement their archiving policies in an effective manner?

Tolson: Many of our competitors have first generation systems that will capture and archive email from various systems including Microsoft Exchange, Notes, Domino or others. Mimosa’s NearPoint second generation solution goes further by capturing, archiving and protecting all data on the exchange server in near real time, including emails and attachments, contacts, task lists, calendar entries and time records associated with those files. This capability also allows companies to use NearPoint as a Exchange disaster recovery system. Email administrators love this capability because if they lose a mailbox or entire Exchange server, they can quickly restore it from our NearPoint archive system with a couple of mouse clicks.

Editor: Are there benefits to an in-house archiving solution when compared with a hosted solution?

Tolson: A hosted solution captures a company’s emails from its email systems and moves them to another facility for storage. These solutions are usually quick to install and run. The main problem with hosted email archiving systems is the fact that company sensitive emails are being held at another company’s facility. Many CEOs are not comfortable with this practice. Also, response times for litigation hold and eDiscovery may be slower than expected.

Mimosa’s NearPoint solution is an in-house solution. This means that a company will buy our NearPoint application, install it on its own servers and storage resources and manage it through their IT department. A major NearPoint differentiator is it does not require the installation of any agents on any of the exchange servers or client desktops. This allows the NearPoint solution to be up and running very quickly with no impact on the existing email system. This capability also means the end-user would potentially never know their email is being archived. Also, IT can decide if they want to allow employees to retrieve their own archived emails to save IT resources. Because we do not change the look and feel of the program used by the client, no extra training is required for the employees to use this system.

Editor: Does this raise privacy concerns that a company should consider before implementing an email archiving system?

Tolson: In the U.S. it does not. The accepted practice in U.S. business is that everything that happens in the company infrastructure belongs to the company. Therefore the employee should have no expectations of privacy.

Outside the U.S. that can be different depending on the country that you have employees and an email system in. For example, in Germany and the UK they have data protection acts which govern how customer and employee correspondence including email can be used and accessed by the company. For multinationals with email systems that span Europe, they should look at those country-specific data privacy acts to determine their limitations. It is important for the legal groups in these companies to understand and create a geography-specific email retention policy for their company.

Editor: Are users able to customize NearPoint to satisfy their regulatory requirements regardless of the location?

Tolson: Absolutely. The granularity of the Mimosa NearPoint system allows companies to set specific policies based on the email box, folder, department, storage server or server. Because of this policy granularity, a company can set different retention policies by country.

Editor: Should the archiving solution capture email metadata?

Tolson: The new Federal Rules of Civil Procedure touch on this point. Email metadata can be very important in court. It can tell the court when the email was created, by whom, on what servers, and the servers it passed through.

Editor: I have heard companies talk about the importance of journaling their email. Can you explain what this is and why it is important?

Tolson: Email archive journaling is a first generation technology that solution providers use to capture email messages as they pass through the server. In a Microsoft Exchange email system, a journal folder would capture every email that is sent or received on that specific server. The first problem with journaling is that it does not capture non-email data like calendar entries, task lists or contacts. The second problem is that it places anywhere from 15% to 30% additional performance load on the exchange server.

NearPoint offers journaling-like functionality in a more effective manner. NearPoint captures the server transactional logs as they are created and incorporates them into the archive server which creates an ongoing real time archive of the Exchange servers. NearPoint does not place any load on the archive server and because we are capturing logs, we are capturing all the data on the exchange server including calendar entries, task lists and contacts. This capability allows end-users to restore lost or deleted emails as well as having access to their entire email archive.

Editor: I have read that single instance storage is important when looking at an email archiving solution. Why?

Tolson: Single instance storage is a storage management function that saves storage space by limiting the duplicate copies of an email or its attachment in the system. For instance, an HR department sends out an email message with a 1MB jpeg map to all 1,000 employees at a company announcing a company picnic. Depending on the number of email servers in the email system, there could be several copies of that 1MB email message. Additionally, if all 1,000 employees created a PST and dragged those PSTs to their share drives on the network, that one message could take up one gigabyte of high-priced tier 1 network storage space. Single instant storage would save that 1GB of disk space by ensuring only one copy of that 1MB message is saved in the archive. Having an email archive also removes the need for employees to create personal archives so no PSTs need be created.

Mimosa System’s NearPoint Exchange system archiving solution offers users the unique ability to capture, store and archive data from their Exchange servers. In the event of a disaster, a company can easily access its archive and restore lost or corrupted data. Once installed, a company can manage its retention policy by setting parameters consistent with geographic and industry specific regulatory requirements. To learn more about NearPoint or to request a free trial version or schedule a live demo, visit www.mimosasystems.com.

Please email the interviewee at wtolson@mimosasystems.com with questions about this interview.