



The Disconnect Between Legal and IT Teams

Retention Policies

*Why lawyers agonize over Retention Policies
and worry about archiving emails.*

*Ideas and suggestions to resolve the issues
while mitigating risks and costs.*

#1 in a series of 4 whitepapers.

Circulate this document to IT, Legal, and company management.
It can be used to start a dialog, get consensus, and get action taken.

© 2009 Waterford Technologies, Inc. All Rights Reserved.

This whitepaper is published by Waterford Technologies, Inc., makers of the popular MailMeter archiving solution. For more information on MailMeter, email archiving, retention policies, ediscovery, FRCP, compliance, etc. go to www.MailMeter.com.



Background

If your organization has still not made a decision to archive emails for business and legal purposes (FRCP, SEC, FINRA, and other regulatory or compliance purposes) or you are frozen (or still debating) in the decision cycle (keep everything vs. don't keep anything), then this whitepaper is for you.

Our goal is to provide understanding of both the legal and IT issues and offer ideas and suggestions to resolve the differences while meeting your business goals and mitigating the risks.

The Disconnect

- Lawyers are worried about saving emails in an archive since they are discoverable records. Nearly every legal action includes an order to produce relevant emails.
 - When your organization is aware that “there is good potential for a legal action” (even before they have been served with a subpoena) you must take formal actions to preserve any records that may be called as evidence or asked for in discovery. This includes notifying people not to destroy email records and tracking responses to the notices (litigation hold).
 - The Federal Rules for Civil Procedure mandate that attorneys “Meet and Confer” to establish the “what do you have and where is it” for all electronic records expected to be searched.
- Your organization’s users believe they need to save every email they ever sent or received forever (just in case).
- The IT team has to maintain backups and is tasked with making most ediscovery searches – which is time consuming, potentially expensive, and has a large potential for errors.
 - Legal holds may require that copies of current mailboxes and messages on backups need to be recovered and placed in a separate, protected location.
 - While the policy debate goes on, the mass of messages in the email server continue to grow and cause long backup times, potential for longer recovery times, and reduce reliability.

The Lawyer's Concerns

At a recent LegalTech conference (a gathering of lawyers around technology issues) it was easy to understand the plight faced by an organization's legal team.

- **Judges are getting "tech savvy"**. There have been a number of legal cases that set precedence for producing ESI (electronically stored information) and decisions and recommendations by the Sedona Conference (really smart legal people giving analysis reports of important legal issues). They realize the pain and burden of producing the information and the high costs for both parties to review the documents, and the amount of court time taken to go through the evidence submitted. Remember, judges want justice – fair treatment under the law. Most judges would like parties to settle every case before it ever makes it to court.
- **Outside legal counsel is on the hook**, personally and professionally. They realize when they sign a pleading (legal document presenting responses and arguments to the court) that they can be fined, sanctioned if later the information about the ESI is found to be untrue. So now they are more concerned with the details of where the data is and who has control of it. Many cited examples of how internal counsel had not provided requested information because it was difficult to produce. They also were worried about producing "privileged documents" in the haste to deliver information to the opposing party. There has been a recent court case setting precedence that makes it easier to "claw back" inadvertently disclosed privileged data. The overall result is that outside counsel wants to spend more time (read money) reviewing the information before it is produced – first pass by a paralegal, next by an associate, then by the litigator.
- **Inside legal counsel is stuck** between a rock and a hard place. They are being mandated to cut legal costs however they can. So they strong arm negotiate with outside legal counsel for better rates (30-40% reduction is not unusual) and decide to do more work with in house staff. The highest expense in ediscovery is in the review of the information (how many eyes and at what costs for each email or document). With the potential for hundreds or thousands of emails needing review at an average cost of \$160 per hour you can see the obvious problem and the "disconnect" - if you have less information, then you lower legal costs.
 - Of course, lawyers realize that it may be unwise to not have email records for discovery – can't find the smoking gun, can't produce the contract change agreed to, can't argue that the contents of an email

produced by the opposing party is not the true version, and can't do an internal investigation to solve HR issues.

- Unfortunately, many lawyers' technical knowledge only extends to their use of Microsoft Outlook or Lotus Notes.
 - They do not realize that if an email is deleted from Outlook, that it still sits on the email server for a time period established by the IT staff (days to weeks).
- While the lawyers may think that IT policy deletes all emails older than 60 days, it is easy for any user to defeat that policy. They don't know that users can save messages to files on their desktop, forward them to outside email accounts, store them in a personal archive, copy them and take them home, or forward messages to themselves (resetting the clock on the age of email).
- Lawyers may not know that the backup files or tapes stored on site or off site may cover a much larger time period. IT people may not be aware of what they have or be unwilling to disclose its existence because of the amount of time they spent on gathering the data from a previous request.
- Many lawyers hold their breath while watching their IT staffs get grilled in depositions by opposing counsel asking detailed questions on security access, IT procedures, processes, and custodial operations. In spite of practice depositions, many lawyers are surprised by the information disclosed by IT under questioning.

The User and Business Concerns

Users are trained by the market place for personal email accounts (Hotmail, Yahoo, Gmail, etc.), that storage is nearly unlimited and free. So users truly believe that they have an inherent right to save every email forever (that's why users go through the gyrations of dragging messages into folders so they can keep track of their "stuff").

Users also use the organization email system as a transport for personal messages (baby and vacation pictures, jokes, YouTube videos, buying and selling on Ebay, news alerts on stocks and other interests, mail from family, etc.).

Over 80% of an organization's business intelligence is in email records.

Sales commitments, discounts, change orders, PO corrections, shipping changes, cost overruns, late deliveries, price changes, back orders, purchases, legal document changes, confidential information, etc. are transported through email.

How users defeat policies (legal) and mailbox quotas (IT).

1. I can forward email to my personal email account or save it to a file on my PC (or thumb drive) and then delete it. The organization no longer has the email – but I do. (Opposing counsel can ask if any of your users do this and then ask for their personal email records).
2. Archive or move mail to a personal archive (PST for Outlook – local archive for Notes) – out of my mailbox. I can make a copy of it and take it home or to my next job. Searching personal archives for legal actions is really expensive. A good policy is to not allow them in the first place.
3. If I know the policy is to delete emails older than x days, then I can grab old emails and forward them back to myself (now they are new messages) or to my outside email accounts. Many users even set up automatic rules to forward all emails to external accounts.
4. I can print any email and save it in a folder.
5. If I have done a bad thing (sent or received inappropriate or confidential material), I can double delete it right away (avoiding backup) making sure it is gone. You will never know I did it.

IT Manager and Technical Concerns

Most IT staff is concerned about resources and their personal time. They are short handed, stressed with problems, and pulled in many directions.

- The **email server storage is full**. Backups take too long. Recovery is impossible. There is no more disk space available. The answer is to set mailbox quotas (let users manage their own space). When the users complain again, let them have personal archives (which end up on their own PCs or on a network share and get backed up anyway).
- **Search for messages**. Users lose critical messages; IT has to go find them. Many disk based backup solutions make this easier. Going to offsite backups to recover messages needed in a legal action takes a long time (put up a new server, recover the email server data, look in mailboxes for the messages) and usually occurs under pressure or over a weekend (with no extra pay).
- **Copy mailboxes**. Legal teams ask for copies of mailboxes (let them do the searching). Usually pretty easy but some people have huge mailboxes.
- **Be deposed**. Yikes this is scary. Most IT staffs are technical people that have never been in a legal action before. Being asked questions (some good and some really dumb) about location of data, who has access, who could of and how could they delete messages (gives them a great way to show technical skills), is uncomfortable the first time but easier the next time since it forces IT to be prepared for depositions.
- **Policies don't match realities**. For example, if legal policy is to delete all email older than 6 months in the Inbox, 2 years if it is in a (save for 2 years) Folder and 4 years if it is in (keep for 4 years) Folder – why do most users (if they remember) drag everything into the 4 year folder? And why do you keep backup tapes for 1 year (means 6 months policy is moot).
- **Email archiving is easy**. It saves space, gives legal staff an easy search and export capabilities, users can search the archive for their own stuff, and the email server storage size can be shrunk by more than 50%. What are we waiting for?

Ideas and Suggestions

License an email archiving solution.

- Employees know that every email sent or received is kept as a company record for 7 years or longer. This insures that employees know not to waste resources on personal or frivolous.
- It prevents obvious use of the organization's email for non-business use since employees realize that every message is saved automatically.
- **Litigation hold is easy.** IT marks the archive. No notices to users are needed. No user can delete messages from the archive.
- When email is reviewed internally, it is marked or "tagged" as privileged, needs review, responsive, case #, etc. and it remains with the message so future legal discovery is less expensive since messages have already been reviewed.
- Any ediscovery action can now be satisfied with internal staff who do the searches requested, review and mark the messages (big cost reduction), and export only the relevant emails to PSTs to hand to outside counsel.
- **Outside counsel costs are lowered.** There are significantly less emails to review. The litigator is familiar with the archiving solution and knows the searches produce all relevant email messages (nothing can be deleted by users from the archive). The meet and confer sessions go smoothly.
- The need for business intelligence is satisfied – any user or manager can search the archive by date, keywords, customer, or person to find any critical email. The "needle in the haystack" can be found in seconds.
- IT is happy since email messages in the email server are removed after one year. **Backups are smaller and recovery is easier.** No more running out of disk space.
- IT is happier because they can disallow PSTs – minimizing backups and controlling retention.
- **Depositions will be easy.** A simple declaration of a description of the email archiving system and procedures usually suffices and can withstand any scrutiny.
- **Retention management is absolutely controlled.** Messages can be destroyed by department, age, subject, person, content, etc.

Message to legal

- Stop delaying a decision. It will only get worse in IT and create more legal problems (read the blogs on the Guidance Software case). Data is getting lost or destroyed and you haven't taken any actions to reduce your legal costs.
- Email archiving systems are not that expensive. In our experience the reduction in legal review costs on your first discovery action pays for the cost of the software.
- **Protect the business** – start collecting information now. You can always change your data destruction policies. Remember, you have anarchy now – people are making their own decisions. If you have a reduction in force, you may have lost years of good messages that can save you money in the future.

Message to Business People

- **Protect the business** – start collecting information now. You are losing valuable data because people are wasting time managing to mailbox quotas (what should I save?) or sending valuable data outside the company to personal email accounts (and you don't know it).
- You can also improve productivity by letting users know you will keep everything so they can find it if they need it. No more dragging and dropping messages into folders or wasting time housekeeping to meet mailbox quotas (that's why executives have bigger mailboxes).

Message to IT

- Lawyers are not bad people. They have a tough job. They look to you to provide the insight into how to meet obligations without huge expenses. They will probably want IT to make the investment in email archiving because they are struggling with more cases and less money.
- Do them a favor – have them sit in on a non-technical demo of an email discovery solution. It will help.