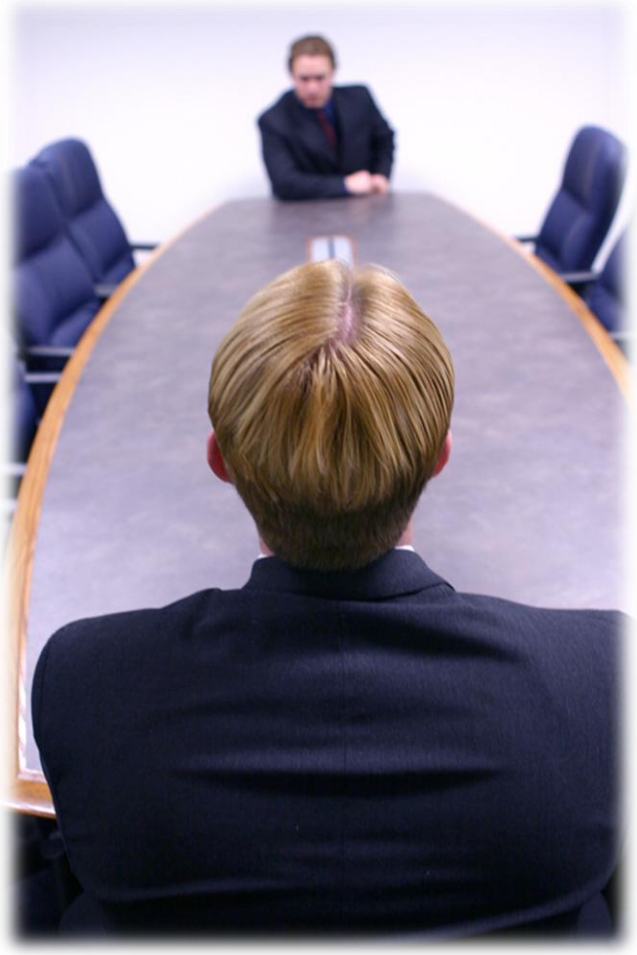


The Disconnect Between Legal and IT Teams

The Duty to Preserve

Why manual email archiving and user categorization doesn't cut it anymore

#4 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.

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.

MailMeter

WATERFORD TECHNOLOGIES

Background

If your organization is thinking about letting users decide on which messages to save, 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.

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.

Just being able to find a single email from a former employee or outside worker on a change order can save your business.

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. The cost of email production can be enormous.
- 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. IT is overwhelmed with storage costs, backups, and limited budgets.
- Legal holds may require that copies of current mailboxes and messages on backups need to be recovered and placed in a separate, protected location.

Lawyers and IT Don't See Eye to Eye

A knowledge gap exists between legal and IT staffs regarding email retention and e-discovery procedures and their respective departments basic needs and expectations. The miscommunication and varying priorities leads to an unknowing wasting of time, money, and security confidence.

Litigation Hold Directive

PRIVILEGED & CONFIDENTIAL
ATTORNEY-CLIENT PRIVILEGE
ATTORNEY WORK PRODUCT

TO:
FROM: Office of General Counsel
COPY: Outside Counsel
DATE:
SUBJECT: Notice of Litigation and Required Preservation of Electronic Data

The Lawyers Perspective

We want less: Many legal staffs want the least amount of electronic information. They may believe that end users can handle the custodial duty of "knowing" what important documents to save and discard. It certainly is cheaper to delete everything (how many users actually do this?) until notice of the need for a litigation hold and then retrieve and review information once an e-discovery request has commenced. Often users delete important messages before they are noticed of the legal hold. Ultimately, a judge will decide the time in history when litigation could have been projected and will expect critical electronic documents be protected and retrievable from that point.

Trigger point, the indication for Litigation: Lawyers know that you must begin keeping information when you have *first indication* of possible litigation, as FRCP regulation requires. In a perfect world, it would be easy to pinpoint a trigger point in which all proceeding information and electronic data could be classified, saved and documented for use in potential litigation. But, what one side may determine their trigger point is may be months or even years later than an opposing side. The judge will have the final say in measuring when a foreseeable issue could be determined, that could mean locating and retrieving documents from 9 years ago.

Request then Retrieve: Lawyers view of the retrieval process is simple as long as a legitimate policy and practice is in place and followed. *Why is it so hard to get all the emails when you have all the backup tapes?*

Immediate gratification: Once a request is given and a litigation hold in place, the search and discovery of necessary documents is placed upon IT. Unfortunately, "all emails" or "messages with these keywords" can be interpreted in many ways by IT personnel. *Lawyers usually believe they can bully IT to wave their magic wands and make data magically appear.*

Save Everything: Legal teams want to ensure that when a hold is activated, everything is saved. They would rather be prepared than caught off guard in court. Using the email server as a protected repository is not possible. It's too easy to delete or alter messages. *If you used the standard journaling of messages, you would be holding all the critical messages. No need to notice any employee.*

The IT Perspective:

Save Space: IT is most concerned with saving space. Not only is storage costly, but it can also tax normal functions and operations of email and storage servers. With requests and policy to save electronic information, IT normally endures the danger of running out of space. Typically the response for shrinking space is to impose mailbox quotas or use PSTs, which moves data from the main email server to another location to free up space. However, searching becomes more expensive.

Requests are Vague: An IT specialist is not trained as a lawyer. What a legal team reads and interprets can vary immensely from that of which an IT understands as being necessary or pertinent. Vague requests can elongate the search and retrieval process by creating an extended dialogue between IT and legal.

Cases vs. Departments: An IT specialist has organized the environment by departments and balancing workloads. Legal causes confusion because it visualizes the data by the strategy and concepts of the cases.

No Feedback: Requests, clarifications and edits can go back and forth multiple times before understanding or reaching a needed resolution. Often IT delivers results, hears nothing for six months, then has a fire drill to get new searches done overnight.

Pressured to Retrieve: When a lawyer requests e-discovery documents, the IT team is put under pressure to find and deliver the appropriate information with a hard deadline.

Where is it? The search for data usually spreads across email servers, backup tapes, personal files, etc. E-discovery requests are not an IT problem. Assigning search and retrieval duties to IT distracts them from everyday operations and responsibilities, assuming that the priority of the request trumps all other IT tasks and obligations.

Searching data in backup tapes **costs thousands of $ per backup tape**. Reloading data from backup tapes is costly and may not have the messages you need.

Why Manual Email Archiving Doesn't Cut It:

Many attorneys believe that they can let users make the decision on what messages to archive for records. Relying on end user preservation is not a safe bet and the practice of manual archiving is not accepted as a policy in court.

(see recent cases and discussions from the Sedona Conference)

1. **Empowerment to the end user has been criticized.** Having a "policy" delegating the responsibility to the end user to determine what to keep and discard can put a company at risk. Guidance is lacking for what constitutes "important email." Frequently users are unaware of classification means and to what extent metadata should be included in retention. A large majority often fail to comprehend policy expectations. Risks of exposure to company intelligence and integrity of sensitive issues is at stake.

2. **Manual archiving is not a policy, it's a practice!** A policy spells out a clear definition of what emails must be saved and needs to be in place before doing anything else. But there is a distinction between "policy" and "practice" in the courts which view the duty to preserve and the duty to retain separately. *The practice of manually archiving and filing email in personal folders is not a policy*. In the case of **Philips Adams vs. Dell**, the magistrate ruled that manual archiving *was only a practice, not a policy* and therefore **NOT AN ACCEPTABLE OR HONORED DEFENSE IN COURT**. It is not secure to rely on manual archiving as a "reasonable" practice for compliance with data retention.

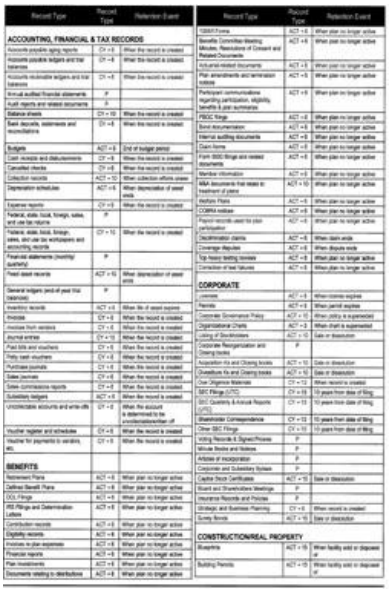
3. **You will be sanctioned.** It is your legal responsibility to ensure the appropriate and necessary documents are retrievable. When called to court, persons need to be fully prepared to articulate the company policy that was followed to defend the recovery and accessibility for finding applicable files and documents. Judges are no longer accepting the limitations of manual archiving and excuses for failing to retrieve documents and data. It is expected that companies and firms anticipate litigation and therefore preserve necessary data from the determined trigger point. The court in Phillip Adams vs. Dell ruled that ASUS should have foreseen the possibility of litigation in 1999 when business was initiated verses in 2005 when they activated a litigation hold from what they considered the point of conflict. Lesson learned – the judge has the final say. *The art of implementing litigation holds at a point deemed likely to expect litigation is a gamble and not worth the risk of attempting to defend in court.*

4. **Prove email wasn't deleted on purpose.** Notification is not enough to make sure emails don't get deleted. How do you go to court and prove emails weren't deleted on purpose (Intel vs. AMD)? You have a duty to preserve and protect all relevant evidence from the first indication of the potential for a legal action – not just when you get served a discovery notice.

5. **The burden of storing too much.** In addition to costs of extra tapes, disk space, management and supervision, excessive amounts of stored data in email servers, personal files, and backup tapes can create burdensome fees if there is a need to comb through data in response to an e-discovery request. Employees can also be creating separate disk drives, backups, forwarding to home emails, etc. that can violate and disrupt electronic management practices.

6. **Heavy reliance on IT.** Internal legal staff depends heavily on the trust and efficiency of IT to understand and secure e-discovery requests. Dependency and the inevitable time crunch can force IT into risky decisions in order to deliver requests that the end user was instructed to save. As indicated in AIIM reports, *email policy decisions are often made by IT with no input from Records Management or Legal in about 20% of organizations.*

7. **Categorization gone wild.** Many record managers think end users should be diligent and categorize all emails. Some examples we have seen run to over 300 different categories a user will choose from to mark an email. First, users won't do it – they are too busy. If pushed, most will mark all emails the same to take as little time as possible – or they will delete all emails.



8. **Training your end user.** If end users are responsible for determining that necessary information is saved or discarded, it is vital they are adequately trained to make correct decisions and save accordingly. This is VERY COSTLY! Activating proper control and monitoring to ensure that policy and protocol is being followed by end users is an additional financial burden.

9. **Issue of ex-employees.** Manual archiving assumes that the end user is still active in the company in relation to when the litigation period commences. Often, requests for documents can be for ex-employees. The tracking and recovery of documents expected to be saved by previous employees is a high cost for IT without ownership.

The reasonable way to deal with ESI and retention

1. **Anticipate Litigation**. As proved in the recent case, **Phillip M. Adams vs. Dell,** Inc., data is expected to be preserved is based upon "good faith in some possibility or notice of a credible threat of litigation." Companies are projected to initiate a litigation hold if there is any possibility of future litigation and most every company will be involved in litigation at some point. Don't get caught in trying to dance your way around your deemed "trigger point" in court. *If you abdicate responsibility, then be prepared when lawsuits appear.*

2. The **best precautionary response** for this expected reasonable retention practice and determination of a "trigger point" is dependency on an email archiving solution that stores a copy of every message and attachment regardless of attempts of deletion or altering. Archiving software eliminates placing the heavy responsibility on the end user to make potentially million dollar decisions. It will also catch any violation or mistake to policy that can essentially save your company and reputation. Archiving software removes the extra responsibility and possibility for human error from IT staff and end users.

3. Analyze your storage and make sure you are confident and prepared for scrutiny if and when an e-discovery request strikes. *Manual or custodial archiving is not a policy and will not serve as a viable defense when prompted by e-discovery.*

4. Have a **POLICY**, not just a practice. An archiving solution can manage your retention policy while ensuring data is saved and is searchable.

5. Handle it, claim custody and prove security. To ensure security and proper defense, abdicate responsibility.

How to Reduce Your Legal Costs

An email archiving solution brings value for legal, IT, and the business.

- Employees know that every email sent or received is kept as a company record for the period of time in the policy. This insures that employees know not to waste resources on personal or frivolous mail.
- 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**. You can mark the message in the archive. No notices to users are needed. No user can delete messages in 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 e-discovery 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.
- Their 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.
- **Depositions are easy**. A simple declaration of a description of the system and procedures usually suffices.
- **Retention management is absolutely controlled**. Messages can be destroyed by department, age, subject, person, content, etc.

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

Message to legal

- Stop delaying a decision. It will only get worse in IT and create more legal problems. 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.
> Be pro-active.
> Head off litigation.

- **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.
- **Be proactive** – head off litigation. With an eDiscovery tool you can do early case assessment in minutes, and can quickly decide if a case has merit.

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 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).
- Audit or sample emails – watch for the word "discount", "guarantee", etc. with an automated process to identify potential risk areas.
- Analyze email activity by department, domain, to give managers insight into their team's activities and help them manage better.

Message to IT

- Do your legal team a favor – have them sit in on a non-technical demo of an email discovery solution. It will help.