The IT Manager’s Indispensible Guide to E-Discovery

October 2010
# Table of Contents

- Introduction .................................................................................................................. 3
- The Legal Discovery Process ......................................................................................... 3
- The Role of IT in Legal Discovery Requests ................................................................. 4
- The Vicious Email Management Circle ....................................................................... 5
- The EDRM Framework .................................................................................................. 6
- Litigation Readiness ....................................................................................................... 7
- E-Discovery: The Old Way ............................................................................................ 9
- E-Discovery: The New Way .......................................................................................... 10
- Five-Step Discovery Workflow ...................................................................................... 11
- Types of Legal Holds ..................................................................................................... 14
- Audit Trails ....................................................................................................................... 19
- Beyond E-Discovery: How Archiving Saves IT Time and Money .................................. 19
- Conclusion ....................................................................................................................... 19
- About LiveOffice ............................................................................................................. 19
- Appendix A: How LiveOffice Discovery Archive Helps Address the EDRM Framework ................................................................................................................................. 20
Many organizations are reporting that the volume of litigation and regulatory requests that they face are continuing to go up. E-Discovery must be regarded like any other business process, so standardizing it and automating the parts that can be automated will yield cost benefits.

– Michael Osterman, Osterman Research, Inc.

Electronic discovery, also known as e-discovery, refers to any process in which electronic data is sought, located, secured and searched with the intent of using it as evidence in a civil or criminal legal case. More often than not, companies are simply not prepared to find electronically stored information (ESI), especially email and the associated attachments, in the face of pending litigation. Plus, tight timelines imposed by the Federal Rules of Civil Procedure (FRCP) have made the process of discovering and collecting relevant information in a fast, defensible and transparent manner critical to legal professionals.

FRCP guidelines stipulate that any company with the potential for litigation within the U.S. federal court system must preserve email and produce relevant emails and other ESI when requested for legal discovery purposes. Companies that fail to produce emails and other electronic content in a timely or appropriate manner face the risk of paying millions of dollars in sanctions and fines, not to mention a tarnished reputation and lost revenue.

This whitepaper discusses a variety of areas related to the discovery process, including the following topics.

- The legal discovery process
- The role of IT in the legal discovery process
- Email management
- The Electronic Discovery Reference Model (EDRM) and each phase of it
- The role that LiveOffice Discovery Archive plays in the discovery process
- Five-step discovery workflow and use case
- Legal holds and case management
- How cloud-based email archiving helps alleviate the e-discovery burden
- Addressing the EDRM framework

The Legal Discovery Process

Legal discovery consists of many stages. It may require several technologies, including content repositories like archives, discovery tools, and specialized legal review software and services. Many departments within organizations play a role in e-discovery, including IT, legal counsel, line-of-business leaders and individual employees. Initial rounds of discovery include identifying people who have a role in the litigation (known as custodians) and compiling all ESI that is relevant to the matter. IT’s primary role in the process is searching repositories and gathering large volumes of ESI.

As the process continues, new custodians may be identified and more documentation (e.g., email, IMs, files) is gathered. Then the data is processed and analyzed to weed out irrelevant content. IT is often involved in narrowing down the initial dataset.

Once a narrower dataset emerges, legal counsel reviews the information and shapes its response to the lawsuit. Opposing parties also exchange relevant ESI, as required by federal rules. If the matter goes to trial, information is produced in a final form for presentation in court. IT leaders may also be called to testify about the organization’s information management policies and processes.
Consider These Statistics:

- Discovery costs represent between 35% and 50% of the cost of litigation.
- Roughly three out of four discovery orders today require email to be produced as part of the discovery process. With billable rates for junior associates at many law firms now starting at $200 per hour, the cost to review just one gigabyte of data can easily exceed $30,000.

The Role of IT in Legal Discovery Requests

More than two-thirds of organizations recently surveyed by analyst firm ESG said that IT was the primary group responsible for collecting emails and attachments pertaining to a legal discovery request. Given the increased popularity of email as a primary source of evidence, “it is readily apparent that more and more IT departments will pick up yet another responsibility when it comes to managing this vital communication application,” according to Brian Babineau, ESG senior analyst.

Figure 1: Groups that Manage the Information Collection Process when Email Messages are Requested

In your organization, who manages the information collection process when email messages are requested for business, legal, and/or regulatory purposes? Which group would you consider to be primarily responsible? (Percent of respondents, N=282)

![Bar chart showing the distribution of responsibilities for information collection.]

<table>
<thead>
<tr>
<th>Group</th>
<th>Percentage of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT organization</td>
<td>85%</td>
</tr>
<tr>
<td>Compliance group</td>
<td>30%</td>
</tr>
<tr>
<td>In-house legal counsel</td>
<td>9%</td>
</tr>
<tr>
<td>Records management group</td>
<td>23%</td>
</tr>
<tr>
<td>External legal counsel</td>
<td>4%</td>
</tr>
<tr>
<td>Specialized forensic consulting services</td>
<td>1%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
</tr>
</tbody>
</table>

IT departments are often asked to support their legal teams in the event of litigation and legal discovery. Whether they realize it or not, this makes IT a vital part of the e-discovery process. However, since they are not always aware of their role in the process, IT does not necessarily evaluate any type of email management solution to solve an e-discovery problem.

1 Source: Pillsbury Winthrop Shaw Pittman LLP
The Vicious Email Management Circle

Dealing with e-discovery-related tasks may be the worst administrative duty for IT because:

- **Unpredictability of Requests.** It is very hard to know when a regulator or litigant is going to request emails as part of the discovery process. There is no telling what parameters guide a specific request. Some discovery notices call out specific people (custodians), date ranges, keywords or a combination of factors. More often than not, in-house attorneys want the collections completed as soon as possible, so they can start reviewing the information.

- **Beyond Searching.** IT has to worry about “chain of custody,” which means collection processes must be documented to prove that information has not been tampered with in any way. There is also a possibility that an IT manager or someone supervising the collection process may have to testify in a deposition or in court as to how they actually executed the data collection.

- **Email is Widespread.** There are several different locations from which relevant messages must be collected (see Figure 2), and the data may be in different formats. Searches for messages are likely going to need to be conducted several times, in multiple locations. No data source can be excluded (unless agreed upon by both parties’ attorneys or dictated by the court). Otherwise, it might look like the organization involved in the litigation is trying to hide something.

**Figure 2: Sources for Email Messages Requested for Business, Legal and/or Regulatory Purposes**

From which of the following sources does your organization currently search for, access and retrieve email message(s) that are requested for business, legal and/or regulatory purposes? (Percent of respondents, N=282)

<table>
<thead>
<tr>
<th>Source</th>
<th>Percent of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary email application and associated storage system(s)</td>
<td>58%</td>
</tr>
<tr>
<td>Individual PCs (i.e. PST files)</td>
<td>57%</td>
</tr>
<tr>
<td>File servers</td>
<td>53%</td>
</tr>
<tr>
<td>Backup tapes</td>
<td>46%</td>
</tr>
<tr>
<td>Other</td>
<td>31%</td>
</tr>
</tbody>
</table>

IT often implements email quotas (storage thresholds based on the size of a mailbox) to control email-related storage costs, improve email server performance and make backups faster and easier. Unfortunately, while email quotas reduce some administrative headaches, they actually make the e-discovery processes more difficult, since employees often start setting up personal archives (.PST or .NSF files) locally, moving old messages out of their inboxes to avoid hitting the quotas. These personal archives are stored on PCs and file shares, and are frequently backed up—even if an employee deletes a personal archive folder, it is likely on a backup system somewhere. Nearly half of the organizations surveyed by ESG stored more than two terabytes of personal archive message data. The personal archives could be anywhere inside or outside the organization, which means when a discovery request arrives, IT has to search for messages in several repositories.
The EDRM Framework

The Electronic Discovery Reference Model (EDRM) provides a common, flexible and extensible framework for the development, selection, evaluation and use of electronic discovery products and services. It guides organizations through all the stages required to meet federal rules that govern the use of ESI in litigation. The model helps companies effectively respond to discovery requests from initial information management to the presentation stage (when the ESI is actually presented to jury, judge or client).

Since it was created in 2005 by consultants George Socha and Tom Gelbmann, the EDRM has been widely adopted by the vendor community. In the case of content repositories, such as email archives, vendors use the model to describe where their products fit in the discovery process. The EDRM is also useful to show what email archives can contribute to an e-discovery undertaking and where other tools are required.

Rational Discovery

The Electronic Discovery Reference Model guides enterprises through the steps they should follow to meet legal discovery requirements.

As the diagram illustrates, there are nine major steps in the discovery process. While presented in a fairly linear fashion, some of the steps, such as Identification, Collection and Processing, are repeated several times throughout a discovery effort. The IT group is often involved in the steps on the left-hand side of the model, while legal counsel is typically more instrumental in the phases on the right-hand side of the model.

There is often a handoff somewhere in the middle of the process, when IT provides relevant (or responsive) ESI based on the initial search criteria established by internal/external counsel. It is vital to preserve the chain of custody during the handoff. This ensures that organizations can quickly demonstrate that the history of any email has not been tampered with and prove its authenticity. For legal discovery, email archiving solutions like LiveOffice Discovery Archive lower overall risk of spoliation and greatly speed up the discovery process because of its message indexing, audit capabilities, deduplication and protection of all email messages stored in the archive.

It is also important for IT to help cull large datasets prior to the handoff, which can save organizations considerable legal expenses down the road (i.e., the less email expensive legal counsel has to review, the better). Another cost-effective option is equipping lawyers with simple tools that enable them to effectively and iteratively search the data in question as much as necessary to help build a case or stage a defense.

Information Management. This is more of a goal than a step. As organizations mature, they are putting structured content management and archiving systems in place. This allows them to enforce company-wide retention policies and more easily respond to discovery requests for a minimum cost and with little or no disruption to the business.

Identification. Once a discovery request is initiated (e.g., because of a lawsuit, a compliance matter or an internal investigation), the organization has to determine what data is required, where it’s stored and who the custodians are, i.e., the individuals who have relevant information under their control. Pertinent data may reside in a variety of locations, including personal computers, file servers and storage systems.
Note: Search and index technologies are required for identification, so a good email archive indexes the metadata and content of email, including attachments. The index makes discovery searches more efficient by returning a high percentage of relevant information.

Preservation. Once reviewers identify the information they want, IT has to preserve the data and ensure it is not altered or deleted. Simply opening a document can change critical metadata, such as the access date, which can then affect the validity of the document. In addition, if the organization has a retention and disposal policy, potentially relevant data must be placed under legal hold, which suspends deletion. Organizations often rely on technology, rather than end-user behavior, to enforce legal holds and document the actions.

At some point during the Identification and Preservation phases, the parties involved in the lawsuit convene for a “meet and confer” session. This gathering, which is mandated by the FRCP, lets both sides agree on guidelines for the scope of the discovery, and how to preserve and produce ESI. The intent of the meet and confer is to reduce the potential cost, for both parties, of overly broad e-discovery requests.

Collection. In the Collection phase, information is compiled in one place for processing. The Collection process should preserve the original metadata associated with the content. The opposing party may request the information gathered during discovery in its native format. IT can save headaches later in the process by collecting information in its native format from the outset, which helps demonstrate its authenticity.

Processing, Review and Analysis. During these phases of the litigation cycle, the Matter is much more dynamic, with formal review and analysis phases that are generally conducted by lawyers. The Processing phase, also referred to as the Culling stage, aims to reduce the initial size of the dataset. A first-round search is likely to produce reams of irrelevant email, documents and files, including duplicates and content unrelated to the legal discovery request. In the Review phase, legal counsel examines the material that remains after iterative culling to ensure that the resulting dataset is relevant to the dispute at hand. They also determine if the material contains privileged information that needs to be withheld from the opposing party and may begin to formulate a strategy based on the data under review. The main goal of the Review stage is to extract relevant messages from archives and export them into a legal review tool. Finally, in the Analysis phase, counsel further hones its legal strategy (or decides to settle).

Production and Presentation. These final phases are typically managed by outside counsel when preparing for trial with the opposing party. Although few Matters end up here, since most parties are often encouraged (and financially motivated) to settle during the previous phases. The Production phase includes exporting relevant material to opposing parties in TIF or PDF files, or native electronic format, while the Presentation phase helps determine how the ESI is used in court.

See Appendix A for details on how LiveOffice Discovery Archive helps address the EDRM framework.

How LiveOffice Discovery Archive Can Accelerate Litigation Readiness

“For some, costs have skyrocketed; one company reported processing and hosting expenditures leaping from under $100,000 three years ago to over $10 million last year.”

— George Socha & Tom Gelbmann, Law Technology News (August 2009)

Discovery Archive provides organizations with a proactive e-discovery solution that offers cost savings, information management, collection and preservation. While other solutions offer simple systems to assist with information management and preservation, they do little to lessen the burden and costs associated with the later phases—especially with culling, which can get expensive very quickly. The more data that is produced, the more a company pays their legal counsel and other associated service providers. This may include a large volume of content that is unrelated to the legal Matter, such as newsletters, spam and notifications. Discovery Archive equips IT and legal teams with the tools they need to further refine and cull the data.
Using Discovery Archive to perform e-discovery in the cloud offers a number of key advantages.

- **Cost.** Reduce the high costs associated with processing and reviewing by first culling large volumes of email data down to only the most relevant content.

- **No maintenance.** Since Discovery Archive is a complete cloud-based solution, there is no hardware or software to manage. Maintenance and deployment are handled by the experts at LiveOffice—so IT staff can focus on using the tool instead of maintaining it.

- **Speed.** When it comes to litigation, time literally is money. The quicker legal counsel can access relevant ESI, the quicker an organization can determine whether it has a defensible case or needs to settle.

- **Streamlined workflow.** Discovery Archive simplifies the process of collecting all email (sent and received), searching across custodians, culling search results and applying legal holds to help ensure organizations are well equipped to address any litigation needs.

Taking an agile and defensible approach can help organizations cut e-discovery costs and risks. It can provide the flexibility that allows legal and compliance teams to act quickly. Moreover, it can deliver the control organizations need to help avoid sanctions, fines and damage to reputations.
E-Discovery: The Old Way

The chart below depicts a normal discovery response workflow from an IT and legal perspective. The boxes have been color-coded to correspond with the EDRM stages. The realm of IT is concentrated in the Collection and Processing (data culling) phases of e-discovery, which can be both expensive and time consuming—especially when an outside service provider is used for culling. With this approach (i.e., the old way), IT is often put in the position of coordinating with the service provider and serving as the intermediary between legal and the service provider.
E-Discovery: The New Way

Discovery Archive helps eliminate several of the steps that can completely consume an IT department in the event of litigation. Plus, it equips legal teams (whether they are on staff or at an outside agency) with the tools they need to perform and iterate their own searches to cull and refine the data. LiveOffice has developed a straightforward five-step workflow that streamlines the process, puts legal in the driver’s seat and helps lessen organizations’ legal exposure.
Discovery Archive’s Five-Step Discovery Workflow

Organizations need to have defined and streamlined processes for quickly culling through large amounts of electronic communications to respond to e-discovery requests or HR investigations. They also need to have a process for creating and communicating legal holds (i.e., preserving specific email communications) to the custodians involved in cases.

LiveOffice has developed a simple, five-step process to help organizations quickly respond in these instances, apply ongoing legal holds, cull relevant messages and export the relevant files to a case management solution for further review and analysis.

Step 1: Delegate Access

IT plays a critical role in data management, collection (archiving email) and preservation, and is directly responsible for all of the data that feeds e-discovery and compliance processes. However, they often wish to be taken out of the discovery process. Discovery Archive lets organizations offload more of the downstream stages to other in-house teams, such as legal, HR or compliance. This process starts with delegating access to approved Reviewers.

Administrators have the ability to delegate Reviewers, who can search across specific groups of custodians’ mailboxes. If an organization wants a Reviewer to review the email of a particular user group, they need to assign the role to a specific user(s). Administrators can delegate access to some or all of the archives with a Role Management feature. They can provision each Reviewer with distinct permissions that determine which mailboxes they can search, review and retrieve emails. This level of security and role-based permissions are vital in the Identification phase of the EDRM.
Step 2: Create Matter

Generally, Matter Management refers to the Information Management and workflow practices that are tailored to meet legal departments’ (or outside counsel’s) specific needs and requirements for pending litigation. Matters can also refer to internal HR investigations (e.g., potential sexual harassment suits) that may never go to court. Creating the Matter in Discovery Archive starts the Identification process for EDRM.

Discovery Archive makes it easy to manage Matters and allow designated reviewers to select custodians. To create a Matter, reviewers just add a new Matter in the Matter Management section, give it a unique name (i.e., related to the material) and select the custodians or user accounts they want to associate with the Matter from the drop-down menu. The Matter Management section also allows reviewers to create groups of custodians for a Matter and facilitate active legal hold for custodians in a litigation event.

Step 3: Apply Legal Hold

Per the FRCP, once litigation is a possibility, organizations are bound to preserve potential evidence by implementing a legal hold and notifying custodians of their role(s) in the matter. Failing to apply legal holds to preserve information in a timely manner and ensure custodians’ compliance with them can put companies at risk.

What is a Legal Hold? A legal hold is a process organizations use to protect all forms of relevant information from being lost, tampered with or deleted when litigation is reasonably anticipated. Discovery Archive allows reviewers and administrators to override an end user’s archive retention settings, ensuring that any emails tagged for legal hold cannot be deleted or expired from an archive. Legal holds applied at the Matter level flag not only all current messages from all users specified in the Matter, but all future emails received in the archive for the duration of the legal hold. Note: Legal holds can only be removed by administrators or reviewers by selecting the Matter in Discovery Archive and ending the hold.
Recent court decisions illustrate the impact of poor legal hold management, including undue leverage for the opposition, costly sanctions and losing cases outright. Applying legal holds is essential in the Preservation phase (EDRM). Managed repositories, such as email archives, are a smart tool to use for legal holds, since they take the onus off the end user and IT, and ensure that every email sent and received is automatically preserved in the archive.

With Discovery Archive, applying legal holds is simple and straightforward. Designated reviewers can place legal holds on specific communications (based on search criteria) to safeguard against an organization’s staff or automated deletion policies from inadvertently deleting case-relevant emails. Administrators and reviewers can also use simple tags to flag attorney-client privileged communications, which are excluded from e-discovery requests.

![Add Tag](image)
Types of Legal Holds

With Discovery Archive, reviewers can initiate a variety of legal holds, depending on the unique circumstances of the Matter, and meet the stringent requirement of Preservation as outlined in the EDRM.

**Static, Search-Based Holds:** In the most basic use case, reviewers and administrators can select specific messages for legal hold by either browsing the archive or conducting a search to find specific messages. Once the desired messages are found, reviewers can tag them and specify legal hold status.

**Static, Custodian-Based Holds:** Authorized reviewers use this type of hold to apply a legal hold to a specified set of custodians. Because it’s “static,” only existing messages in the archive are flagged for legal hold. **Note:** With this approach, any new messages meeting the initial criteria for the legal hold are not automatically captured and tagged. In order to do this, reviewers need to use the Saved Search functionality in Discovery Archive. Reviewers can browse across existing Matters under the Archive tab and then apply a unique Tag Name to reference all emails from this Matter. The system suggests a Tag Name based on the Matter name, but reviewers can specify an alternative name or append the Tag Name with additional information.

**Dynamic, Search-Based Holds:** The limitation of static legal holds is that they only apply to existing email that meets a defined set of search criteria (either based on a list of custodians or a specific keyword-based search). However, they do not capture new messages that may meet the same criteria. Discovery Archive allows authorized reviewers to apply ongoing or dynamic legal holds, using the Saved Search functionality.

Saving a search actually saves the search scope and criteria, not the email results at the time a reviewer executes the search. Reviewers should tag individual items when they want to identify a particular issue or action. Remember that email is continuously archived for active accounts, so the search results are dynamic.

Once reviewers determine relevant keywords that pertain to their organization’s business policies and/or response (i.e., relevance) to a Matter, the next step is to conduct and save searches, using those criteria. It is important to remember that unless the selected accounts contain only historic email or use specified dates as criteria, saved searches may find new results when they are run again.

After a search is saved, reviewers can setup policy alerts based on those searches to help streamline and expedite the review process. They can also decide whether or not to specify the saved search as ongoing for legal hold purposes.
Discovery Archive distinguishes the saved searches that are actively tagging emails with legal hold (ongoing) versus those that are not (standard).

**Dynamic, Custodian-Based Holds:** To apply a legal hold to a specific Matter and set of custodians, reviewers can use the saved search functionality. They simply browse to the selected Matter and apply a unique Tag Name to distinguish all emails related to this Matter. The system suggests a Tag Name based on the Matter name, but reviewers can specify an alternative name or append the Tag Name with additional information.

After a Matter is created, a Matter Search helps find a specific user (Account or Reviewer level) when there are a large number of users setup in Discovery Archive. Authorized reviewers can search against these users’ archives by selecting New Search under the saved searches menu of the Matter.

**Point-and-Click Hold:** With this type of legal hold, reviewers simply select individual emails from search query results or choose a specific custodian to place on hold. This type of hold allows reviewers to get very granular with their holds, which is required in some cases to ensure that a wide and complete dataset is captured.

**Ongoing Legal Hold: Proactive Alerts**

When reviewers setup an ongoing legal hold, they are automatically alerted whenever an email that meets the criteria specified in the hold is sent or received.

Reviewers can also leverage the Discovery Archive alerting functionality to proactively protect their organizations from liability and common lawsuits, such as discrimination, sexual harassment or wrongful termination. This helps prevent problems before they happen by ensuring that critical emails get the appropriate approval from managers or senior executives. For example, reviewers can flag any emails that contain profanity within the subject line, message body or attachment. To setup an alert, reviewers simply create a policy name, select a saved search from the drop down menu and enter their email address in the Alert Email(s) field.
Step 4: Cull the Data

It’s not about reviewing faster; it’s about reviewing what’s relevant to any given Matter. Many organizations process all collected data and apply simple culling techniques (e.g., by date range, keywords and/or named custodians) for lack of a better option. However, the culling step is critical in the Processing, Review and Analysis stages of EDRM. Too broad of an approach during Processing and Review can result in very high costs (an average of $1800 per gigabyte).

With Discovery Archive, reviewers can quickly narrow their search results by metadata fields, keywords, data ranges and/or specific groups of user mailboxes. They can also perform iterative searches and search within a search (see below) to help further cull the data and increase the number of highly responsive emails, rather than relying solely on custodian-based searches. Best practices outlined at the The Sedona Conference recommend that customers iterate their keywords and culling strategies to hone them appropriately.

Discovery Archive’s Web 2.0 technology-based browsers allow authorized IT and legal staff to easily search, cull, hold and analyze case-relevant email data. Plus, they can also grant outside counsel access to the archive without poking holes in the firewall or setting up new, non-employee mailboxes within Exchange’s Active Directory. As a result, reviewers and legal counsel can quickly gain access and early insight into case-related content and formulate e-discovery plans during meet and confer – before entering the high-cost Review phase.

Lightning-Fast Search
Discovery Archive’s lightning-fast search functionality allows reviewers to quickly search the entire contents of archived emails and attachments, using a variety of search criteria, including to, from, date, subject, message body, message attachments and other message properties. They can then efficiently navigate through search results, identify highlighted search terms and tag potentially harmful emails, so the content in question is easily retrievable for further review.

Quick Search: The quick search field allows users to quickly and easily search for emails containing specific keywords or phrases. Discovery Archive fully supports Boolean search conditions (using AND, OR, NOT), and the queries are executed against an entire email message, including the text of attachments.
**Advanced Search:** An advanced search allows users to construct more sophisticated search criteria. Reviewers can use all of the features in a quick search, in addition to specifying email addresses, dates and other parameters.

**Iterative Search/Search within a Search:** In addition to quick and advanced searches, reviewers can conduct iterative searches and fine-tune the results, effectively searching within a search. This functionality offers significant time savings when building a complex query involving varied criteria, since the reviewer can apply and remove search filters and change the Boolean logic without having to rebuild the search criteria from scratch.

**Responsive vs. Non-Responsive Emails:** In order to significantly reduce expensive review costs, organizations should explore ways to perform early stage culling and filtering to simplify e-discovery, reduce data volumes and drive down the total cost of review. An effective early case assessment capability relies on two things. First, companies need to make sure they have enough “responsive” ESI (i.e., data that meets specific criteria relating to the case at hand) to truly see where they stand. (“Non-responsive” ESI is any data resulting from a search that does not specifically apply to the case.) Second, organizations must have the ability to analyze the ESI in a way that gives them the best possible picture of the circumstances. This helps them determine the best legal strategy to pursue. Creating a legal strategy based on incomplete data raises a company’s risk of spending large sums of money and time to defend a case that may be unwinnable.

Discovery Archive lets designated reviewers (attorneys or less expensive paralegals) perform an unlimited number of iterative searches to tag responsive and non-responsive emails, so attorneys can start analyzing and filtering their data immediately upon initial data collection. Throughout the life of a Matter, reviewers can always return to the original dataset to identify emails they want to include in the review.

**Step 5: Export Results for Early Case Assessment**

Rule 26(f) of the FRCP, often referred to as the Meet and Confer rule, requires the parties in a litigation matter to meet at an early stage to discuss the information they have and what they will share. The purpose of Rule 26(f) is to “direct the parties to discuss discovery of electronically stored information during their discovery-planning conference.” This “early case assessment” rule directs the parties to meet as soon as practicable (but no later than 21 days before a scheduling conference) to develop a plan that addresses any and all foreseeable discovery issues.
This does not leave a lot of time for culling and analysis. Consequently, organizations need to move quickly from Collection to Culling to Analysis to determine whether they have a defensible case or need to work on other options (i.e., settling out of court). This is often addressed in the Processing and Review stages of EDRM and generally leverages third-party software that is specifically designed to process a wide range of ESI to narrow the result set to the most relevant and responsive content. Organizations can save significant time and money if the initial dataset has already been culled (through iterative searches) before being processed by these solutions.

Organizations can leverage Discovery Archive to not only cull a responsive dataset, but also to quickly export it to third-party case management solutions for additional analysis and processing. Once reviewers have tagged all emails related to a specific case or Matter, they can use Discovery Archive’s intelligent export feature to load the files into a case management solution or other application for further review and analysis.

Discovery Archive lets reviewers easily export emails resulting from a search in PST files (MSG format), ZIP (EML format) and NSF file formats. In addition, LiveOffice now supports the Extensible Markup Language (XML) standard developed by EDRM. Socha and Gelbmann are also overseeing the creation of an EDRM XML schema to facilitate data transfers from one discovery product to another.

To export a set of responsive messages, preauthorized reviewers conduct a quick or advanced search (or when they are browsing through emails), select the Export button in the toolbar, determine whether they want to “Export current page” or “Export selected emails” and select the preferred file type.

Reviewers are then prompted to save a file to the desktop, which can be burned onto a DVD or saved on a removable drive for transport. Note: Emails are automatically zipped and saved in EML format. Discovery Archive automatically breaks up large exports. However, customers are encouraged to contact LiveOffice Client Services for very large exports (more than 10 GB).
Audit Trails

Discovery Archive provides a complete audit trail, which can be exported and used in court to increase the defensibility of email evidence. These auditing capabilities provide a defensible and trackable process that ensures no spoliation of evidence by preserving the metadata (which meets the Preservation requirements of EDRM). Discovery Archive audits and reports on the entire e-discovery process to ensure that user behavior is accurately tracked and accounted for in a complete chain-of-custody approach.

Key Advantages of Discovery Archive

- Protect email data in a highly scalable, enterprise-level email archive
- Leverage built-in tools to rapidly assess, cull and hold ESI
- Provide lawyer-friendly tools for rapid search and early case assessment
- Enable a speedier handoff for attorney review and production
- Implement proactive processes for information retention and e-discovery to maintain consistency

Beyond E-Discovery: How Archiving Saves IT Time and Money

According to ESG, 40 percent of organizations using a dedicated archiving solution cited “fewer IT staff hours required for email administration” as a key metric to justify their investment. Most IT departments include fewer help desk calls related to email performance, streamlined backup operations and minimal storage management operations as part of this calculation. ESG believes that the 40 percent figure would likely increase if IT actually thought about how much simpler e-discovery tasks are when there are fewer places to search for emails.

Conclusion

Can your organization quickly and easily respond to a legal discovery request and produce specific email communications, potentially a year or more old, within 21 days? For most companies, the answer is an emphatic “no.”

To avoid heavy fines, severe legal sanctions and lost reputation, companies need an easy way to search for relevant messages to quickly meet legal discovery requests (or simply respond to internal HR investigations). Leveraging the EDRM framework to proactively take control over your ESI increases your company’s e-discovery readiness and agility in responding to case preparation.

Discovery Archive can help affordably mitigate these legal risks with minimal IT involvement—saving you time and money when it really counts.

About LiveOffice

We’re all about software-as-a-service—and have been since our inception in 1998. No matter what your organization’s industry or size, we are ready to serve you. Nothing speaks louder for us than our 12-year track record of processing and protecting millions of messages a day and 97% client-retention rate. Our extensive archiving experience has earned us a premier client roster, ranging from established Fortune 100 companies to fledgling organizations that are just opening their doors.
Appendix A: How LiveOffice Discovery Archive Helps Address the EDRM Framework

**Information Management.** Discovery Archive captures all messages and attachments in a hosted archive and does not require additional hardware, software or resources to manage it. All emails, IMs and attachments are stored and indexed in a centralized, online repository. As email comes into the system, it is time stamped, serialized and given a unique signature to ensure its authenticity in court. Organizations can quickly and easily query Discovery Archive to find email that may be relevant to a particular case or Matter (instead of finding and restoring email data from tape backups, assuming the tapes have not been overwritten or corrupted).

**Identification.** Discovery Archive makes it easy to manage Matters and allow designated reviewers to select custodians. Reviewers can create a new Matter and determine who to delegate access to for searching (which can include designated IT staff and/or internal/external legal counsel). Powerful and granular search tools enable IT to quickly search the entire contents of archived emails and attachments, using a variety of search criteria, including to, from, date, subject, message body, message attachments and other message properties.

**Preservation.** Discovery Archive allows reviewers and administrators to override an end user’s archive retention settings (i.e., their messages are preserved and not destroyed according to an organization’s regular disposition policy). Any emails tagged for legal hold cannot be deleted or expired from an archive. With Discovery Archive, organizations can initiate a variety of different legal holds depending on the unique circumstances of the Matter while meeting the stringent requirement of Preservation as outlined in the EDRM.

**Collection.** Discovery Archive prevents spoliation (the alteration or destruction of a document to make it invalid or unusable as evidence) by disallowing users and administrators from deleting any emails in the archive. Plus, search results can easily be exported in a variety of formats to streamline the handoff to opposing counsel.

**Processing, Review and Analysis.** Discovery Archive helps IT and/or legal counsel further cull the dataset, saving organizations considerable costs associated with the previous EDRM phases. Not only is the email data automatically stored in a single instance (i.e., identical and duplicate copies of messages and files are removed from the dataset), but simple searches can help locate relevant material. IT can use various search criteria, including custodians, date ranges and keywords or phrases, and easily discard any extraneous data. **Note:** While these phases are often conducted by outside counsel, using third-party case management tools, Discovery Archive can help with the preliminary culling and exporting (via EDRM XML) while preserving the chain of custody.

**Production and Presentation.** Discovery Archive can assist in these phases by allowing IT to export relevant data (emails and attachments) via EDRM XML (Extensible Markup Language) to third-party case management solutions. This reduces the time and risk involved with the data exchange by providing a robust, flexible, transparent and well-documented schema. The uniform format can be leveraged by third-party solution providers (that analyze a variety of ESI types) and preserves the underlying information about the content and metadata being transferred (e.g., the source of the underlying ESI, processing of the ESI and production of the ESI).