

The Growing Importance of E-Discovery on Your Business

An Osterman Research White Paper

Published June 2008

SPONSORED BY



Why You Should Read This White Paper

Discovery is the process of identifying, preserving, collecting, reviewing, analyzing and producing information during civil legal actions. The goal of discovery is to obtain information that will be useful in developing relevant information for pre-trial motions and for the trial itself. Information sought during discovery can include documents, testimony and other information deemed necessary by a court.

E-discovery is simply the extension of the discovery process to information that is stored electronically and includes email, instant messages, word processing files, spreadsheets and other electronic content that may be stored on desktops, laptops, file servers, mainframes, smartphones, employees' home computers or on a variety of other platforms.

E-discovery is becoming much more important in the context of civil litigation – for example, roughly three out of four discovery orders today require email to be produced as part of the discovery process. E-discovery today represents 35% of the total cost of litigation¹, and companies that fail to produce emails in a timely or appropriate manner face the risk of paying millions of dollars in sanctions and fines, not to mention loss of corporate reputation, lost revenue and embarrassment.

Implementing an appropriate e-discovery capability is critical to the long-term viability of any organization, particularly larger ones that face a greater chance of being involved in civil litigation. E-discovery best practices include several key elements, starting with management recognition for the need to be ready for e-discovery to developing a set of corporate policies to implementing the right technologies that will manage corporate data properly.

The goal of this white paper is to focus on the key issues involved in developing an e-discovery capability and to help organizations plan to become better prepared for the rigors of the e-discovery process. However, the goal of this document is not to offer legal advice or legal opinions on specific legal issues related to e-discovery, and it should not be used in this context.

This document was sponsored by eight vendors of archiving, email management, e-discovery and related technologies, including Barracuda Networks, C2C, CommVault, Global Relay, Google, GWAVA, Recommind and Trend Micro. Information on each of these vendors is provided at the end of this document.

Source: Pillsbury Winthrop Shaw Pittman LLP

Why is E-Discovery So Important?

DISCOVERY DEFINED

Wikipedia defines *discovery* as “the pre-trial phase in a lawsuit in which each party through the law of civil procedure can request documents and other evidence from other parties or can compel the production of evidence by using a subpoena or through other discovery devices, such as requests for production and depositions.”

E-discovery is simply the extension of this well-established process to the electronic content that an organization might possess, including email messages, instant messages, word processing files, spreadsheets, presentations, purchase orders, contracts, wiki and blog postings, files stored in collaboration systems, and all other electronic content to which an organization might have access. Further, e-discovery extends to all of the venues in which this data might be stored, including desktop machines, laptops, smartphones, servers of all types and even employees’ home computers.

THE GROWING QUANTITY OF ELECTRONIC CONTENT

Businesses receive, generate and store large and growing amounts of information. According to an analysis conducted by the University of California at Berkeley, 93% of all information today is created in an electronic format; the American Records Management Association (ARMA) has estimated that more than 90% of records created today are electronic. Further, more than 70% of electronic information is never printed. Unified communications and unified messaging systems will make this problem significantly worse as it adds additional data to the already crowded mix of data types that organizations must retain and manage.

ORGANIZATIONS MUST INCREASINGLY FOCUS ON E-DISCOVERY

In 2005, 16.7 million total civil cases were filed in state courts in the United States²; in 2006, 244,343 civil cases were commenced in US District courts³. This means that roughly 17 million civil cases are filed annually in the United States alone, or 56 civil cases for every 1,000 people.

As a result of the changes to the Federal Rules of Civil Procedure (FRCP) discussed later in this report, the discovery of information that is stored electronically is now a mandatory point of discussion in every civil case that is filed in the federal courts. Because a growing number of states are passing their own requirements for discovery of electronic information, e-discovery is increasingly becoming a point of discussion in state civil cases, as well.

What this means for organizations of all sizes and in all industries is that:

- The Electronically Stored Information (ESI) to which an organization has access will play an increasingly important role in its future litigation.

² Source: Court Statistics Project, *State Court Caseload Statistics, 2006* (National Center for State Courts 2007)

³ Source: Administrative Office of the U.S. Courts, *Statistical Tables for the Federal Judiciary*, annual

- The timeliness and breadth of the response required to discovery requests under the revised FRCP will make e-discovery a more important part of litigation-related decisions.
- Organizations must preserve all relevant electronic data that might reasonably be considered relevant for e-discovery using management systems that can preserve this data and its metadata.

Key Drivers for E-Discovery

FEDERAL RULES OF CIVIL PROCEDURE

The FRCP are a set of rules focused on governing court procedures for managing civil suits in the United States district courts. While the United States Supreme Court is responsible for creating and managing the FRCP, the United States Congress must approve these rules and any changes made to them.

One of the most important drivers for e-discovery has been the new set of amendments to the FRCP that went into effect on December 1, 2006. These changes represented several years of debate at various levels and will have a significant impact on electronic discovery and the management of electronic data within organizations that do business in the United States. The changes to the FRCP require organizations to manage their data in such a way that this data can be produced in a timely and complete manner when necessary, such as during legal discovery proceedings.

The amendments to Rules 16, 26, 33, 34, 37, 45 and revisions to Form 35 are aimed at electronically stored information (ESI). The amendments attempt to deal with the important issues presented by ESI:

- ESI is normally stored in much greater volume than are hard copy documents.
- ESI is dynamic, in many cases modified simply by turning a computer on and off.
- ESI can be incomprehensible when separated from the systems that created it.
- ESI contains non-apparent information, or metadata, that describes the context of the information and provides other useful and important information.

The changes reflect the reality that discovery of email and other ESI is now a routine, yet critical, aspect of every litigated case. First, the amendments treat ESI differently. Second, they require early discussion of and attention to electronic discovery. Third, they address inadvertent production of privileged or protected materials. Fourth, they encourage a two-tiered approach to discovery – deal with reasonably accessible information and then later with inaccessible data. Finally, they provide a safe harbor from sanctions by imposing a good faith requirement.

Unlike many information retention requirements in specific industries, such as those imposed upon broker-dealers, hedge fund managers and investment advisors by the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), the FRCP apply to virtually all organizations in all industries, including private, public and non-profit organizations. In short, if an organization can have a civil lawsuit filed against it, then the FRCP should figure prominently in that organization's data management strategy.

For more information on the FRCP, please see *The Impact of the New FRCP Amendments on Your Business*, available at www.ostermanresearch.com.

FEDERAL RULES OF EVIDENCE AND AUTHENTICATION

The Federal Rules of Evidence (FRE), formally enacted in 1975, are a set of rules that determine how evidence is presented during trial in the US federal courts. These rules are focused primarily on the initial presentation of evidence during trials. Individual states may use these rules as the basis for their own rules of evidence, or they may adopt a different set of rules for presenting evidence at trial. For purposes of presenting evidence, a printed or otherwise human-readable version of electronic evidence is considered to be an original and can be presented at trial according to FRE Rule 1001(3).

Authentication is a very important part of the e-discovery process because its goal is to prove that a document is what its presenter claims it to be – a true and verifiable representation of an electronic document. Authentication for electronic content is even more critical than for paper-based documents, since electronic documents are more easily altered. Therefore, in order to prove the authenticity of a particular electronic document, such as an email, those submitting this evidence must provide affidavits or otherwise demonstrate that an original document was not modified after the fact.

Despite the admissibility of electronic evidence in court proceedings, the authenticity of electronic records is a major issue that many organizations have not considered adequately. A classic case in point is *Vinhnee vs. American Express Travel Related Services Company, Inc.* In this case, American Express sought payment for more than \$40,000 in charges on two credit cards from a California resident who had filed for bankruptcy protection. However, because American Express could not prove the authenticity of the electronic statements it presented during trial, it lost the case even without the plaintiff being present.

An important case that deals with the authenticity of ESI is *Lorraine v. Markel American Insurance Co.* [2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007)]. This case involved a dispute between the owner of a ship that had been struck by lightning and the insurer of the ship. Although the insurance company paid for the damages, the ship's owner subsequently found additional damage and made a second claim, which the insurance company disputed. During arbitration, the damages awarded to the plaintiff were reduced by \$22,000. While both parties presented email evidence during arbitration, Chief Magistrate Judge Paul W. Grimm who presided over the case found that the email evidence presented could not be authenticated. In his ruling, the judge wrote:

“...there are five distinct but interrelated evidentiary issues that govern whether electronic evidence will be admitted into evidence at trial or accepted as an exhibit in summary judgment practice. Although each of these rules may not apply to every exhibit offered...each still must be considered in evaluating how to secure the admissibility of electronic evidence to support claims and defenses. Because it can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, counsel should know how to get it right on the first try.”

“computerized data ... raise unique issues concerning accuracy and authenticity ... The integrity of data may be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling.”

In short, Judge Grimm ruled that for ESI to be approved for use as evidence, a variety of FRE rules must be taken into consideration, including Rules 104, 401, 403, 801, 901, 902 and 1001-1008.

RELEVANT COURT RULINGS

There are a large and growing number of cases and decisions that are relevant to consider in the context of e-discovery, including the following:

- ***Qualcomm, Inc. v. Broadcom Corporation***
No. 05-CV-1958-B(BLM), 2007 WL 2296441 (S.D. Cal. August 6, 2007)
Although Qualcomm initially prevailed in this case, it was discovered after the ruling that thousands of emails were withheld during the case; the Court awarded \$8.5 million in attorney's fees and costs against Qualcomm.
- ***Disability Rights Council of Greater Washington v. Washington Metropolitan Area Transit Authority***
2007 U.S. Dist. LEXIS 39605
Production of email from backup tapes was ordered by the Court at the expense of the producing party. The Court also noted that the Safe Harbor provisions of Rule 37(e) do not apply if data destruction is not suspended after a litigation hold.
- ***Ryan v. Gifford***
Civ. No. 2213-CC, 2007 WL 4259557 (Del. Ch., Nov. 30, 2007)
The Court ordered “the production of documents identified in plaintiffs’ ...motion to compel in a format that will permit review of metadata, as plaintiffs have clearly shown a particularized need for the native format of electronic documents with original metadata.”
- ***Orrell v. Motorcarparts of America, Inc.***
2007 WL 4287750 (W.D.N.C. Dec. 5, 2007)
The court ordered the production of a plaintiff's home computer for forensic examination.

- ***Auto Club Family Insurance Co. v. Ahner***
2007 WL 2480322 (E.D. La. August 29, 2007)
“Like other courts that have addressed this issue, this court will not automatically assume that an undue burden or expense may arise simply because electronic evidence is involved.” FRCP Rules 34 and 45 “were amended...to provide for routine discovery of electronically stored information from parties and non-parties. In fact, whether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format (a distinction that corresponds closely to the expense of production). But **in the world of electronic data, thanks to search engines, any data that is retained in a machine readable format is typically accessible.**” [Emphasis added]

Although there are hundreds of cases that can be cited in the context of e-discovery, Osterman Research believes that these cases focus on five relevant e-discovery lessons that organizations of all sizes should heed:

- A failure to diligently search for and assess relevant content during the e-discovery phase of a legal action can have serious consequences.
- Legal protections, such as the Safe Harbor provisions of the FRCP, are not necessarily afforded to parties that do not adequately protect data to which a legal hold has been applied.
- Metadata, as discussed later in this white paper, is an important component of the data that must be evaluated and presented during e-discovery.
- Data sources that must be searched during e-discovery can be far-reaching, including employees’ home computers.
- The difficulty of accessing ESI will not necessarily shield parties from their obligation to produce this data.

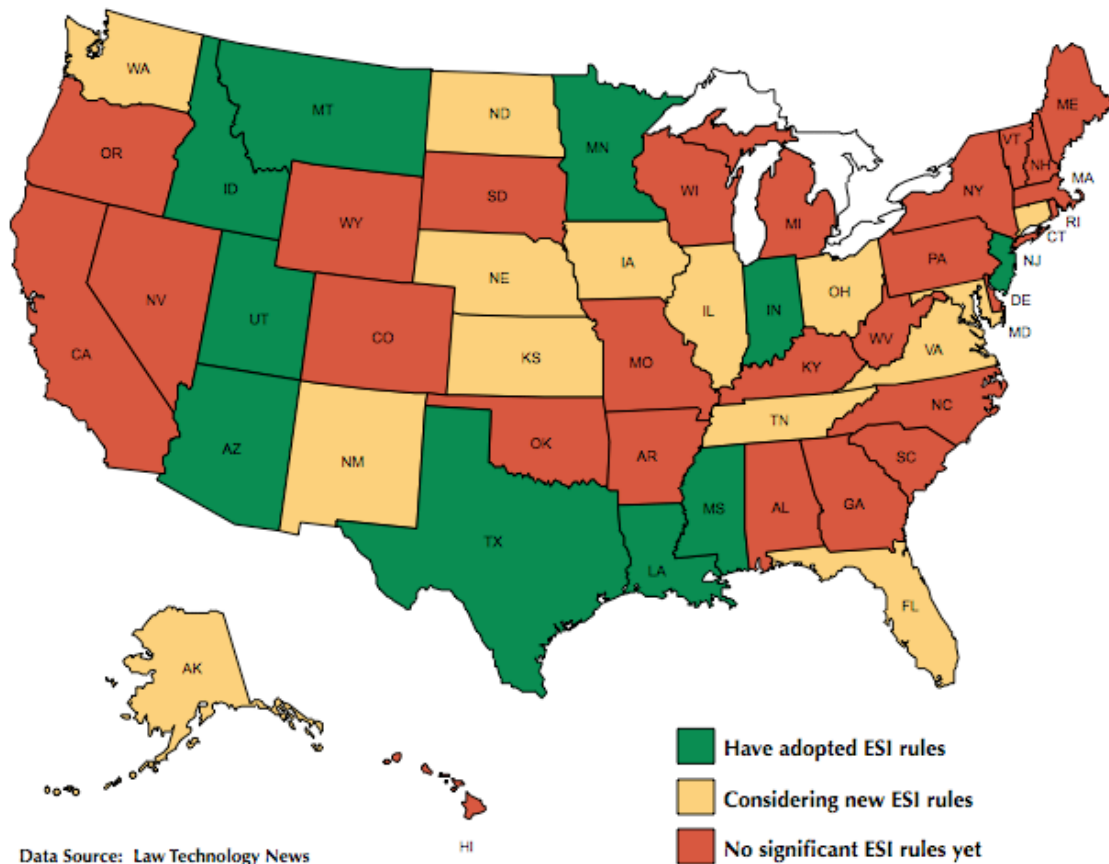
STATE LAWS

The FRCP represents just the tip of the iceberg: many US states have already passed, or will soon pass, their own version of the FRCP for civil litigation that takes place within their respective state court systems. For example:

- Minnesota modified its Rules of Civil Procedure, effective July 1, 2007, establishing procedures for the discovery of ESI.
- New Jersey adopted the new FRCP e-discovery rules effective September 1, 2006.
- Texas adopted Rule of Civil Procedure 196.4 in 1999, which states, in part, “to obtain discovery of data or information that exists in electronic or magnetic form, the requesting party must specifically request [it] and specify the form in which the requesting party wants it produced.”

- Through early 2008, other states that have integrated the new FRCP amendments into their respective statutes include Utah, Louisiana, Arizona, Montana and Indiana.
- A number of other states are also considering enhancements to their civil procedure laws that will focus more on ESI. Among these states are Washington, Alaska, Florida, Illinois, Kansas, Connecticut, Ohio and Virginia.
- As of mid-2008, roughly one-half of US states have not taken steps to amend their civil procedure rules to include a specific emphasis on ESI, as shown in the following figure.

Status of ESI Adoption in the United States



LAWS OUTSIDE OF THE UNITED STATES

While e-discovery in North American legal proceedings is difficult enough, laws in other parts of the world can significantly complicate e-discovery (often referred to as “e-disclosure” outside of the United States). For example:

- The European Commission Directive 95/46/EC, adopted in October 1995, was designed to standardize the protections for data privacy among all of the member states of the European Union and to protect individuals’ right to privacy. The Directive focuses on the processing of individual’s data within the EU, but also applies to any

entity outside of the EU to whom this data might be provided, such as during an e-discovery exercise. The Directive does not permit data to be provided to anyone whose national laws do not adequately safeguard privacy rights.

- France imposes even more stringent requirements than Directive 95/46. French Penal Code, Law No 80 – 538 imposes fines and/or jail time for those who seek, request or disclose information intended to develop evidence for foreign legal proceedings.
- Blocking statutes, such as the French law noted above, have been in place for many years in various countries and were enacted specifically to block discovery proceedings. For example, blocking statutes exist in Ontario, Canada (Business Records Protection Act), the United Kingdom (The Shipping and Commercial Documents Act) and the Netherlands (Economic Competition Act).
- Australia's Supreme Court of Victoria, in its Practice Note No. 1 of 2007⁴ (February 2007), strongly suggested that parties to a legal action should consider using technology to improve the efficiency of legal proceedings, including e-discovery. The Federal Court of Australia has gone further and developed e-discovery rules similar to those contained in the new amendments to the FRCP.
- India's Technology Act of 2000 modified the country's rules of evidence, effectively expanding the scope of electronic data in e-discovery efforts and widening parties' obligations for producing electronic data.

THE SEDONA CONFERENCE

The Sedona Conference is a non-profit [501(c)(3)]institute focused on the study of law and policy. It provides important input to the discussion of e-discovery issues in North American and internationally, and is an important resource for those who must go through the e-discovery process and for vendors alike. The mission of The Sedona Conference⁵ is:

The Sedona Conference exists to allow leading jurists, lawyers, experts, academics and others, at the cutting edge of issues in the area of antitrust law, complex litigation, and intellectual property rights, to come together - in conferences and mini-think tanks (Working Groups) - and engage in true dialogue, not debate, all in an effort to move the law forward in a reasoned and just way.

Our hallmark is our unique use of the dialogue process to reach levels of understanding and insight not otherwise achievable. Our Working Group Series is designed to focus the dialogue on forward-looking principles, best practices and guidelines in specific areas of the law that may have a dearth of guidance or are otherwise at a "tipping point." The goal is that our Working Groups, the open Working Group Membership Program, and our peer review process, will produce output that is balanced, authoritative, and of immediate benefit to the Bench, Bar and general public.

⁴ http://www.supremecourt.vic.gov.au/wps/wcm/connect/Supreme+Court/resources/file/eb913b0785d01df/PracticeNote-No1-2007_GuidelinesForUseTechnology.pdf
⁵ http://www.thesedonaconference.org/content/tsc_mission/show_page_html

The goal of The Sedona Conference is to create a think tank-like atmosphere where leading attorneys, jurists and others can discuss key issues focused on intellectual property rights, anti-trust law and complex litigation in a non-adversarial setting. Each year, the Conference hosts a series of events focused on these three areas that are each limited to 60 participants, one-quarter of whom comprise a panel of “faculty” members. A particular meeting may result in the creation of a working group whose goal is to develop guidelines or industry best practices that will spur the advancement of the legal system in regard to the focus areas of the Conference.

Among The Sedona Conference working groups that are most relevant to e-discovery are WG1 (Electronic Document Retention and Production) and WG6 (International Electronic Information Management, Discovery and Disclosure). A key source of input to WG1 is the RFP+ Group that focuses on technology for e-discovery and the management of electronic information. This group consists of a vendor panel and a user group.

THE ELECTRONIC DISCOVERY REFERENCE MODEL (EDRM)

The Electronic Discovery Reference Model (EDRM) Project was a response to the relatively few standards and lack of generally accepted guidelines for the process of e-discovery that existed prior to its development. The team that developed the EDRM was facilitated by George Socha (Socha Consulting LLC) and Tom Gelbmann (Gelbmann & Associates), and included 62 organizations, among whom were software developers, law firms, consulting firms, professional organizations and large corporations.

Begun in May 2005, the EDRM Project had as its goal the creation of a framework for the “development, selection, evaluation and use of electronic discovery products and services”⁶. The EDRM, which was placed into the public domain in May 2006, is designed to help organizations manage the process of e-discovery from the initial stages of managing electronic information through to its presentation.

The development of the EDRM was important because it represented a major step forward in the standardization of the e-discovery process. Standardization will become increasingly important for e-discovery for several reasons, most notably because of the growth in quantity and diversity of ESI and the large number of entities that will need to process this data (internal and external legal counsel, senior managers, archiving vendors, outside forensics firms and others).

Following development of the EDRM was the EDRM XML project in the 2006-2007 timeframe. The goal of this project was to “provide a standard, generally accepted XML schema to facilitate the movement of electronically stored information (ESI) from one step of the electronic discovery process to the next, from one software program to the next, and from one organization to the next.”⁷ The EDRM XML 2 project (2007-2008 timeframe) is continuing the development of the EDRM XML schema for metadata, developing protocols for the number of electronic files that are preserved in their native format, and developing a compliance validation tool, among other projects.

⁶ <http://www.edrm.net>

⁷ http://www.edrm.net/xml_2006_2007.php

EDRM SECTIONS

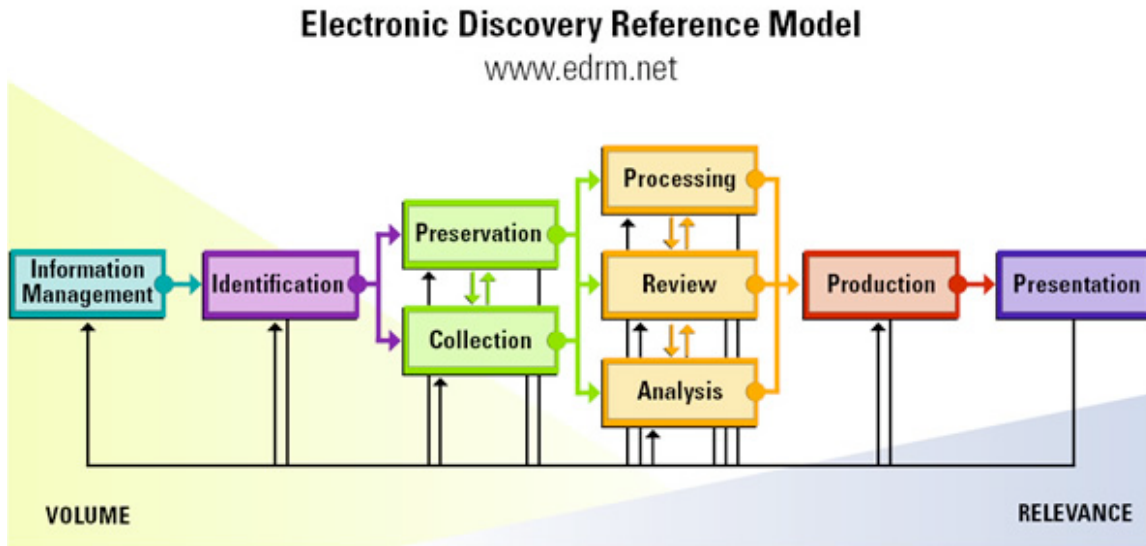
The EDRM is divided into eight sections that focus on the process of managing an e-discovery effort:

- **Identification**
Understand the “inventory” of ESI that might be relevant in a particular legal action and that might have to be presented during discovery. At this point in the process, discovery demands, disclosure obligations and other pertinent claims and demands are reviewed and considered. The goal at this stage of the process is to understand the universe of information that might be required in order to respond to appropriate e-discovery requests and then determine the subset of information that will be relevant for further processing.
- **Preservation**
This is a critical step that ensures that ESI is protected from spoliation and modification, such as through the imposition and enforcement of a legal hold on all relevant ESI. If spoliation does occur, the consequences can be expensive. For example, in the case of *Leon vs. IDX Systems Corporation*, the plaintiff deleted 2,200 files from the laptop computer his employer had issued to him. The court dismissed the case and awarded the defendant \$65,000 for the spoliation.
- **Collection**
During this phase, all relevant ESI is collected from the various sources that contain it, including messaging archives, backup tapes, file servers, desktops, laptops, employees’ home computers, smartphones and other sources.
- **Processing**
At this point, collected data should be de-duplicated in order to reduce the amount of data that must be processed during subsequent phases of the discovery process. Collected data should also be prioritized into a) that content that will likely be relevant later in the process and b) content that will likely not be relevant. At this point, decision makers may want to convert ESI into a form that will permit the most efficient and thorough review of its contents.
- **Review**
The review phase includes redacting ESI as appropriate, evaluating the content for its relevance, determining if specific items are subject to attorney-client privilege, etc.
- **Analysis**
This phase involves a variety of activities, including determining exactly what the ESI means in the context of the legal action at hand, developing summaries of relevant information, determining the key issues on which to focus, etc.
- **Production**
The production of data involves delivering the relevant ESI to any parties or systems that will need it. It also includes the activities focused on delivering ESI in the appropriate form(s), including DVDs, CD-ROMs, paper, etc.

- **Presentation**

The presentation of ESI is a key consideration at various points of the e-discovery process – as information is reviewed, analyzed, produced, etc. The specific forms of presentation for ESI will vary widely depending on the content; how, where and by whom the content will be presented; and other factors.

The EDMR is summarized in the following figure.



Recommendations

This section focuses on general recommendations for any organization, whether public or private, for-profit or non-profit, large or small. It is not intended to be an exhaustive set of recommendations for protecting an organization during legal proceedings, but rather as a starting point for developing a set of best practices focused on e-discovery.

UNDERSTAND YOUR OBLIGATIONS

First and foremost, it is critical for any organization to understand the obligations that it faces with regard to the retention and disposition of electronic data. These obligations include:

- Local, state, provincial, federal and international obligations to retain certain types of data.
- Legal obligations and legal precedent to retain certain types of data and to establish retention periods that are appropriate for certain data types.
- Industry-specific obligations and/or best practices for the retention and disposition of certain types of records. For example, the Truss Plate Institute has established that “an

in-plant quality control manual shall be maintained for each truss manufacturing facility”, and that a document retention policy must be established⁸.

Cohasset Associates has published the results of a survey⁹ that provides some interesting findings on records management and organizations’ development of data retention policies:

- Only 60% of the respondents’ organizations had comprehensive records retention schedules in 2007 that include electronic records, up from 51% in 1999. Only 49% of organizations have a formal email policy focused on retention practices for email, up from 45% in 1999.
- Only 55% of organizations have records retention schedules for email, instant messages, blogs, collaboration tools and other types of communication; and only 43% have such schedules for electronic documents.
- Only 14% of organizations *always* follow their retention schedules, while another 50% generally do so.
- Only 16% of organizations has a formal policy focused only retention of voicemail, 15% have such a policy for instant messages and only 7% have a retention policy for blog content.
- Only 56% of organizations have a formal plan that will allow them to respond to discovery requests for their records.

What this survey points out, among other things, is that organizations simply are not retaining as much data as they need to retain, nor are they implementing policies and procedures to protect themselves from the consequences. Plus, there does not seem to be significant progress over time in this regard on the part of many decision makers, despite the fact that the new amendments to the Federal Rules of Civil Procedure, recent court decisions and the growing quantity of electronic content that most organizations possess mean that there really should be more progress than has been the case.

BEING PROACTIVE IS CRITICAL

While some believe that e-discovery can be accomplished adequately and less expensively in a reactive mode once a legal action has started, Osterman Research believes that it makes more sense to be proactive about e-discovery. Taking a proactive approach to e-discovery, instead of a purely reactive one, is ultimately less costly, it reduces the risk of spoliation, improves the chance of winning legal actions and is less disruptive to IT, legal and other staff members.

The following points represent a few key guidelines to consider in developing an e-discovery strategy:

· TPI Alternative Method for Quality Criteria in Metal Plate Connected Wood Trusses, AM-3.2.1
· *The 2007 Electronic Records Management Survey* (<http://www.cohasset.com>)

- **Leverage technology to help classify data as it is produced**
Human review of data generated during an e-discovery exercise, as well as intervention by humans in the data classification process on an ongoing basis, will continue to be a requirement for at least the next several years until automated classification technologies are sufficiently robust. However, there are technologies available today that can classify, process and review email and other electronic documents quite well and can significantly speed classification and e-discovery processes. These technologies should be employed, where appropriate.
- **Establish sound data retention and deletion schedules**
All organizations, regardless of their size or industry, should establish sound data retention policies for all of the different data types that they manage or will have occasion to manage over the next several years. Different types of business records will be subject to different data retention schedules, and so retention schedules should be sufficiently granular as to accommodate all of these requirements.

While establishing data retention schedules is critically important, an often-overlooked – but no less important – consideration is the deletion of data after it no longer needs to be retained. Retaining unnecessary data can result in a variety of problems, including higher e-discovery costs because of the volume of data that must be reviewed, increased liabilities associated with ‘smoking guns’ that might reside in old data stores, and higher storage costs. Some data should probably be deleted after 30 or 60 days.

- **Understand the evolving requirements for data retention**
As a corollary to the point above, organizations must continually remain aware of the changing nature of data retention requirements based on new court decisions, new statutory requirements and industry best practices.
- **Understand where data resides in your organization**
There can be a large number of different platforms on which discoverable data is stored, including email servers, instant messaging servers, file servers, desktops, laptops, smartphones, employees’ home computers, backup tapes, archives, voicemail systems, mainframe and other host-based systems, ‘live’ message stores that have not yet been backed up or archived, USB thumbdrives, CD-ROMs and even old diskettes. It is imperative for organizations a) to know where all of its relevant data resides, b) how to access that data without interrupting normal business processes, and c) how to access that data without spending huge amounts on IT, legal or other staff members’ time searching for it.
- **Make sure that all needed data is accessible**
Although data may exist in an organization, it may not be easily accessible during the timeframes required for e-discovery. For example, Osterman Research has found in a recent study that the vast majority of organizations allow users to store information in local message stores, such as local hard disks. However, only 31% of these local message stores are backed up to a central location and are accessible to the organization at large for long periods of time. That means that while the data in your organization is *technically* accessible, it may not be *practically* accessible.

Clearly, restoring every piece of data is not necessarily a sound practice in every situation. Each organization must decide, based on a variety of factors, what data it should restore and what data it can safely leave inaccessible.

- **Create as complete an e-discovery repository as necessary**

Centralizing data stores and consolidating them into a smaller number of repositories can provide significant benefits during e-discovery. Migrating old backup tapes into a messaging archiving system can result in faster searches, reduced costs and greater responsiveness to e-discovery requests. For example, some vendors offer services that will migrate data from tape to an archive. Migrating tapes in this manner can provide a dramatic reduction in the IT costs required to manage backup tapes.

It is important to note, however, that some litigators would advise their clients not to make all data accessible for e-discovery purposes – each organization will have to determine the most appropriate and least risky strategy.

- **Develop a post-processing strategy**

It is also important to develop policies and procedures for activities that occur after the legal action, legal hold, etc. have been completed. For example, it will be important to develop a policy for ingesting data back into the archive or otherwise noting that certain files, emails, etc. have been part of the legal action. While there are a variety of methods that organizations may want to consider, this should be on list of “to-do” items in developing an appropriate strategy.

CONSIDER ALL STAKEHOLDERS’ REQUIREMENTS

E-discovery will impact all parts of an organization: legal, HR, IT, finance, corporate management and others. It is important, therefore, to implement an e-discovery strategy and to make technology choices based on the needs of all relevant stakeholders. For example, the legal department and the IT department will often have very different requirements for the technologies designed to support e-discovery. It is critical to make sure all relevant parties in an organization are represented in some sort of cross-functional team that will develop the e-discovery strategy and choose the right technologies to meet all requirements.

IMPLEMENT A LEGAL HOLD CAPABILITY

When a hold on data is required, it is imperative that an organization immediately be able to begin preserving all relevant data, such as all email sent from senior managers to specific individuals or clients. A properly configured archiving system will allow organizations to immediately place a hold on data when requested by a court or on the advice of legal counsel and retain it for as long as necessary.

If an organization is not able to adequately place a hold on data when required, it can encounter a variety of serious consequences, ranging from embarrassment to serious legal sanctions or fines. Litigants that fail to preserve email properly are subject to a wide variety of consequences, including brand damage, additional costs for third-parties to review or search for data, court sanctions, directed verdicts or instructions to a jury that it can view a defendant’s failure to produce data as evidence of culpability.

DEPLOY THE RIGHT ARCHIVING TECHNOLOGY

All organizations should deploy an archiving capability. An archiving system should automatically index messaging and other content that the organization must retain, store this content in archival storage where it can be retained for long periods, and provide robust capabilities so that the archive can be searched and the appropriate data selected during e-discovery.

There are several options for deploying an archiving capability, including software installed on in-house servers, self-contained appliances, and in-the-cloud services. Regardless of the form factor chosen, it is critical to select an archiving capability that can accommodate long-term requirements for data retention. Many organizations have been forced to replace older archiving systems, often because the systems were not architected with sufficiently rapid search capabilities.

Because email is the largest and, for the majority of organizations, the most important data repository, it certainly makes sense to first implement an email archiving system. However, organizations must consider all ESI in their e-discovery strategy, including instant messages, files in collaboration systems like Microsoft SharePoint, postings in wikis and blogs, word processing files and spreadsheets on shared file servers, and any other electronic content that might be relevant in a legal action. As a result, it is important to choose an archiving technology that will meet all of your ESI-production requirements.

DON'T RELY ON BACKUP TAPES AS YOUR "ARCHIVE"

Almost all organizations perform regular backups of their email system, file servers and other data repositories. While many organizations believe that these backups constitute an "archive" of their business information, this is not the case. A traditional backup takes periodic "snapshots" of active data so that deleted or destroyed records can be recovered, such as after the failure of a server's hard disk or an application upgrade gone awry. Most backups are retained typically for no more than 60 to 90 days as subsequent backups on tape or disk are recycled or overwritten. While backups can be preserved indefinitely in order to preserve business records, there are three fundamental problems with using backups as an archive:

- Backups constitute "raw" content and lack any sort of indexing. If information, such as content that must be produced in response to a discovery order, must be obtained from a set of backup tapes, the process is typically time-consuming, highly disruptive to IT staff and very expensive, particularly if third-party forensics firms must be used. For example, in the case of *Bank of America v. SR International Business Insurance Co. Ltd.*, it was estimated that the cost to produce emails from 350 to 400 backup tapes would range from \$3,750 to \$4,300 per tape.
- The integrity of backup tapes is not guaranteed. There have been many cases in which older tapes were not readable due to data corruption or physical corruption of the media itself.
- Because backups capture a snapshot of data, information generated and deleted between backups will not be captured. For example, if an organization is required to preserve communications between senior management and external auditors for

purposes of compliance with Sarbanes-Oxley, an email sent from the CEO to the external firm at 10:00am and then deleted from the “Sent” folder at 2:00pm on the same day will never be captured in the nightly backup.

- Interestingly, the most legally significant reason not to immediately restore backup tapes or use them as an archive is that doing so makes what is arguably “inaccessible” under the revised FRCP quite accessible, and therefore subject to discovery. Whether or not you migrate content on backup tapes to an archive will depend on the advice of your legal counsel, among other factors.

While backups are a critical and necessary component of an organization’s data management strategy, they are not a substitute for an archive. In short, a backup is designed to preserve data for short periods in support of the physical infrastructure that an organization maintains, while an archive is designed to preserve information on a long-term basis in support of more strategic corporate objectives.

PRESERVE METADATA

Metadata – the structured, encoded data that describes characteristics of information-bearing entities, or data about the data – is an increasingly critical source of corporate content. Metadata is important for a variety of purposes, not least of which are statutory requirements and e-discovery purposes. An inability to maintain or produce metadata can have serious consequences.

In many cases, the metadata associated with electronic content is just as important as the data itself, and so must be preserved along with this content. Further, the authenticity of the metadata must be maintained in order to satisfy regulators or courts that the electronic content demanded is genuine. Illustrating the need to preserve metadata adequately are the following sample court cases in which metadata played a role:

- ***Nova Measuring Instruments Ltd. v. Nanometrics, Inc.***
417 F. Supp. 2d 1121 (N.D. Cal. 2006)
In this patent infringement case, the judge ordered Nanometrics to produce documents in their native file format along with their original metadata within 14 days of the order. In issuing the order, the judge cited two previous cases in which native file formats and metadata were required to be produced.
- ***Williams v. Sprint/United Mgmt. Co.***
230 F.R.D. 640 (D. Kan. 2005)
In this case, the defendant deleted metadata associated with the Microsoft Excel spreadsheets it provided to the plaintiff as part of the discovery process. While the court did not sanction the defendant for doing so, the court ruled that metadata is relevant and that it should have either been provided along with the spreadsheets, or an objection to its production should have been raised during discovery.

Metadata will increasingly be required for production during legal discovery or regulatory audits. Even in the absence of requirements to preserve or produce metadata, Principle 12 of The Sedona Principles for Electronic Document Production (2005) states in part, “if the producing party knows or should reasonably know that particular metadata is relevant to

the dispute, it should be produced.” Metadata preservation, therefore, is clearly a best practice and will become increasingly critical as a part of the e-discovery process.

KEEP ONLY WHAT YOU NEED

It is important for any organization to retain all of the electronic data that it will need for current and anticipated e-discovery and other retention requirements. However, many organizations, either by overspecifying the amount of data they must retain and/or not establishing appropriate data deletion policies, retain more information than is necessary. This can result in dramatically higher e-discovery costs because more data must be reviewed, as well as unnecessarily high storage costs.

Related to the best practice of retaining only the information necessary to satisfy e-discovery and other obligations is the best practice of deduplicating data. For example, true single-instance storage can reduce the size of some data repositories by up to 80%. This can significantly reduce e-discovery and storage costs.

IMPLEMENT AN INFORMATION RISK MANAGEMENT PROCESS

An information risk management process focused on e-discovery is an important best practice that will help an organization to identify the risks it faces and help it to mitigate these risks. The advantages of establishing an information risk management process are that it will make senior management aware of the risks associated with e-discovery, aid in the development of policies focused on managing or mitigating risks, improve the methods by which information assets are managed, improve information security, and assist organizations in choosing the appropriate technology to manage e-discovery and information security.

Summary

E-discovery is becoming an increasingly important consideration for almost all organizations as a result of the enormous number of civil cases filed each year, the growing proportion of business records that are stored electronically, new statutes at all levels of government focused on electronically-stored information, and a growing body of court rulings that are making the discovery and presentation of electronic data more important.

In order to satisfy e-discovery obligations, organizations should be fully aware of their current and reasonably anticipated information retention obligations, become much more proactive about how they retain and manage data, implement appropriate technology that can archive data and allow legal holds to be implemented easily, and take the other steps necessary to minimize the risks of non-compliance with e-discovery obligations.

Sponsor of This White Paper

Trend Micro™ Message Archiver efficiently manages secure email storage in an encrypted archive. It provides fast, easy search capability and reduced storage cost, while enabling e-discovery and compliance with data retention regulations. The tamper-resistant archiving solution allows authorized personnel to search and retrieve emails and attachments quickly throughout an organization and export them in native format.

Message Archiver's secure, tamper-evident design can prove emails have not been altered thus increasing their legal weight:

- Digital fingerprints and timestamps on each email prove it has not been modified
- Emails are stored with encryption to prevent tampering and protect privacy
- Secure logs track all administrative activity and privileged user searches
- No SQL database is required which could provide a backdoor to access, alter, or delete data

Trend Micro Incorporated, is a recognized global leader in Internet Secure Content and Threat Management with 20 years in the security industry. Trend Micro focuses on securing the exchange of digital information for businesses with in-the-cloud, gateway, server, and desktop solutions on multiple form factors. For over 10 years, customers have relied on Trend Micro's messaging security solutions and in 2008 this protection was extended to cover email archiving, email encryption, and e-discovery.

A transnational company, with headquarters in Tokyo and operations in more than 30 countries, Trend Micro's trusted security solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit the Trend Micro Web site at www.trendmicro.com.



Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014
+1 800 228 5651
www.trendmicro.com

© 2008 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.