E-Discovery Quagmires
An Ounce of Prevention is Worth a Pound of Cure

Rebecca Herold, CISSP, CISA, CISM, FLMI
Final Draft for February 2007 CSI Alert

While updating the two-day seminar Chris Grillo and I give through CSI (Effectively Partnering Information Security and Privacy) we have had much discussion about the impact of the new electronic discovery (e-discovery) rules within the Federal Rules of Civil Procedure (FRCP) that went into effect on December 1, 2006. Chris has been addressing this issue within his own organization, and I have been helping some organizations to create or update procedures for e-discovery activities. We both agree that e-discovery must include significant IT participation and preparation to not only be most efficient, but also to help mitigate costs and prevent fines related to e-discovery activities. A comparatively small amount of preparation for e-discovery could save a significantly large amount of money and resources in the long run.

Is your organization prepared for e-discovery? Odds are it is not. According to an October 2006 LexisNexis survey of the members of the Association of Corporate Counsel, only 7% of corporate attorneys indicated they were prepared for the new rules. In fact, over 50% of the lawyers were not even aware that new rules were going into effect on December 1. Here are some things you need to discuss with your IT folks to help ensure they know about the new e-discovery rules.

IT and E-Discovery

Unfortunately, most information security and IT professionals get thrown into the deep end of the legal pool when it comes to dealing with e-discovery and they must quickly learn the issues involved, or they may find their career with their organization quickly sinking if e-discovery activities are launched and they overlook some key data that subsequently results in large fines and penalties. I'm going to discuss some e-discovery issues IT and information security folks need to know about. This is not to be considered as legal advice. This is just to help you establish a basic foundation of knowledge about this topic as it relates to IT.

The term "discovery" basically describes the methods by which the parties to a lawsuit, the prosecution and the defendant(s), can obtain information from witnesses and documents from the opposing parties. Discovery methods have historically relied predominantly upon exchanging paper documents. However, as more and more information is stored in multiple forms electronically, e-discovery is becoming the most common discovery activity, and organizations are quickly realizing that they need to work closely with IT and information security to help with the e-discovery processes. According to a 2003 study from the University of California at Berkeley, 93% of business information was in electronic format. According to Kazeon, an information management company, that has now increased to 99% of business information in electronic format. It makes sense that when suits arise involving the production and inspection of information that IT will need to be closely involved.

What is the E-Discovery Process?

The judicial recommendations for the updated FRCP require the following. I've included a few notes about the IT-related tasks:

1. The parties involved in the suit must meet within twenty days after each defendant has appeared in a civil proceeding. The parties must discuss whether there exists electronically stored information that is reasonably likely to be requested during the

discovery process. IT will need to be involved with answering this question. If there is, the parties must discuss:

(1) **Preservation of the information**. IT must be able to discuss current retention practices and locations where possible data related to the case is stored.

(2) **The form in which the information will be produced**. IT must be able to discuss the forms in which data is stored, such as within specific servers, on backup tapes, in voice mails, in instant messaging files, on DVDs, and so on. They must also be able to discuss how to get this information, such as in raw data files, in easy-to-read lists or text documents, only after decrypting files, and so on.

(3) **The time within which the information will be produced.** IT must be able to tell if the data is active (still being used for business processing) or is inactive (no longer used for business processing, often less accessible as a result, such as on archived backup tapes, in legacy storage systems, and so on.) IT must then be able to indicate how long it would take to produce each type of data, and the costs involved.

(4) **The method for asserting or preserving claims of privilege or protection as trial-preparation materials, including whether claims may be asserted after production.** There may be information being requested subject to lawyer/client privilege that your organization should not provide; for example, email discussions about a case between legal counsel and the CEO, or data with protected health information, and so on. IT should be able to determine the methods for how such data can be withheld or protected.

(5) **The method for asserting or preserving confidentiality and proprietary.** There may be some very sensitive and confidential data within the same storage locations that cannot realistically be removed and have no relation to the proceedings; such as personally identifiable information within a database or flat file that also includes data related to the case. Confidential data could also be within metadata found within data files and electronic documents. IT should be able to determine the methods, if any, for how such data can be withheld or protected.

(6) **Whether allocation among the parties of the cost of production is appropriate.** IT should be able to provide estimates for the costs, man-hours and other related resources that would be necessary to produce the requested data.

(7) **Any other issue relating to the discovery of electronically stored information**. IT should be able to indicate if the data was created using a system no longer available or no longer in production, whether the data is physically housed in a different geographic region, if the expertise to extract the data exists in-house, and any other issue impacting the ability to produce the data.

2. If the parties agree that discovery of electronically-stored information is reasonably likely to be sought during the discovery process in the proceeding, the parties must develop a proposed plan for the discovery of electronically-stored information that indicates the views and proposals of the parties concerning the matters specified in subsection (a) of the FRCP. IT must ensure the details related to the tasks and costs for retrieving the data are accurate and complete.
3. Each attorney and each unrepresented party that has appeared in a civil proceeding are jointly responsible for arranging the conference required under subsection (a), for participating in good faith in the conference, developing a proposed plan, and

submitting to the court a written report within fourteen days after the conference that summarizes the plan and specifies the issues about which the parties were unable to agree. IT should plan to attend such meetings and provide accurate information about the technical issues of the data being discussed.

What Are the Costs for E-Discovery?

When organizations become involved in e-discovery activities it will cost them potentially large amounts of not only money but also other resources. According to the National Center for State Courts, "One reported case, for example, involved the restoration of 93 backup tapes. The process was estimated to cost $6.2 million before attorney review of the resulting files for relevance or privilege objections. Complete restoration of 200 backup tapes of one of the defendants in another prominent reported decision was estimated to cost $9.75 million, while restoration of eight randomly selected tapes to see if any relevant evidence appeared on them, could be done for $400,000."

Kazeon indicates that historically most of the e-discovery work was either done manually or was outsourced. "However, the costs we are seeing range from $2,000-$3,000 per GB to do this work. Large organizations are now looking to bring this in house given the new FRCP requirements and control costs." Kazeon also provided the following statistics:

- Discovery is the number one new litigation-related burden for general counsel at companies with annual revenue exceeding $100 million
- Average US companies with annual sales of $1 billion or more are engaged in 556 open legal cases, with about 50 new suits added yearly (2006 survey by Fulbright & Jaworski, LLP)
- Market price for "processing and review" is $2,000 per GB

The costs come not only from the time it takes the organization's own personnel to collect the data, but there are often additional costs for hiring e-discovery systems and applications experts to obtain the files and data requested by the opposing party. E-discovery experts frequently are engaged to take the collected data, convert the data to indexed and reviewable files, and then make the data ready to be produced for the opposing party. The most expensive experts are forensic examiners who are often also engaged to search for deleted documents, e-mail messages, and systems data and logs.

How Does Safe Harbor Relate to E-Discovery?

Most organizations have some type of records retention practices in place, formal or informal. Many IT areas have established retention periods for email, shared folders, and other typical "non-production" storage areas in an attempt to save storage space. However, what happens if some important records related to a lawsuit were deleted as a result? The safe harbor amendment to the FRCP, Rule 37(f), is significant because it allows organizations party to suits to be protected from court sanctions if the stored information was deleted, or otherwise lost, as a result of "routine, good faith operation."

Another safe harbor is a change to Rule 26(b)(2) that requires the requesting parties in a suit to get a court order before the responding party has to provide any electronic information that it indicates is "not reasonably accessible because of undue burden or cost." The responding party would need to identify the sources of the data that has not been searched or obtained because of the excessive costs and other burdens related to getting the data. The responding party must document and demonstrate why is it not reasonably accessible. However, the court could still order the data to be produced with “appropriate terms and conditions.” This means that, as one possibility, partial data (sampling) could still be required, or as another possibility, that the requesting party would have to pay the producing party for the involved costs.

Sampling is an option that the Advisory Committee included in their notes with the amended rule 26(b)(2) to determine whether the data is relevant or not reasonably accessible. By taking a sample the respondent to the request can provide the court a way to determine if relevant information is truly not reasonably accessible, and also allow them to determine the burdens of producing the data versus the value of the data to the case.

What Metadata Should You Worry About?

According to advice published October 19, 2006 by the Maryland State Bar Ethics Committee, Maryland attorneys who produce e-discovery materials must take reasonable measures to avoid the disclosure of confidential information embedded in the electronic materials. IT folks more commonly know this embedded data as “metadata.” IT must work closely with their legal counsel during e-discovery to identify and clearly communicate where metadata related to the case may be located, and then to ensure that all metadata not necessary for production has been removed as much as possible.

Metadata is also addressed within an amendment to FRCP 26(b)(5) about the inadvertent production of privileged information in discovery. The amendment allows parties to retrieve electronically stored information that is provided to other parties unintentionally during discovery. After being notified by the producing party that it received privileged information, the receiving party must return it. If the receiving party believes it is entitled to the information, it has the burden of proving this need to the court.

Other IT Related Issues

A revision to Rule 33 states that the responding party "may be required to provide some combination of technical support, information on application software, or other assistance" to enable the requesting party to understand the business records produced. IT resources need to be available to provide this support, information and assistance.

An amendment to Rule 34(a) added a specific category of "electronically stored information" that would be included as information expressly subject to production in discovery along with "documents," which broadened the scope of the types of documents that can be requested for inspection, copying, testing or sampling. Now basically any type of electronic data can be requested, such as audio files, sound records, images, messaging files, and any other type of electronic data. Your organization may need to extract information from such files as voice mails, streaming video, VOIP files, instant messaging files, and so on.

An amendment to Rule 34(b) allows a requesting party to specify the form in which electronic data must be produced. If a party does not specify the form of production, a responding party must produce the information in the form in which it is "ordinarily maintained," or a form "which is reasonably useful by the requesting party."

How Should Legal Work With IT?

E-discovery typically is launched when receiving a:

- notice to produce documents, or a
- subpoena that requires documents be made available for inspection and copying, or a
- request for admission requiring the accuracy of specific facts to be confirmed.

Your legal counsel should be the person receiving such requests, as is appropriate. Your legal counsel should also be spearheading and overseeing all e-discovery activities. However, your legal counsel is typically not an IT expert. An IT contact, or team of contacts, with expert knowledge of your organization's network, computer, systems and applications should be involved to provide your legal counsel with the information necessary for the correct legal decisions to be made.

Legal counsel drives the need for e-discovery, but IT must provide the technology expertise and activities to perform the e-discovery. Legal counsel must be responsible for ensuring the relevant data is preserved and available, but IT must provide the means to preserve and make available the appropriate data. The e-discovery issue cannot be delegated to the IT department, but it cannot be conducted without IT.

Legal counsel must be knowledgeable about your organization's records retention policies and data management processes. Likewise, IT must possess an understanding of the legal issues involved with records retention, records disposal, and other data management and discovery issues that are covered by laws, regulations and contractual requirements.

What Steps Should an Organization Take?

Read through the FRCP closely; you can find it at: http://www.supremecourtus.gov/orders/courtorders/frcv06p.pdf. Also know the state level rules governing e-discovery. On Novebmer 21, 2006 the National Conference of Commissioners on Uniform State Laws (NCCCUSL) published a draft of proposed uniform state court rules governing e-discovery. This draft is verbatim in many places from the FRCP and is available at http://www.law.upenn.edu/bll/ulc/udoera/2006postdraftnovember.htm.

The FRCP and growing numbers of state level rules require the identification of contact persons with extensive knowledge of IT systems to assist in e-discovery activities. Use the following as a checklist and talking points when discussing this with Legal. The "FRCP Issue" column shows the terminology that should be familiar to legal counsel. The "IT Activities" column lists what IT and information security will typically need to do for the issue.

FRCP Issue	IT Activities
IT Responsibility	• Be part of a records management and data discovery team. Members should include representatives from legal, IT, records management, information security and human resources. • Ensure there are formally documented responsibilities for each team member. • Identify a team member from IT to work with the requesting party if they need help understanding the records provided. • Establish a procedure to provide requested data without giving the

FRCP Issue	IT Activities
	opposing party access to your network and computer systems if at all possible. Doing so could result in unauthorized access to confidential data, inadvertent loss or modification of data, or other negative impacts. • Document all activities involved with each discovery process performed.
Formally Address E-discovery	• Ensure IT activities are included within a well-documented e-discovery policy that legal typically should manage. • Have well documented e-discovery IT procedures based upon your business environment, computer systems, and resources (both financial and personnel) available. • Have well-documented procedures for retrieving data in response to e-discovery or court orders. • Ensure litigation hold procedures include ways to ensure: o All forms of electronic information related to the case are included o All potentially involved personnel are effectively notified and comply with the hold o Data is not inadvertently or intentionally modified or deleted after the hold has been established • Educate legal counsel and other records management and discovery team members about the IT discovery and retention procedures.
Producing data	• Consistently follow well-documented information classification policies and procedures. • Maintain an inventory showing the storage locations for all types and classifications of data. • Create a data flow map showing where each type of data is collected, stored, and where it leaves the network and other corporate systems. Be sure to identify the mobile computing devices and storage media, audio and video files, and so on.
"Reasonably Accessible"	• Identify and document the locations that are "reasonably accessible" according to IT defined parameters. • Document procedures to produce the reasonably accessible data as quickly and economically as possible. • Identify and document the locations that are NOT reasonably accessible and document why they are not accessible. Include estimates of the associated costs and times that would be involved to access the data from these locations.
Safe harbor & Records Retention	• Create or update existing records retention and disposal policies and procedures to include: o How and when to store each type of data o How and when to dispose of each type of data
Sampling	• Establish procedures to extract representative samples of data from identified storage locations. • Document the resources and costs for extracting varying sizes of samples.
Metadata	• Document possible metadata relevant to the case and the corresponding storage locations.

FRCP Issue	IT Activities
	• Establish procedures to return, sequester or destroy data when responding parties indicate they have inadvertently given your organization privileged data. • Establish procedures to request data back when your organization inadvertently gives privileged information to the requesting parties. Clearly indicate the data, data format and other details to enable the other party to completely return, sequester or destroy the data, based upon what your legal counsel determines appropriate.
Types of data	• Document active data and corresponding storage locations relevant to the case, such as but not limited to: o Databases o Email o Worksheets o Websites on both the Intranet and Internet o Electronic documents o Metadata • Document inactive and inaccessible data, and corresponding storage locations, related to the case, such as but not limited to: o Backup media o Off-site storage and archives o Legacy data and any legacy systems that must be used but are no longer supported o Deleted data and other residual data that may exist • Document all the possible types of forms in which the data can be produced. • Communicate the data types and locations to legal counsel.
Notice of litigation	• Document procedures to o Determine where electronic data is or could be stored and the individuals who may have the electronic data o Establish a “litigation hold” for the relevant data o Hold a records management and discovery team meeting o Determine the relevant data and how to produce the data o Identify the active and inactive data o Identify the accessible and not easily accessible data o Document the costs and resources for producing each kind of data
Provide Key Information to Legal Counsel	• Document the hardware and software relevant to the case used within your organization. • Gather documentation for how, when and where relevant data is saved. • Gather documentation for the email systems that are used, and whether they are managed in-house or outsourced. • Gather documentation for the backup procedures that are used. • Document the archival and legacy information relevant to the case. • Provide the current document retention and disposal policy and related procedures. • Participate in discussions to address any additional specific inquiries for each particular case.

FRCP Issue	IT Activities
Pretrial conferences	• Identify IT positions and/or personnel to participate in pretrial conferences.

Rebecca Herold, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. Her latest publication is The Privacy Management Toolkit (Information Shield). She can be reached at rebeccaherold@rebeccaherold.com or http://www.rebeccaherold.com.