

# DRAFTING A 'DREAM TEAM' TO PREVENT E-DISCOVERY NIGHTMARES

RIM professionals are in a unique position to help their organizations prevent electronic discovery problems. But, this requires them to take the lead in facilitating coordination and cooperation among RIM, IT, and legal staff.

**Amy Dove, PMP**



The proliferation and explosion of electronic information has forced IT, legal, and RIM professionals to work together to gain control of organizational information. The legal stakes are higher now, as well, as lawyers and judges have become more savvy about e-discovery. A case can take a turn for the worse if an organization's document preservation processes are called into question and a judge sanctions it for *spoliation*, which is the legal term for the intentional or negligent alteration or destruction of evidence before or during litigation.

The January 2010 ruling issued by Judge Judy Scheindlin of the U.S. Southern District of New York in *Pension Committee of the Univ. of Montreal Pension Plan v. Banc of America Securities LLC (Pension Committee)* emphasizes that organizations need to have control over their data at all times. RIM professionals must be cognizant of their own role in preparing their organization for litigation and protecting it from negligence by bridging the gaps between legal, IT, and records business units in responding to a discovery request.

For example, litigation teams often request *data maps*, which are graphical representations of the location and flow of an organization's electronically stored information (ESI), as part of the e-discovery process. Usually, IT is tasked with creating the map; however, RIM professionals can use the push to help get their RIM program in place and compliant with e-discovery requirements. RIM professionals are especially well poised to take the lead in this area to ensure the organization is prepared for litigation – and to develop a new set of skills and value within the organization in the process.

### Legal Issues to Understand

To interface effectively with legal staff and be prepared for litigation,

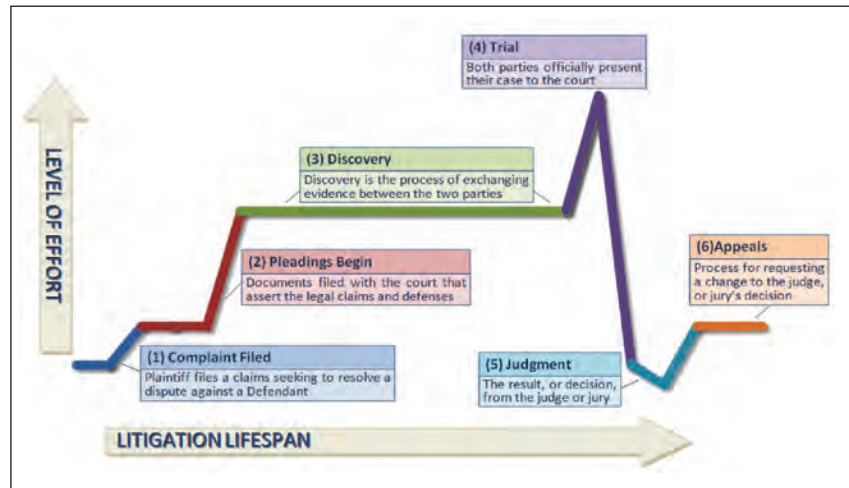


Figure 1. Phases of a Lawsuit

RIM professionals must understand the following legal issues.

#### The Litigation Hold Process

A litigation hold notification is issued by the legal department and requires the organization to preserve all material that may be relevant to a litigation matter and ensure that it is not destroyed while the litigation is pending. Notifications should include the type of information to be retained and for how long. A litigation hold covers hard copy material, as well as ESI.

Implementing and maintaining a litigation hold is an iterative process that may include interviews, reminders, audits, and follow-up to ensure compliance. This requires an organization to have a good understanding of where its data is stored so it will not be destroyed or rendered unusable.

A litigation hold must go into effect as soon as an organization has reason to believe that it will be sued. Events that might trigger a litigation hold could be as subtle as a manager receiving a report about an internal harassment incident or as evident as a letter from an attorney threatening a lawsuit.

In the *Pension Committee* case, Scheindlin determined plaintiffs were grossly negligent for not having suffi-

cient written litigation hold guidelines and for continuing to destroy documents after the litigation had commenced. She ruled the jury could assume that the missing documents were detrimental to the case. The plaintiffs took a severe blow because they did not implement a solid litigation hold, and they deleted relevant electronic material due to sloppy document retention policies.

Organizations are commonly sanctioned for failing to preserve documents, and the attorneys are sometimes sanctioned, as well. A diligent RIM professional can help prevent these sanctions.

#### The Discovery Process

*Discovery* is the process of exchanging evidence between parties. As shown in Figure 1, it is the third phase of a lawsuit, and it is the most costly and time-intensive part of litigation. During discovery, each side must share with the other side all information that is relevant to the matter, and significant penalties may be levied on any party that does not hand over information properly.

For example, in August 2010, in *Harkabi v. Sandisk Corp.*, Sandisk Corp. was ordered to pay the plaintiffs \$150,000 in compensation for its delay in producing evidence and to

## The inability to show proper and consistent records management practices early in the case can call into question the organization's entire discovery response and start its legal team off in a very bad position.

deter similar future conduct.

Because discovery involves the physical collection, restoration, and review of information, it is a costly process. If the scope of the information an attorney requests is too broad and results in excessive information being produced, the litigation costs will be exponentially increased.

However, a request that is too narrow also carries a risk in that another costly and time-consuming collection may be required. For this reason, RIM professionals should be mindful of the attorneys' approach and work with them to define the search and collection criteria to fit that approach.

The discovery process includes many avenues for gathering information:

- *U.S. Federal Rules of Civil Procedure* (FRCP) Rule 26(a)(1) Disclosures – The FRCP are for all federal and many states' court cases the general rules governing the scope of discovery. Rule 26(a)(1) mandates disclosure of basic information about the case, such as descriptions of document categories and names of witnesses, to the other side prior to a discovery request.
- Meet and confer – One of the most important aspects of the 2006 amendments to the FRCP is that parties in a lawsuit must “meet and confer” to address discovery issues, particularly e-discovery, early in the case. FRCP Rule 26(f) specifically

states that parties must bring discovery issues out in the open as early as possible to avoid delays and possible penalties. To ensure this, at this conference:

- The timeline for the case is outlined and agreed to by both parties and the judge.
- Attorneys discuss what type of electronic information exists that may be relevant to the case.
- Attorneys begin working out what information will be produced and when.

Therefore, RIM professionals can help the legal team prepare well before the meet and confer. At the most basic level, the attorneys need to know what type of information is relevant to the lawsuit, the format type, quantity, and if any of it is duplicated. They should also develop templates of data charts that can be filled in with these document specifics.

- Discovery requests – This document, usually called a “request for production,” lists all of the types of information each party wants the other party to provide. Ultimately, information is “produced” when it is formally delivered to the opposing party.
- Subpoena – This is a formal document filed with and ordered by the court that compels a person to appear in court to answer questions related to the litigation or to turn over

information. In civil litigation, third-party subpoenas are often issued to acquire documents from entities that are not direct parties in the lawsuit, but have information that pertains to the matter.

- Depositions – Depositions are statements taken under oath from witnesses involved with the litigation. The purpose of depositions is to get the facts of the case into the official record prior to the trial. RIM professionals are increasingly called to testify as FRCP 30(b)(6) expert witnesses about the state of records in their organizations, so they need to be able to explain the records management structure and processes and how they ensure compliance with these processes. Increasingly, this type of deposition is used to find out the process an organization took to secure, locate, and produce documents.

The inability to show proper and consistent records management practices early in the case can call into question the organization's entire discovery response and start its legal team off in a very bad position. Increasingly, opposing counsel use these types of depositions as fishing expeditions to find deleted or ruined data they can use to secure sanctions. To be prepared, RIM professionals must:

- Ensure records management procedures are up to date.
- Be ready to discuss the litigation hold process in detail.
- Collect manuals, instructions, and notices the organization uses to educate, train, provide notice, and ensure compliance, as well as audit procedures; these may need to be produced to opposing counsel.
- Have a good understanding of IT department practices and be prepared to speak to data storage and back up processes. There are areas of overlap between IT and RIM and it is especially important to make sure everyone is on

the same page.

An organization needs to start thinking and preparing for discovery well before the discovery request arrives – maybe even before the complaint is filed. If attorneys are caught behind and unprepared, well-prepared RIM professionals can help save the day by having current information about the state of their organization's data readily available. They should also make it part of their routine business to know what lawsuits are coming and set up templates and checklists for

the most common types of matters.

### IT Issues to Understand

Similarly, part of being prepared for collaboration with IT and for litigation includes understanding the following issues related to information technology.

#### IT Roles and Responsibilities

The various IT roles and knowledge areas can be quite diverse, so it is important for RIM professionals to understand each position so they know

where to turn to locate the information they need. Figure 2 lists these position names and functions.

#### Server Types and Virtualized Data

The problem facing many IT departments can be likened to urban sprawl – where servers spread. (See Figure 3 for a list of common server types and their functions.) This problem is multiplied when IT departments create *virtual servers* by using software to “carve up” spaces on a single server, allowing it to function – and “virtually” appear to other machines – as multiple servers. This is attractive to IT departments because, with each space on the virtualized server available to be dedicated to a specific need, they don't need to buy additional hardware to bring up a new server for a specific purpose.

It is important that RIM professionals understand where and how IT is using virtual servers so they know exactly where their data is stored. If an organization's virtual servers are hosted in offsite locations, the organization does not have direct control over the physical machine. Therefore, RIM professionals should understand the agreements in place for retrieving information that is not stored in their own facility.

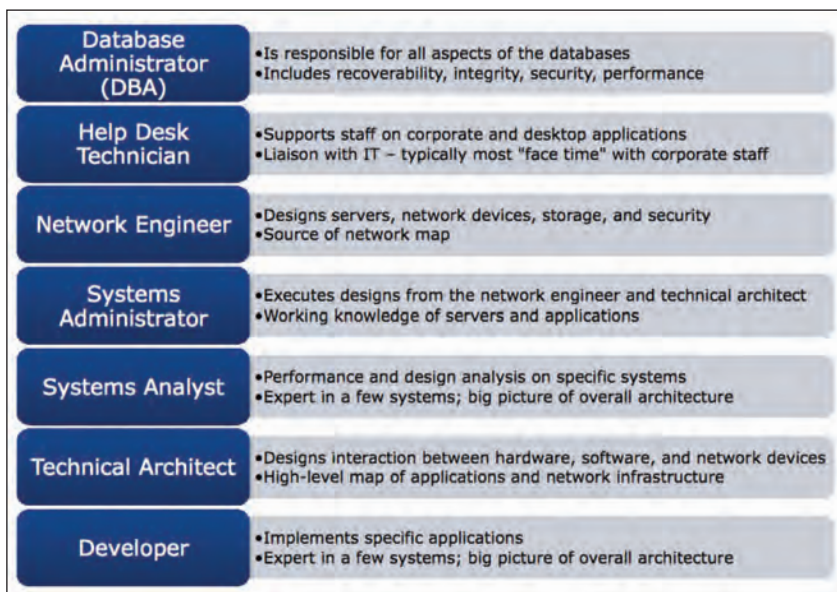


Figure 2. IT Roles and Responsibilities

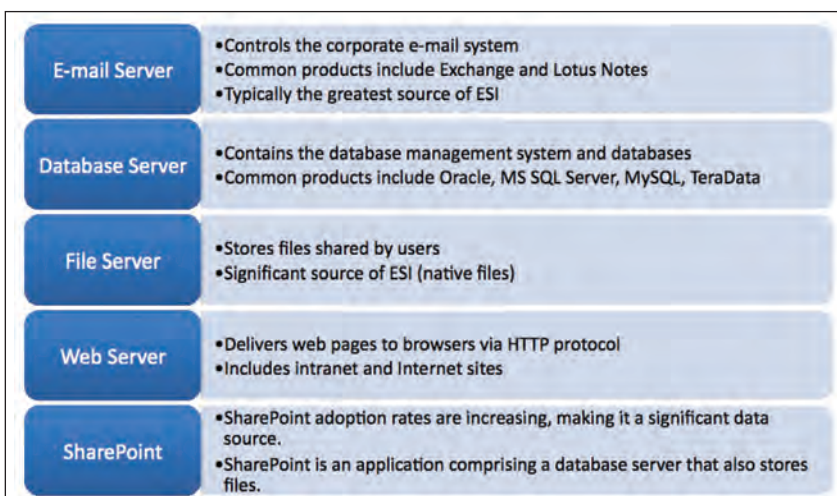


Figure 3. Common Server Types and Their Functions

#### Data Maps

A *data map* is a graphical representation of the location and flow of an organization's ESI. The IT department creates data maps to:

- Understand the location of all the assets in their control
- Aid in load balancing the machines in the network, identifying road-blocks, and creating efficiencies
- Help with planning security controls

A data map is an extremely rich source of information to prepare for a discovery request. Data maps have been used successfully in court to visually demonstrate the complexity of a computer network and to get the court to agree that certain portions of data

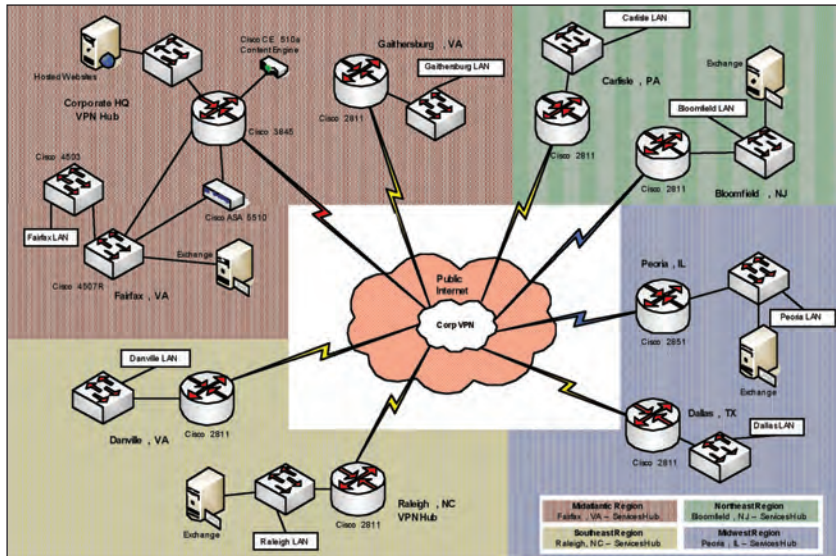


Figure 4. Data Map: Visual Depiction of Where Data Resides

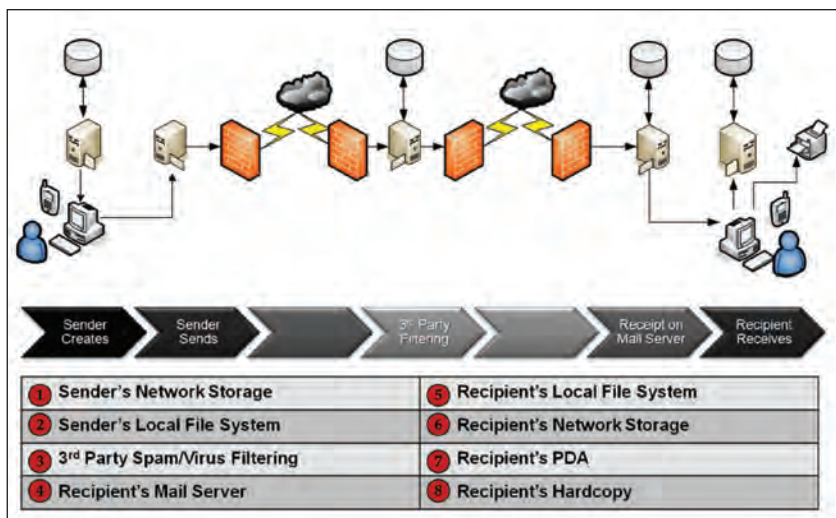


Figure 5. Path of One E-Mail Stores it in Many Places

were inaccessible and did not have to be produced.

Figure 4 is a portion of an actual graphic representation of a company's wide area network server structure used in a 30(b)(6) deposition. The attorney and deponent, the chief technology officer, successfully used this map to explain the complexity of the network to the opposing side and to come to agreement that large amounts of data were either irrelevant or inaccessible and, therefore, not discoverable. This agreement

saved the organization substantial discovery costs by helping the opposing side understand the data was difficult to access, not likely to contain much relevant information, and not worth the expense for either party to review.

Data maps should also include supplementary information about the data on the servers, including time periods when servers and systems were online, the content of the servers, and who has access to this information. For example, it may be valuable to

show that a particular server is a file server at the corporate headquarters that holds all of the accounting departments audit files, but not the human resources personnel files.

This supplemental information can help point people to the right place more quickly and is valuable, but it can be time-intensive to gather. Information about the content of the servers is extremely valuable to RIM professionals aiding in the discovery process.

It is also important to know where all duplicate data resides in order to decrease the size of the collection and review costs by collecting only one set of the data and as a potential backup for an accidental deletion. E-mail, as shown in Figure 5, is a good example of data that may reside in multiple locations.

#### Backup and Rotation Schedules

Data on network servers and machines is routinely used primarily for disaster recovery and business continuity purposes. This information must be considered when responding to discovery requests. RIM professionals are obligated to understand how the backup process works at their organizations.

At Duke Law School on May 10-11, 2010, the Federal Advisory Committee on Civil Rules held a conference to re-examine the FRCP. During the two-day conference, a new rule to address preservation and spoliation of ESI was developed to more closely define and govern this area. This movement further emphasizes that organizations must understand when and how their data is getting backed up and deleted on a regular basis, not just when litigation is pending.

The key information RIM professionals need to learn from the IT department is:

1. What data is backed up?
2. When is the backup made? What is the frequency – daily, weekly,

monthly, annually?

3. In what format is the backup copy made?
4. Where is the backup copy stored?
5. For how long is it stored?
6. How and when are backups overwritten or destroyed?

Once backups are targeted for the discovery process, the legal team will also need to know what kind of effort it will take to recover that information so it can be produced.

### **Safe Harbor Clause**

The Safe Harbor clause recognizes that there are routine and necessary computer operations that can alter or destroy information and that, absent exceptional circumstances, sanctions cannot be imposed for loss of ESI as the result of routine, good-faith operation of those systems. Web pages are an example of information that is routinely deleted and resides on a computer for a very short amount of time. As a result, an IT department cannot be held responsible, under the Safe Harbor clause, for failing to record the content of a website viewed by an employee.

### **RIM Professionals as Safe Harbors**

RIM professionals can offer a safe harbor of sorts, too. This requires that RIM professionals understand the key legal and IT issues and for them to collaborate effectively with staff in those departments to ensure the implementation and management of a solid, documented, and explainable records management program. When a RIM program is in effect and adhered to as it is written – and the organization can show proof of compliance with the program – the organization's attorneys are in a much better position to defend its e-discovery processes and the information it did – or didn't produce. **END**

*Amy Dove can be contacted at [adove@iediscovery.com](mailto:adove@iediscovery.com). See her bio on page 35.*