E-Discovery: Identifying and Mitigating Security Risks during Litigation

Faith M. Heikkila, *Pivot Group*

When producing electronically stored information (ESI) in response to lawsuits, businesses face several security risks as well as legal requirements they must satisfy. Customized document management programs and e-discovery policies are key tools in protecting against inadvertent disclosure as well as meeting business and legal needs.

The amendments to the US Federal Rules of Civil Procedure (FRCP; www.uscourts.gov/rules/EDiscovery_w_Notes.pdf) that went into effect in 2006 place a substantial burden on nonlegal personnel to figure out how to implement legal holds for electronically stored information (ESI). The FRCP rules require that organizations respond to lawsuits by producing any relevant electronic information stored on any media—in some cases, they must do so in the ESI's native format. Legal holds must thus halt all deletions and revisions to responsive documents to be produced in federal lawsuits in the US. European Union countries typically don't comply with the US FRCP rules, but foreign companies that transact business in the US are required to comply with the FRCP rules when involved in US federal lawsuits, even while being careful to abide by the privacy laws within their own countries.

Because documents related to lawsuits can be found on anything from hard drives to PDAs to CDs to smart phones and could be stored as electronic communications or even MP3s on many disparate devices,[1] businesses run increased risk of failing to provide the required documents in response to litigation. This can lead to monetary judgments against them or sanctions from the court.

Many companies will be involved in lawsuits at some point involving ESI production.[2] Yet, recent studies show that most organizations are unprepared to respond to e-discovery requests for ESI.[3] (E-discovery is the process in which opposing parties in a lawsuit exchange documents

1520-9202/08/$25.00 © 2008 IEEE

that provide evidence to prove their cases.) An effective information security program defines how a company safely conducts its daily business, but it should also include how to approach legal holds and ESI preservation. Organizations' e-discovery policies and document-management programs must also account for ESI security during transit, while in the possession of third parties such as attorneys and application service providers (ASPs). Information systems managers and IT departments are integral to all such endeavors.[4]

Security Risks in Producing ESI

Organizations face definite risks when producing business trade secrets or personally identifiable information (PII) in response to document-production requests for relevant ESI during lawsuits. The lingering question is how to protect this sensitive information.

One of the first security issues is how to protect against inadvertent disclosure to outside parties who don't need to know what's in the files. When a lawsuit deals with the core business processes that separate a business from its competitors, protecting this information while it's out of the company's control is crucial.

When turning over ESI to any third party, including your own attorney, consider the following questions:

- How do we know that we can trust you with our confidential information?
- Who will load and maintain the data?
- Have all employees had security training and passed security clearance background checks?
- When was your last vulnerability assessment and network-penetration test?
- What procedures do you follow to stop, contain, recover from, and investigate security incidents?
- Do you have remediation specialists lined up ahead of time?
- What disposal methods do you use after the legal case is over?

A protective court order should also spell out who can access the data and how it should be handled during a litigation case. Once the case ends, an independent security firm should complete a risk assessment of the third party's system to validate the data's safe destruction, including all copies of the data as well as residual information on any hard drives involved.

Inadvertent Disclosure

Given the voluminous nature of ESI responses to document-production requests, attorneys often place the gathered data on Web portals controlled by their law firms or by ASPs. Hackers penetrating this Web access or curious ASP employees can thus create extremely costly security breaches. If the information contains PII, the monetary consequences can be quite substantial because of the need to notify all individuals whose sensitive data was exposed.

> **The lingering question is how to protect this sensitive information.**

To protect a company's sensitive ESI and ensure that only authorized users gain access to the Web portal during a lawsuit, the information recipient must implement firewalls (to protect the gateways, routers, and end points), intrusion detection systems, intrusion prevention systems, encryption, and appropriate access controls.

Confidentiality, integrity, and availability are core information security concepts in all organizations. The information must remain unchanged and safe from accidental or intentional disclosure to unauthorized users. Moreover, it should be available whenever authorized users need it to do their jobs.

In addition, think of the potential impact on the companies in litigation. Their reputations are already at stake, and exposure can cost them dearly. Corrupted or disclosed data could lead to lost client trust, not to mention the potential productivity losses that could result if employees are unable to access the information they need.

Document Productions

During the initial phase of e-discovery (known as the *meet and confer*[1]), attorneys need to know the locations of their clients' responsive ESI—the documents relevant to the current lawsuit—as well as the economic impact for their clients of having to produce documents that are inaccessible. The court forces a proactive review of ESI production to determine up front whether the

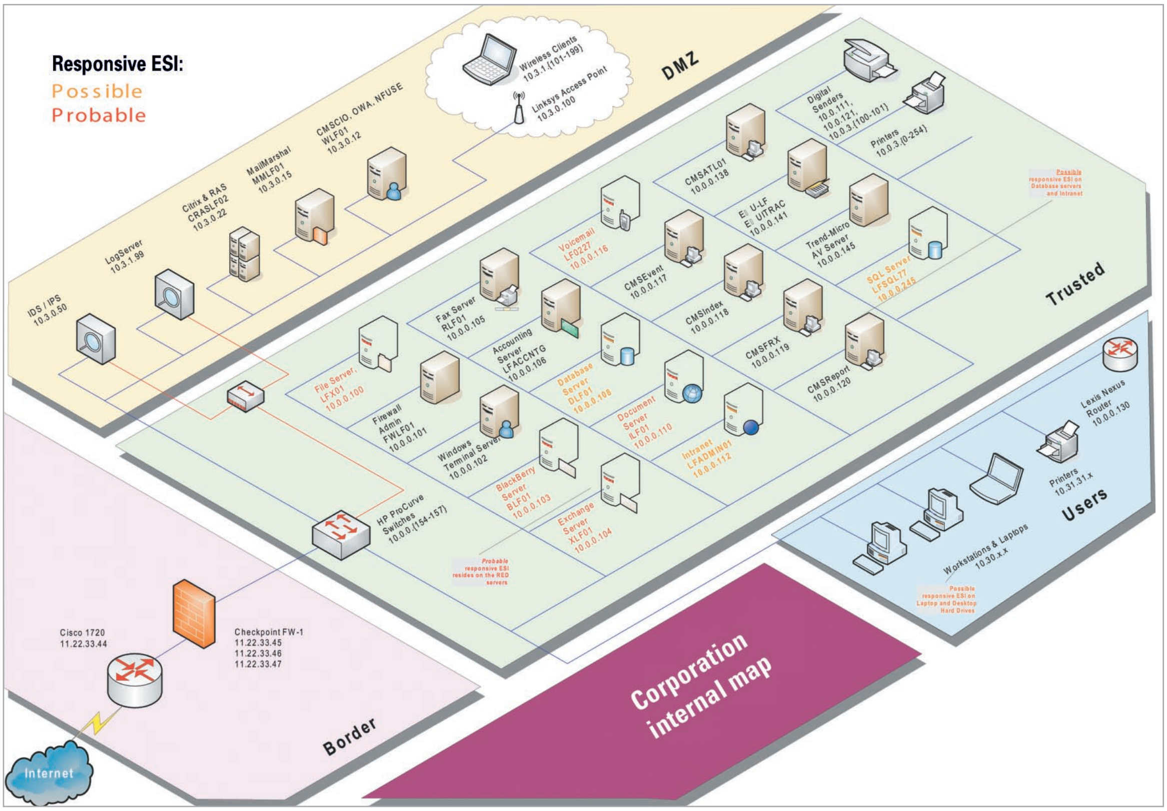
Responsive ESI:
Possible
Probable
Wireless Clients 10.3.1.{101-199}
Linksys Access Point 10.3.0.100
DMZ
CMSCIO, OWA, NFUSE WLF01 10.3.0.12
MailMarshal MMLF01 10.3.0.15
Citrix & RAS CRASLF02 10.3.0.22
LogServer 10.3.1.99
IDS / IPS 10.3.0.50
Digital Senders 10.0.111, 10.0.121, 10.0.3.{100-101}
Printers 10.0.3.{0-254}
CMSATL01 10.0.0.138
E U-LF E UITRAC 10.0.0.141
Trend-Micro AV Server 10.0.0.145
Possible responsive ESI on Database servers and Intranet
Voicemail LF0227 10.0.0.116
CMSEvent 10.0.0.117
SQL Server LFSQL77 10.0.0.245
Trusted
Fax Server RLF01 10.0.0.105
Accounting Server LFACCNTG 10.0.0.106
CMSIndex 10.0.0.118
CMSFRX 10.0.0.119
CMSReport 10.0.0.120
File Server, LFX01 10.0.0.100
Firewall Admin FWLF01 10.0.0.101
Windows Terminal Server 10.0.0.102
Database Server DLF01 10.0.0.108
Document Server ILF01 10.0.0.110
Intranet LFADMIN01 10.0.0.112
BlackBerry Server BLF01 10.0.0.103
Exchange Server XLF01 10.0.0.104
HP ProCurve Switches 10.0.0.{154-157}
Probable responsive ESI resides on the RED servers
Lexis Nexus Router 10.0.0.130
Printers 10.31.31.x
Users
Workstations & Laptops 10.30.x.x
Possible responsive ESI on Laptop and Desktop Hard Drives
Cisco 1720 11.22.33.44
Checkpoint FW-1 11.22.33.45 11.22.33.46 11.22.33.47
Border
Corporation internal map
Internet

Figure 1. Network map. Graphically displaying possible or probable locations of ESI provides legal counsel with a visual picture of the network environment, making it easier to explain to the court where ESI is located, as well as any issues with collecting it. With each case, the responsive ESI's location might change. In this example, probable responsive ESI resides on the file, exchange, document, voicemail, and Blackberry servers, whereas responsive ESI might also possibly be located on the database, SQL, and intranet servers, as well as the workstations and laptops. This graphic shows the disparate systems where ESI can reside and gives an overall view of the network to the court.

case merits the expense of retrieving inaccessible files. One way to clearly identify where possible or probable ESI resides is to use a network map, like the one in Figure 1.

In a typical corporation, ESI will be located on multiple enterprise servers (file, voicemail, databases, SQL, and so on). By providing such a snapshot of the network, the company can help the court understand the ESI production's magnitude and complexity. It can also serve as a roadmap for the IT department as it implements the legal hold for each lawsuit—because the facts in each lawsuit are different, the network map ESI locations will change with each case.

During a lawsuit's discovery phase, the company's attorneys and paralegals will assist in searching, identifying, and culling documents, as well as reviewing documents for attorney–client privilege, which they remove from the documents to be produced in court. Prior to production, the attorney's office then numbers the responsive, nonprivileged documents to adequately identify and introduce them into evidence.

Document Management Program

Every company has its own business needs that its document-management policies must meet. Data classification is a difficult process unless designed for users to easily follow on a daily basis. Getting the data custodians' buy-in from the beginning is essential in establishing long-term solutions that will ensure appropriate file storage. Among other productivity benefits, such as the ability to efficiently locate data to respond to customer and organizational needs, as well as knowledge of where sensitive information that needs protection from unauthorized access resides, a good data-classification and document-management program enables companies to locate responsive ESI quickly when a legal hold goes into effect.

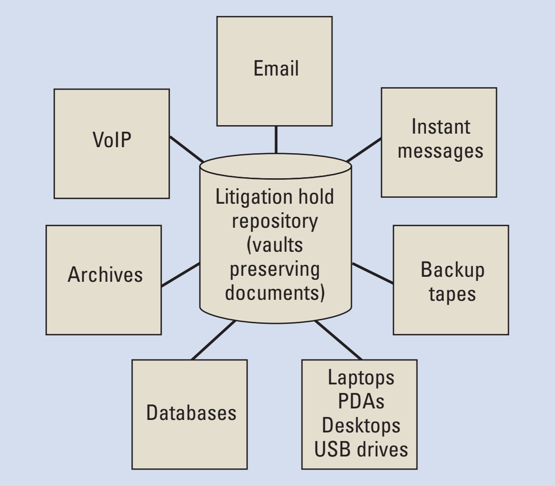
Email
VoIP
Instant messages
Litigation hold repository (vaults preserving documents)
Archives
Backup tapes
Databases
Laptops PDAs Desktops USB drives

Figure 2. Legal hold repository. Vaults for preserving documents remove data from the main network. Establishing such designated legal hold repositories separate from the main network keeps the ESI safe from accidental deletion or alteration. Although the content will change with every case, the example illustrates the forms of ESI that might need preservation in this repository.

A document-management program should

- identify where records reside,
- classify data by category,
- mandate that documents be stored in designated folders on the network (not just on hard drives), and
- inventory computer systems (how many and who has them).

In identifying mission-critical assets that need top protection—patient health information, intellectual property, trade secrets, financial information, and other sensitive or confidential information—companies must categorize and separate documents into appropriate data silos during data classification. All employees must be involved in performing this continuous process.

The level of risk that management will accept with regard to various forms of information is a primary component of this process. Public exposure of PII is a high risk that must be minimized. For example, management might decide as part of the document-management program to allow PII on laptops only if encrypted—or perhaps not allow it under any circumstances.

Accurately classifying and storing data in correct locations is vital for confidently responding to legal holds. The cost of locating improperly filed responsive ESI can be substantial in terms of person hours as well as attorneys' fees—particularly if the ESI is stored in multiple places.

Legal Holds

When anticipating that it might face litigation—a former employee seems likely to file a wrongful-termination lawsuit, for example—a company should immediately put a legal hold into effect[1] halting all deletions and revisions to responsive documents.[5] Typically, the lawyer involved will provide a written definition of documents and data to be preserved once a lawsuit is filed. At that point, the company must suspend all deletions or possible overwriting of any responsive data until the case is over.[6]

A designated person should regularly verify that the legal hold is being enforced. If a hold is in place, any attempts at *spoliation*—destroying evidence, whether electronic or hard copy—can lead the court to impose sanctions or monetary judgments against the offending party.[7]

E-Discovery Plan

As I mentioned, a proactive e-discovery plan begins with a good document-management program. Given that a designated data-classification system takes time to build, it's crucial to involve the business units and data custodians throughout the process. For documents classified as sensitive or confidential, companies should employ appropriate storage and access control from cradle to grave.

Designing data vaults with folders named according to category, case, project, product, custodian, and client makes it easier to locate all relevant documents in one general area, such as a specific drive or server. Companies can even establish designated servers as legal hold repositories or vaults to preserve documents gleaned from various ESI sources, as Figure 2 illustrates. Ideally, a forensics expert should store the ESI in the vault, under the company attorney's direction, by creating a mirror image of the data to save its metadata.

To effectively respond to a legal hold, businesses should create e-discovery policies in advance, outlining the exact steps that each business unit should take, including IT, human resources, and the security and compliance departments.[8] Every company's circumstances are unique, and no sin-

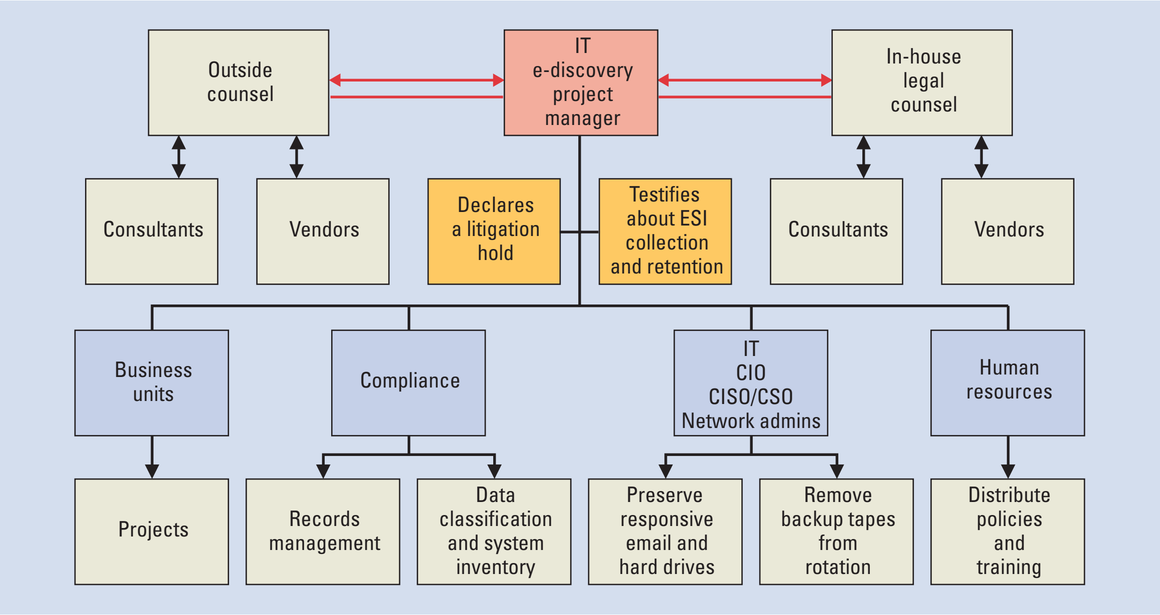
Outside counsel
IT e-discovery project manager
In-house legal counsel
Consultants
Vendors
Declares a litigation hold
Testifies about ESI collection and retention
Consultants
Vendors
Business units
Compliance
IT CIO CISO/CSO Network admins
Human resources
Projects
Records management
Data classification and system inventory
Preserve responsive email and hard drives
Remove backup tapes from rotation
Distribute policies and training

Figure 3. E-discovery response team's responsibilities. Under the legal counsel's direction, the IT e-discovery project manager leads the legal hold effort by communicating with the various departments. Consultants and vendors assist with collection and preservation efforts. IT plays a critical role by preserving the responsive electronically stored information (ESI) and halting ESI deletions and alterations.

gle solution exists. That said, the following steps should help assist with the development of any e-discovery policy.

Designate a Lead Person

The *e-discovery project manager* needs to fully understand the document-management program and e-discovery requirements, as well as the IT and regulatory-compliance issues. This person declares the legal hold upon request of the company attorney or outside counsel and should be able to testify about how the legal hold process was enforced and how the document management program works. This lead person should also be able to explain the difficulty of retrieving inaccessible ESI as well as what makes it inaccessible.

Develop an E-Discovery Response Team

The *e-discovery response team* is similar to an incident response management team in that a designated person declares the legal hold and designated staff controls the ESI, and investigates where it resides in response to document-production requests. The e-discovery team is responsible both for stopping the deletion of responsive ESI and protecting the confidentiality, integrity, and availability of ESI against inadvertent disclosure during the lawsuit.

The team should include members from a diverse range of business units or departments, tailored to the company's specific needs. Each member of the response team must know what to do if the project manager declares a legal hold so that they can immediately begin preserving the responsive ESI.

Train All Employees

Not every business unit or department will be host to responsive ESI when a legal hold is declared, but all employees must know their individual responsibilities in advance in case they are affected by one. Figure 3 shows an example of employee responsibilities. The individual employees in each department must understand the procedures necessary to effectively implement a legal hold. The human resources department provides the training and distributes the policies to all employees. The IT department has a critical role in preserving the ESI, and the compliance and business units assist with identifying where responsive ESI might be stored. Ensuring that each individual is trained to perform their role in executing a legal hold is critical.

Having a clear document management program and data-classification system in place is a key step in ensuring that employees understand their responsibilities. Otherwise, the business must undertake more costly reviews to identify which business units are affected by a legal hold—a process made more challenging because it must be completed quickly by the e-discovery project manager and the data custodians as soon as a lawsuit is anticipated.

Preserve Responsive ESI

Once a legal hold takes effect, the IT department must take backup media out of rotation (tapes, drives, and so on) and preserve responsive emails.[6] The company's attorney must be prepared to contact in-house forensic experts to preserve attorney–client privilege and the work-product doctrine, which keeps any work performed at the request of legal counsel safe from disclosure to the opposing party.

The forensic experts must document the custody chain and indicate all who were in contact with any hardware removed from the place of business. These experts should make forensic images of hard drives, collect relevant data, and document all actions taken with this ESI. When third-party forensic experts examine and preserve ESI, the company should have IT department representatives present to control access and ensure the documents' confidentiality and preservation against accidental deletion or corruption in any manner.

Due to the volume of ESI generated daily, information systems managers, IT departments, corporate counsel, and compliance officers are greatly concerned with how to handle legal holds. Information security departments are also concerned with the security of data no longer in their control. Numerous seminars, webinars, and Web sites discuss e-discovery and how to get your arms around the topic. At the Sedona Conference, top e-discovery lawyers, consultants, academics, and jurists confer.[6] The Web site has many well-written articles and whitepapers with insight into how to deal with e-discovery issues (www.thesedonaconference.org). To learn about e-discovery, read as much as you can on the topic. Then, work with your legal counsel to create an e-discovery response team to prepare an e-discovery plan, policy, and procedures that meet the business requirements of your company.

Establishing a good document-management program makes it easier to identify and handle security breach issues. Creating an e-discovery response team will also assist in responding to security breach incidents. The same type of developmental processes used to create an e-discovery plan can be utilized as a framework for responding to security breaches. IT

References

1. J.M. Redgrave et al., "The Sedona Principles: Second Edition—Best Practices Recommendations & Principles for Addressing Electronic Document Production," white paper, *The Sedona Conf.,* 2007, pp.1–104; www.thesedonaconference.org/content/miscFiles/TSC_PRINCP_2nd_ed_607.pdf.
2. L. Volonino, J.C. Sipior, and B.T. Ward, "Managing the Lifecycle of Electronically Stored Information," *Information Systems Management*, vol. 24, no. 3, 2007, pp. 231–238.
3. N. Swartz, "Firms Unprepared for E-Discovery," *Information Management J.*, vol. 41, no. 6, 2007, p. 6.
4. R. Herold, "E-Discovery Quagmires," *Computer Security Inst. Alert*, Feb. 2007, pp. 10–15.
5. J. Isaza, "E-Discovery Compels: A Seat for RIM at the Counsel Table," *Information Management J.*, vol. 41, no. 1, 2007, pp. 46–49.
6. T.Y. Allman et al., "The Sedona Conference Commentary on Email Management: Guidelines for the Selection of Retention Policy," *The Sedona Conf. J.*, vol. 8, Fall 2007, pp. 239–250.
7. J.J. Isaza, "Determining the Scope of Legal Holds: Waypoints for Navigating the Road Ahead," *Information Management J.*, vol. 42, no. 2, 2008, pp. 34–40.
8. M.E. O'Neill, K.D. Behre, and A.W. Nergaard, "New E-Discovery Rules: How Companies Should Prepare," *Intellectual Property & Technology Law J.*, vol. 19, no. 2, 2007, pp. 13–16.

Faith M. Heikkila *is Pivot Group's regional security services manager for the Great Lakes region. She has more than 18 years of paralegal and IT project management experience. Currently a PhD candidate in information systems specializing in information assurance at Nova Southeastern University, her research interests include e-discovery, secure remote access, information security policies and procedures, and privacy issues. Contact her at fheikkila@pivotgroup.net.*