



## E-DISCOVERY RULES REACH BEYOND LITIGATION

As environment, health, and safety (EH&S) professionals, you most likely are part of a lean staff, have more work than you need, and have strict budget constraints. You have the bandwidth to focus only on the most pressing issues. You must be able to find information when you need it, and trust that the information is good (i.e., current, with a verified chain of custody) to make sound business decisions. If your organization is involved in a civil lawsuit or regulatory action, then information issues move to center stage.

New U.S. federal rules regarding electronic document discovery (i.e., e-discovery) in civil lawsuits have caught some organizations unprepared. The new rules affect how organizations manage and track all sorts of electronic documents, whether or not they face civil litigation or regulatory actions. E-discovery can cause a big headache for those who lacked electronic information policies and procedures when the rules became effective on December 1, 2006. According to a 2006 American Management Association/ePolicy Institute survey, 66% of companies lack policies for saving, purging, and managing e-mail communications (D. Gage and K.S. Nash, E-Mail Retention: The High Cost of Digging Up Data, *Baseline Magazine*, August 2, 2006).

### E-DISCOVERY REQUIREMENTS

E-discovery refers to finding and producing documents stored in electronic form in response to litigation or regulatory requirements. Managing this information is a critical part of an organization's governance, risk, and compliance strategy, requiring alignment across all business lines.

New statutes added to the Federal Rules of Civil Procedure make e-discovery a standard part of federal legal proceedings (see [www.uscourts.gov/rules/EDiscovery\\_w\\_Notes.pdf](http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf)). Key provisions are:

- An electronic document is just about any type of information stored electronically.
- Organizations must maintain a detailed inventory of data assets, systems, retention policies, and backup strategies.
- Organizations must demonstrate that they have policies and consistent enforcement for chain of custody, controlled access, search, and retrieval.
- A 120-day e-discovery timeline starts when a lawsuit is filed. Parties must hold a conference to discuss the handling of archived data. After attorneys present their information needs, a business must disclose what information is available, where it is stored, how the files can be accessed, and why any relevant data may be missing.
- A "safe harbor" provision limits e-discovery to what is reasonably accessible. All parties to the litigation must reach a consensus on information that is not reasonably accessible.
- E-mails may be covered by Attorney-Client privilege.

A company must now recognize, declare, and produce e-documents when involved in civil litigation.

### IMPACTS AND ISSUES

The new e-discovery rules cover almost everything electronic. Companies must examine how they manage all sorts of information throughout the organization, whether structured (e.g., individual and shared databases) or unstructured (e.g., e-mails, instant messages, letters, reports, memos, spreadsheets, slide presentations, Web content, phone messages). Before the e-discovery rules, the courts were more likely to accept excuses such as computer problems, lost data, or incompetence for failing to produce e-documents. Now, the courts are more likely to assess stiffer penalties for failing to produce information.

The rules do not address records retention—that is, which documents must be kept, and for how long. Internal policies and external regulatory requirements help to define



Jill Barson Gilbert, QEP, is president of Lexicon Systems, LLC. She helps organizations increase business value by designing and implementing EH&S management solutions that leverage technology. E-mail: [JBGilbert@Lexicon-Systems.com](mailto:JBGilbert@Lexicon-Systems.com).

how we keep EH&S records, but an EH&S records retention policy alone is not sufficient. Faced with litigation or a regulatory action, companies might be required to produce all sorts of operations and financial records as well.

E-mails and instant messages, the convergence of cell phones and computers, and the availability of cheap flash drives let us easily capture information as never before. Thus, it is essential to have a complete IT inventory—which types of information are stored in which systems, how and when each system is backed up, and where backups are stored.

E-mails are perhaps the greatest risk during e-discovery. Backup tapes containing deleted e-mails can be restored, but restoration is expensive, since the tapes are not indexed and e-mail threads can be extensive. Historical information stored on old technology requires the proper hardware for retrieval.

### E-DISCOVERY MARKET GROWTH

Hundreds of e-discovery vendors exist today. One analyst estimated the e-discovery market to be US\$1.6 billion in 2006, and expected it to double in 2007 (New Rules Make Firms Track E-mails, IMs, MSNBC.com, December 1, 2006). IT analyst firm Gartner estimates the e-discovery market at US\$2.7 billion in 2007, with 30% growth each year through 2010 (John Edwards, Follow the E-mail Trail, CFO.com, January 10, 2007). And IT analyst firm Forrester says that the e-discovery market will exceed US\$4.8 billion by 2011 (Debra D'Agostino, What E-Mail Can You Delete?, *CIO Insight*, May 8, 2007).

There is a bright side to all this, however. The e-discovery rules

- provide a consistent framework for e-discovery, eliminating the guesswork regarding how to respond to electronic information requests;
- recognize the inadvertent alteration or loss of data during routine IT operations, making it more difficult for judges to levy fines for failing to produce information;
- require a good faith effort, but do not require organizations to have “perfect” systems; and
- can help organizations to manage risks and to reduce or avoid e-discovery costs.

### BEST PRACTICES FOR MANAGING DATA

E-discovery is not a standalone issue. While the new statutes apply only to U.S. civil procedures, they impact just about every bit of information throughout the enterprise. Thus, even if you work outside of the United States, or do not anticipate lawsuits or regulatory actions, it makes sense to learn, and follow, best practices for managing electronic information.

### FIVE TIPS FOR E-MAIL RETENTION

1. Catalog your company's data and know which backups are stored where.
2. Suspend deletion programs as soon as you anticipate a lawsuit or regulatory action.
3. Be aware that your lawyer (and the judge in your case) may still be learning about how to identify and preserve electronic evidence.
4. If sued or audited, keep the IT group (or anyone else) from touching data on servers and PCs.
5. Assemble an e-discovery response team.

(Source: *Baseline Magazine*, August 2, 2006)

Get senior management support and establish a multidisciplinary team. Include IT, business, subject matter experts, lawyers, as well as content and document management specialists. Planning is the key. If you have not begun to implement data archiving and management policies, then start with an assessment. Address any immediate legal risks while moving toward a comprehensive system. Ensure that your e-discovery policies and methodologies align with your organization's overall governance, risk, and compliance strategy.

Implement organization-wide information retention and destruction policies. Take the opportunity to optimize your information, disposing of outdated or duplicative items. Enforce these policies consistently. Once you anticipate litigation, be careful to halt information deletion and make full data backups. Do not be tempted to keep everything—this will come back to bite you. If required to produce documents to litigants or regulatory agencies, you must examine each document for relevance and admissibility. This would require an army of experts and lawyers to review the information, at great expense.

Communicate your e-discovery initiative throughout the organization and train people at all levels, making sure that communication and training has relevance to a person's job. Develop a flexible e-information infrastructure that will grow with your organization. As always, if you do not have the resources in-house, seek the assistance of professionals.

New types of evidence exist today that never existed in the past, and managing data for litigation costs millions of dollars. Many companies seek outside assistance to develop and implement an e-discovery process, and the number is growing. They look to lawyers and content management consultants who specialize in e-discovery, and look to information technology vendors to provide flexible, scalable systems that incorporate best practices. **em**