



From: www.cio.com

How to Comply With E-Discovery Rules Before You're Hit With a Lawsuit

– Judi Hasson, CIO

October 30, 2007

No one wants to be sued, that's for sure. But in today's litigious world, it is rare that any company can escape a lawsuit in its business life. It is becoming the CIO's job to make sure, when the time comes, that IT is ready for the onslaught of directives to turn over all electronic documents in a legal case. And that's where the headaches start for any IT department that does not have a good e-mail retention and retrieval system.

MORE ON CIO.COM

[Introduction to E-mail Management](#)
[E-mail and Regulatory Compliance](#)

The need for better electronic record keeping evolved nearly a year ago, when the federal government overhauled its rules of civil procedure and made electronic documents an official part of the discovery process during a lawsuit. The rules for what is called "e-discovery" that took effect Dec. 1, 2006, make production of electronic documents as important as turning over hard copies of material in any legal case. Companies typically have 30 days to answer any e-discovery request (though the court may grant extensions) and face thousands of dollars in fines—not to mention risk forfeiting the case—if they fail to respond promptly.

In this new world that marries the legal system with technology, the CIO is adding company archivist to his job description. IT departments must work with the legal department to come up with a plan that saves necessary e-mails and makes them easily retrievable. Yet there are few rules for setting up an electronic records management system, training employees to catalog their e-mail and creating a standard procedure so employees consistently follow the procedures to turn over electronic documents quickly. And so, many CIOs are still scrambling to organize their corporate e-mail and keep track of these records in a comprehensive way.

The key to compliance with e-discovery rules, say legal experts and IT leaders who have already tackled the problem, is to establish enterprisewide document management and retention practices for e-mail and other types of digital documents, then deploy the appropriate software to support them. "You can achieve a lot of protection, reduce your risk and reduce the cost of discovery by adopting reasonable, repeatable and scalable processes and tools," says John Rosenthal, a partner and co-chair of the e-discovery committee at Howrey, a Washington, D.C., law firm.

Here are ways to get ready for the inevitable:

1. Get in sync with legal and business leaders.

"The problem with e-discovery is the first time it hits your radar screen is when the general counsel calls and tells you what the court wants," says Paul Zazzera, a consultant and former CIO at *Time*. To mitigate such surprises, IT and legal should work to develop processes, policies and tools for saving e-mail that everyone in the company follows. "A CIO and the legal department should be fused at the hip," Zazzera says.

And don't leave business leaders out of the discussion. "Too many CIOs think of litigation as something that belongs to the legal department," says Leslie Wharton, who heads the e-discovery team at the Arnold and Porter law firm. "Litigation is something that belongs to the company, and whether the company is a plaintiff or defendant, the company [as a whole] must be able to meet document preservation and production obligations."

Such preparation makes you "discovery ready," according to Mark Reichenbach, the former director of discovery and regulatory response with [Merrill Lynch](#) (now vice president, client and industry development with vendor MetaLincs), rather than needing to react to litigation or regulatory investigations when they come up. Some companies have even begun to appoint cross-functional e-discovery teams to address the issue, adds Zazzera, run either by IT or the general counsel's office.

2. Get rid of unneeded documents.

For example, if the statute of limitations has passed in a tax case or environmental issue, delete the associated records. Many companies keep data from legacy systems that are obsolete, so there's no business reason—and unlikely any legal reason—to have them around, observes Julie Brickell, associate general counsel at Altria Corporate Services, which handles tobacco litigation for affiliate Philip Morris USA.

Defining what you should preserve is murky, however, and depends on what kind of business you're in. Most important, says Zazzera, is to have a consistent policy for what is permissible to delete—and what is not. Have the same rules for e-mail as for other electronic documents.

"You really have to think through a policy about everything," Zazzera says. "What records you are keeping and how you are keeping them." Most companies will say that all electronic and paper documents generated by company employees on company property can become part of the e-discovery record. But there are gray areas. For example, if a person sends a personal e-mail using a company computer, should that be turned over in e-discovery? And if a person sends e-mail from his own computer about company business, can it be protected?

3. Know where the e-mails are.

Have a map showing the location of every e-mail you keep, and how to retrieve it. Make sure the IT department and business units know where to find the material.

Howrey centralized all its e-mail servers in one data center in Ashburn, Va., including e-mail from its office in Taiwan, according to CIO Brian Conlon. Data from its offices in Europe is consolidated in London. By storing all e-mail in just a few places, it's easier to comply quickly with discovery orders. The law firm also plans to apply technology to help it catalog paper files. In the next year, Conlon plans to deploy radio frequency identification (RFID) to find paper documents, which could make it much easier to search for hard copies of documents.

In addition, make e-discovery compliance part of your due diligence if you are thinking about buying a company. Look at the e-mail storage plan of any potential acquisition to make sure you will be able to produce all electronic data without a glitch if there is a lawsuit down the line.

4. Train your staff—and end users.

Make sure everyone in the company knows what materials to keep and what to discard. "It is reasonable for a corporation to rely on employees to save documents that might be in litigation," says Howrey's Rosenthal.

If you have a personal e-mail policy in your office, make sure employees know what kind of messages should never be sent from an office computer. It may be OK to talk about your dog or what's for dinner. But a disparaging remark about a person or another company may come back to haunt you.

All e-mail, both personal and corporate, creates a potential litigation risk, says Patrick Oot, [Verizon's](#) director of electronic discovery. "Employees should realize the lack of privacy in e-mail. If executives imagine their e-mails blown up on a highway billboard, that's exactly how it looks at trial," Oot says. He offers a general rule: "Never put anything in an e-mail you wouldn't want your mother to read."

5. Invest in the right document search and retrieval technology for your company.

Get used to the idea that supporting e-discovery is a necessary expense. You'll pay a premium if you wait until a lawsuit hits before you prepare to comply.

There are e-discovery tools designed to meet the needs of any company, from startups to large multinationals. How much you spend has a lot to do with how much litigation you usually face. You also have a choice whether to outsource instead of deploying the technology yourself. But a basic system includes search and retrieval software as well as archiving capabilities, says Zazzera.

E-Discovery Tools

There's a burgeoning supply of e-discovery products and services. Here are a few examples.

[Attenex](#) provides tools for law firms to standardize e-discovery procedures.

Zantaz, a subsidiary of [Autonomy](#), supports discovery and review processes without requiring a reviewer to code or tag documents.

[Digital Mountain](#) provides tools for collecting, processing and analyzing electronic data for law firms.

Encase is a suite of products by [Guidance Software](#) to search and retrieve electronic data. It can find data across a network from a centralized location.

[First Advantage](#) provides litigation support services including e-discovery and data recovery services.

[Stratify](#) products include the Stratify Legal Discovery Service, which provides a search tool that can handle 300 documents an hour.

The cost of these tools varies depending on size and sophistication of the system. Rosenthal says it may cost \$1 million to \$2.5 million for a company to prepare for e-discovery, depending on the tools it needs. Zazzera says a large company with 10,000 employees might spend \$500,000 for "entry-level" e-discovery tools that include basic e-mail retention and retrieval capabilities. "When you reach beyond e-mail, the number can quickly grow beyond \$1 million," he adds.

A small firm might spend its money more wisely implementing better document management processes instead of technology. Because small companies don't face many lawsuits, e-discovery experts say it's more important for them to ensure they save records in a consistent and reliable way.

The bottom line, according to e-discovery experts, is that waiting until the last minute to deploy technology—when the e-discovery order comes—can be more costly than planning ahead. "We are all trying to feel our way," Zazzera says. His final piece of advice: "Collect stuff for a long period of time efficiently so it doesn't cost you a fortune. Discovery is expensive."

[Judi Hasson](#) is a freelance technology writer.

© 2010 CXO Media Inc.