

# SAVE IT!

## Rethinking retention policies

*Robert Eisenberg, an attorney, is East Coast director of litigation support services for Gresham, Ore.-based New Technologies Inc. He can be reached at reisenberg@forensics-intl.com.*

By Robert Eisenberg

SPECIAL TO THE NATIONAL LAW JOURNAL

IN THE ENRON imbroglio, auditors at Arthur Andersen's Houston office may be paying a dreadful price for committing transgressions in the realm of document retention and risk mismanagement.

Andersen advised the Department of Justice that a poorly designed document retention plan created the false impression among employees that they were permitted, even encouraged, to destroy relevant documents, although litigation was anticipated. What Andersen did not emphasize, of necessity, was the belief among Andersen's people that as long as they abided by the retention protocols set forth by senior management, they would be protected from repercussions. Regrettably, the belief that a mandated procedure was nothing short of an 11th commandment-and that close adherence would protect the shredder of paper and scrubber of hard drive-was misplaced.

Corporate document-retention policies that favor robotic obliteration over preservation have been fostered by a flawed principle commonly accepted by attorneys and information-management specialists who craft policies. This is the concept that a document-retention policy that is truly protective must mandate the destruction of various types of electronic data upon a fixed timetable. It is the common belief that document retention must emphasize document destruction.

To be responsible-and to operate within the law-both counsel and client must re-evaluate this notion and focus on what electronic documents to retain, rather than what to destroy. There are good reasons for this approach:

- Retention protocols established upon a psychological and procedural foundation of destruction, if not extremely well designed, could lead a court or jury to decide that there has been an attempt to bury data rather than to control and organize it rationally.
- A retention policy focused on destruction is much more likely to lead to the elimination of data that may have been exculpatory or, at least, supportive of the company in the defense of a claim. The targeting of contemporaneous evidence by the typical destruction-oriented retention protocols may do much more harm than good.
- A retention policy built upon the shifting sands of a self-preservation protocol encourages employees to be much less prone to examine the causes of a multiplicity of potential "smoking guns."

### The reasonableness factor

Most importantly, it is the direction of the case law on spoliation of evidence and the reasonableness of retention policies that requires a change in attitude. Some case law emphasizes the reasonableness of a retention policy. The courts' definitions of "reasonableness" span the spectrum from courts that see a duty to preserve electronic data relevant to pending or probable litigation, to courts that add a requirement to preserve evidence for litigation that is reasonably foreseeable. When courts base a retention policy's validity on whether there is "bad faith" at its core-and whether management acted in a "haphazard or uncoordinated manner" in designing protocols-it is time to implement a policy that emphasizes saving important information over trashing the dicey data.

Certainly, there are additional costs associated with the collection and organization of data. These costs, however, can be controlled through the use of forensic search tools that permit data-mining and categorization of e-mails and associated attachments as well as standard electronic files. A vendor of computer forensics and electronic data-discovery services can help a firm establish a document risk-management system grounded upon notions of preservation, not elimination.

There are a number of computer forensic principles that could be applied to document retention initiatives. For example, an e-mail filtering program could be customized to search both messages and attachments and save copies of any that contained keywords or phrases deemed sensitive. This would safeguard the organization from relying on endusers to save these messages, and would guarantee that all e-mails are retained in a universal format in a single location. It would also save money and storage space by not archiving every message that passes through the company's servers. By indexing these messages and attachments, an organization will greatly streamline future data requests-and save significant dollars in the process.

Individual files, such as word processing documents and spreadsheets, raise several retention policy questions: Does the organization have a policy that allows documents to be created and saved on a local machine? If so, is it possible to set up workstations so that duplicate files are saved on the servers? But what happens with files created on laptops being used on the road? Synchronization software could be used to update the files on the server the next time the laptop logs onto the network. Once the files are on the network, forensic search tools could be deployed to identify key files that would fall under the retention policy. They could then be copied and archived according to the procedures established in the policy.

### **Planning ahead**

Every large organization must be prepared to meet the three major challenges posed by every demand for discovery data: the duties of preservation, retention and production. An organization that has determined to be thoroughly proactive in its attitude will take the following measures:

- Long before the demand for production is served, the firm should have developed comprehensive document retention and risk-management protocols containing rigorous enforcement mechanisms, which encompass electronic files, e-mails and attachments, as well as paper. The firm also should have regulated both individual personnel in their document-retention behavior and the IT department in the backup of electronic data and rotation of storage media.

- A joint company/outside counsel/ computer forensics provider "electronic discovery rapid response team" should be assembled. The team should include inhouse counsel, a representative of the IT department, the company's own litigation support specialist (if there is one), an attorney experienced in electronic discovery matters, the law firm's lit support specialist and a vendor experienced in both computer forensics and the processing of electronic evidence for production.

- An IT employee of the firm-and member of the rapid response team should be selected and prepared to be the designated witness for a Federal Rule of Civil Procedure 30(b)(6) deposition taken for the purpose of gaining knowledge of a party's computer network and data-storage methodology. This individual should be well-schooled in the retention protocols and capable, together with other members of the firm's response team, of participating in conferences under Fed. R. Civ. P. 26 and 16 in order to stipulate to a plan for discovery. Such conferences should be sought both to make a showing of reasonableness to the court and to avoid a broad demand that may, for whatever reason, successfully defeat the discoverability restrictions found in Rule 26(b)(2). This rule both controls evidentiary fishing expeditions on the part of the demanding party and requires the respondent to have discoverable data easily and cost-effectively accessible or to face potentially crippling sanctions for spoliation of evidence.

- All storage media containing potentially discoverable data should be secured immediately upon demand-including hard drives of PCs and laptops-and steps taken to preserve the electronic evidence to avoid claims of spoliation. A generalized preservation plan should be documented. This process should be carried out in a way that does not place the company's day-to-day business in limbo. The targeted company should be ready with its own forensic experts for the imaging and examination of storage media. In paper productions, the opposing side is not entitled to rummage through a file cabinet containing nonrelevant documents as well as discoverable ones; likewise, the opposing side is not entitled to have its own experts search, at will, through the data on a hard drive in an attempt to extract specific files, whether active or residual.

- Most importantly, all the targeted firm's Personnel with a need to know should be kept in the information loop, especially IT people. Clearly stated written document-retention protocols, e-mail risk-management procedures and an explanation of spoliation of evidence must be distributed to all affected employees, with updates and modifications meticulously distributed as well. Employees should be aware that penalties range from the imposition of an adverse inference against the respondent to an action grounded in the tort of spoliation.

Demonstrating to the court the existence of a reasonable, well thought out, comprehensively distributed and carefully adhered to and monitored retention program with penalties for noncompliance rigorously enforced is critical in limiting a firm's exposure to a dangerous and expensive e-discovery demand. Such a proactive retention program will also prevent a potentially ruinous claim of spoliation of evidence, either in civil litigation or a criminal prosecution, and -pr2tgt- the,organization's, outside counsel from claims of negligent representation or even malpractice. **NLJ**