Legal Times
WEEK OF JANUARY 28, 2008 • VOL. XXXI, NO. 4
ALM

The First Steps in a Legal Crisis

If employees are deleting inboxes, you may have problems.

BY JEANE A. THOMAS AND JAMES L. MICHALOWICZ

The first few hours and days after the eruption of a legal crisis such as a major lawsuit, government investigation, or product recall are often the most critical for in-house counsel. In addition to the mad scramble to research facts, understand legal issues, retain outside counsel, manage publicity, and address management concerns, counsel must also ensure the preservation of key documents throughout the organization.

The consequences from improper destruction of documents can be severe, ranging from fines and sanctions to, in extreme cases, default judgment. Since the duty to preserve evidence is triggered as soon as the company learns of a reasonably credible threat of a claim, it is critical to have a process in place to implement legal holds before the crisis hits.

IN-HOUSE COUNSEL

There are many examples of companies getting into trouble by mishandling document preservation, particularly when it comes to implementing legal holds for electronically stored information (ESI).

A major challenge for counsel is to be both fortuneteller (determining that the duty to preserve has been triggered) and public address announcer (getting the word out to relevant personnel that preservation must begin). Time is of the essence once the duty to preserve has been triggered, particularly with respect to ESI.

During this critical period, an employee may be innocently cleaning up his inbox, or an IT staffer may be overwriting a hard drive used by a former employee. Moreover, in the ordinary course of routine business operations, e-mails are subject to automatic deletion, backup tapes are recycled, dynamic databases are overwritten, and other electronic information is destroyed in accordance with information management policies and protocol. When the duty to preserve is triggered, a company must have a plan for interrupting or suspending those routine processes and activities as needed to preserve relevant information.

PRIORITIES

The critical task is to quickly preserve the most obviously relevant information throughout the organization. In most companies, two types of personnel control evidentiary material: employees who create, receive, and maintain documents in the ordinary course of performing their job functions, whom we refer to as "custodians;" and information technology staff and others who manage data for the company, whom we refer to as "supercustodians."

For both groups, the objective is to deliver an effective hold notification as quickly as possible.

CUSTODIANS

It is important to remember that, unlike lawyers and IT staff, typical custodians may not be familiar with or comfortable with the legal hold process. They may be concerned about their involvement in the events at issue or what may be revealed in their documents. They may need guidance on how to preserve electronic information.

Without specific instruction, some might move relevant material to folders on their hard drives; others might move it to shared drives, while others might copy it to a flash drive or send it by e-mail to legal counsel (all of which potentially create spoliation issues). With that in mind, we suggest the following day-one approach to preservation with regard to custodians:

1. Identify the core group of people likely to have relevant information. Don't fret if you later learn that others should be included; it is more important to get the notice out quickly and add others as you learn more about your case.

2. Consider whether there is a risk of spoliation by notifying employees of the fact that there is a potential claim or investigation. For an unscrupulous employee, a notice to preserve may have the exact opposite effect, or it may be the case that the company just doesn't want to take chances and would prefer to preserve certain information without the knowledge of certain employees. In these situations, there are forensic tools that can be employed to collect the data without the employee's knowledge or consent. Often this is done in the first few hours after companies learn of an incident, and once information is collected, the general hold notice can be issued.

3. Prepare and distribute a legal hold notice that defines the subject matter of documents to be preserved and includes specific instructions on how custodians should preserve them. If a case likely will have a very broad scope of relevant information, or if it is just too early to define what is relevant, it may make sense to ask custodians to preserve all of their documents until further notice. Follow-up hold notices can be more specific and targeted.

4. Counsel should meet with key custodians, those who may not be familiar with the process, and those whom counsel considers a "compliance risk," to make sure they understand their obligations and are able to comply. It is not enough to issue a hold notice and cross your fingers. You must make sure it has been received and understood.

Supercustodians

Again, supercustodians are managers of large masses of data, such as e-mail systems, servers, databases and backup systems. The day-one priority is to work with supercustodians to identify electronic information that could be destroyed, lost, or overwritten in the course of normal system operations. Potential sources of relevant information to consider include (but are not limited to):

- **E-mail systems.** These may be automatically deleted based on age.
- **Databases.** Some types of databases are dynamic and automatically purge data at a certain age or allow manual overwriting on a regular basis.
- **Backup tapes.** Typically, they are recycled and overwritten on a regular schedule.
- **Enterprise content or document management systems.** These may be purging data automatically.
- **Collaborative work spaces.** They may require an "electronic snapshot" to capture data at a point in time.
- **Voice mail and audio recordings.** These, for example, could be calls with customers that may be routinely recorded or backed up on media that is recycled.
- **Video.** This could be electronic information recorded from security cameras and may have a defined life cycle.
- **Anything else.** Think broadly, and include PDAs, instant messages, temporal data—any and all ESI that is potentially relevant and could be lost or changed.

If there is an established legal hold protocol, supercustodians should be able to take the required steps to preserve vulnerable information if they are given clear instructions on what to preserve. However, in many (if not all) cases it helps for counsel to sit down with them on day one and discuss their approach, which may include taking electronic snapshots, pulling backup tapes out of rotation, turning off auto-delete functions, or other steps.

Also for Day One

Remember former employees. Most companies have a standard protocol for dealing with ESI for employees who leave the company, which is often handled by the human resources department in conjunction with IT. Consider whether there are former employees who may have relevant information and notify human resources, IT, or other involved personnel as to the files, e-mail, hard drives, and other ESI relating to those employees that should be preserved.

In addition, in certain cases, it may be helpful to retain an e-discovery consultant to assist in identifying relevant information on IT systems that is subject to preservation, and overseeing the technical steps taken to preserve (and collect) that information. Consultants also may act as technology experts in later discussions with opposing counsel and may testify as to the steps taken to properly preserve ESI. They can be particularly valuable in high-profile or high-risk cases where spoliation may become a contentious issue or if a company is addressing preservation obligations with certain types of ESI for the first time.

Many companies, especially those that are frequent parties to litigation or investigations, have found it very helpful to have a "preservation response team" including representatives from legal, IT, and human resources, that can swing into action to implement legal hold orders in a very efficient and consistent manner. At minimum, a policy and set of protocols about how to implement legal holds is necessary to ensure that roles and responsibilities are clearly defined and preservation is executed in a comprehensive and consistent manner—especially during a crisis.

Jeane A. Thomas is a D.C. partner in Crowell & Moring's antitrust group and co-chair of the firm's e-discovery practice. She can be contacted at jthomas@crowell.com. James L. Michalowicz is a director with ACT Litigation Services. He can be contacted at jmichalowicz@actlit.com.