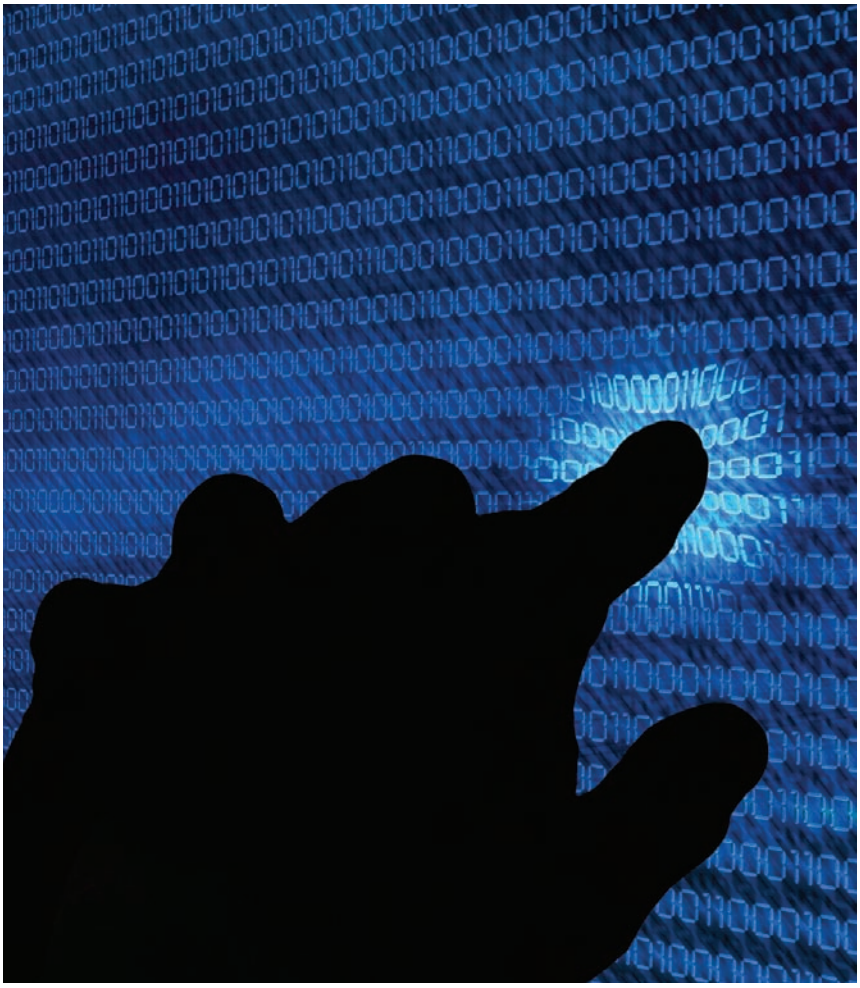
E-Discovery Process and Electronically Stored Information (ESI) Strategies

Preparation Is Key to Lower Litigation Exposure and Expenses

By Duke G. Smaroff



When it comes to lawsuits and managing litigation, most accountants prefer to leave the details to the lawyers. In today's environment, however, that mindset is no longer an option. With high-profile audit failures and Ponzi schemes making front page news, accounting firms are increasingly called upon to divulge information about clients or find themselves a target of lawsuits or other court-imposed sanctions.

One of the significant impacts of litigation has been the rapidly increasing rules of procedure and evidence related to producing electronically stored information (ESI) on a complete and timely basis. E-discovery is the process of identifying, preserving, collecting, processing, reviewing, analyzing, producing, and presenting ESI that may be relevant to a case. Though e-discovery may seem far removed from the core practice of accounting, it is something that accounting professionals should be aware of. In litigation, failure to produce all the necessary information can, and often does, result in significant fines, loss of credibility with the courts, and adverse judgments.

In a 2005 case, *Coleman Holdings Inc. v. Morgan Stanley Inc.*, financier Ronald Perelman won a nearly $1.6 billion judgment against Morgan Stanley after a Florida circuit court judge sanctioned Morgan Stanley and its law firm for not properly responding to e-discovery requests. The firm drew the ire of the judge when, despite its representations otherwise, it repeatedly found and produced ESI in backup files, laptops, and e-mails. In one instance, it found more than 1,000 tapes in an office closet in Brooklyn, even after certifying it had turned over all potentially relevant data to Perelman's side. Consequently, the judge actually reversed the burden of proof, instructing the jury to infer that Morgan Stanley's inability to properly produce electronic documents demonstrated fraud. While the court's decision was later reversed on appeal (*Morgan Stanley & Co. Inc. v. Coleman Holdings Inc.*, Fla. App. Lexis 4167, Fla. Ct. App., 4th Dist., Mar. 21, 2007), this landmark case caught the attention of many experts and cost the financial services firm markedly higher legal fees and years of negative publicity. This case demonstrated that it doesn't matter if a firm is malicious, negligent, or just unorganized—being ill-prepared for e-discovery requests has real consequences.

Ideally, accounting firms will prepare for potential litigation by involving their management, attorneys, IT and computer forensics experts in the early development of an effective strategy for managing ESI. Too often, strategy and discovery is abdicated to IT staff alone; however, the stakes are high and the task too great to follow this model. The cost of preparing for one substantial lawsuit can ruin a small com-

pany. By adopting a proactive approach to ESI and the e-discovery process, accounting firms can be in a better position to reduce both costs and the risk of a negative outcome.

Risky Devices

The explosion of electronic data is the primary catalyst changing the way discovery is managed. In the past, discovery involved boxes of paper files that lawyers would examine for information relevant to the lawsuit. Now that most information is electronic, it is easier to store and harder to eliminate. The amount of data that even a small accounting firm produces is staggering, and it is constantly increasing. Electronic data may exist in multiple formats and locations for every participant on the engagement, including client, auditors, reviewers, and administrative personnel.

As currently implemented, most ESI strategies focus on laptop and desktop computers. What they fail to appreciate is the potential significance of other types of digital evidence that can be gained from thumb drives, external hard drives, scanners, copiers, GPS devices, iPads, iPods, and cell phones. According to Mark Lanterman, chief technology officer of Computer Forensic Services, some of the most risky modern-day devices are copiers and cell phones.

Copiers contain a hard drive that can contain sensitive client data. Lanterman's team, when working an e-discovery case, processed the hard drive out of the copier and found a digital copy of every document that it had ever scanned.

Cell phones are also commonly used for business transactions to review e-mails, change documents, send text messages, and even transfer data as a portable storage device. Although the increasing trend of allowing professionals easier access to data can bring efficiencies and flexibility to a workplace, these devices are discoverable and need to be managed as part of an ESI strategy.

Designing an Effective and Proactive ESI Strategy

While each accounting firm will have its own infrastructure and technology, any good ESI strategy includes several standard steps:

Step 1: Implement an effective document retention/destruction plan. Developing, implementing, and monitoring document retention and destruction policies are the most effective tools in reducing risk when the discovery of an accounting firm's documents is sought. Most accounting firms have a policy in place, but if these policies are not properly executed and monitored or, as in the Morgan Stanley case, if compliance is inconsistent, e-discovery becomes much more complicated.

A good document retention plan must consider regulatory and statutory requirements, case law, industry best practices, and the firm's culture and technology. The plan cannot exist only on paper—it must be implemented. Everyone needs to be trained to understand the importance of compliance and the processes it entails.

Remember, an attorney should be consulted before rolling out a new or updated document retention/destruction plan, especially if a lawsuit is pending or suspected. In fact, any actions taken while litigation is threatened or in-progress could be interpreted as spoliation under the guise of policy.

Step 2: Know where information is. In order to find information during discovery, one needs to know where it might be stored. Create a process map of each type of engagement, as well as the firm's network topology, identifying the appropriate creation, collection, transmission, processing, storage, backup, and destruction points. The process map should also identify which types of data users create or receive and the devices used for any work-related purposes, including home computers, personal e-mail accounts, and cell phones. The backup and retention schedules for each device should also be documented. Such a data map will typically reveal who may have touched which data, and it can be the single most important document with respect to compliance with document preservation requirements.

Step 3: Initiate an effective litigation hold process. An effective litigation hold process is critical. When a company learns that a lawsuit has been filed, or is likely to be filed, any data that may be relevant to the matter must be preserved, and destruction policies with respect to these data must be immediately suspended. Potential data custodians must be identified, notified in writing, and have the hold process clearly explained to them.

The hold process and the collection and preservation of discoverable information are critical and fraught with complications. Documents must be produced in an unaltered, native state, including metadata as well as actual contents. Today's courts have little patience with inadvertent spoliation of evidence.

Step 4: Designate and prepare a rule 30(b)(6) witness. Under the Federal Rules of Civil Procedure, companies involved in lawsuits need to designate an entity spokesperson to testify about the matters involved in the lawsuit. This so-called rule 30(b)(6) witness must be able to testify on behalf of the organization with respect to "information known or reasonably available" to the organization, including how the firm's ESI systems and processes work.

The witness should be knowledgeable about a company's policies and procedures, in theory and in practice, and prepared to offer testimony during a legal procedure. Incidentally, a senior IT person may not be the most suited to answer questions under a lawyer's grilling. A designated partner may represent a better choice, as long as she has the requisite knowledge long before litigation processes accelerate.

Step 5: Periodically audit and refresh the policy. After policies have been created, they cannot simply be filed away and ignored. Processes need to be monitored to ensure they are properly implemented, and education needs to be ongoing. In addition, all policies must be reviewed and updated periodically.

Be Prepared, Not Surprised

In today's litigious environment, almost every accounting firm will need to manage an e-discovery process at some point. In litigation, as in life, the right strategy is to hope for the best and prepare for the worst. An effective ESI policy, when executed properly, will allow accounting firms to immediately focus on legal strategy, rather than spending time digging through piles of old backup tapes, e-mails, and other data sources to find potentially relevant information. ❑

Duke Smaroff, CPA, *is a managing director with the accounting industry services group at RSM McGladrey Inc. and a partner at McGladrey & Pullen, Bloomington, Minn.*