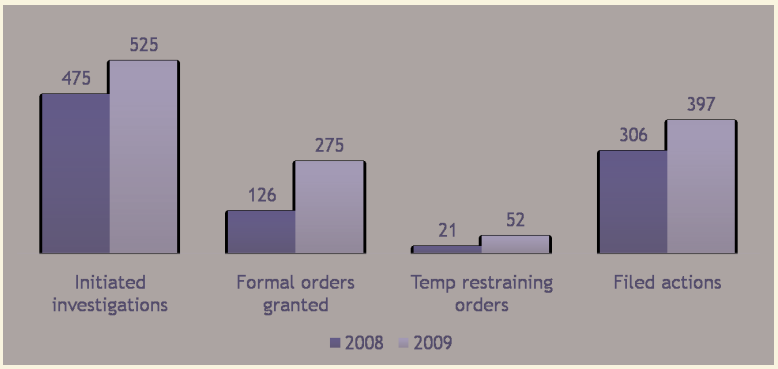
E-DISCOVERY: INSIDE THE INVESTIGATION

Stephanie L. Giammarco, CPA, CITP, CFE, CFF and Lee M. Dewey, CPA, CFE, CFF

Corporate investigations of financial fraud are increasing and e-discovery is a progressively more important component of those investigations. Ballooning amounts of electronically stored information ("ESI") are placing an enormous burden on the office of the general counsel at many organizations (or the audit committee of the board of directors who may also direct investigations). This article discusses how to address that burden with cost-effective ESI solutions, focusing on the differences between e-discovery involved in investigations versus litigation and identifying the skill sets required for cost-effective e-discovery in the context of an investigation.



**SEC Activity from late January 2009 to August 2009.*

Investigations on the Rise

Robert Khuzami, Director of Enforcement at the Securities and Exchange Commission ("SEC"), in a speech on August 5, 2009, told the New York City Bar Association that the SEC opened 10 percent more investigations (January through August) compared with the same time period last year — and filed nearly 30 percent more actions. The SEC is also committed to increasing its support staff to three times the current level, employing new technology to improve its process for managing cases and handling tips, and creating specialized units dedicated to highly complex areas of securities law. In addition, the SEC will flatten its management structure, making frontline staffers accountable in an effort to reduce the chances that fraud and other crimes slip through multiple layers of management.

More organizations are also involved in e-discovery in the context of both litigation and investigations (and those numbers are already high; according to a 2008 research report by the Enterprise Strategy Group ("ESG"), one out of two organizations, regardless of their size, had been through an electronic discovery process within the previous year). The ESG also estimates that corporate information is growing at about 60 percent a year, adding an unfathomable number of terabytes of data in which to locate potentially relevant ESI. This data and document proliferation will place an increasing burden on general counsels ("GCs") to identify potentially relevant ESI. The GCs, who are already under pressure as they deal with day-to-day legal, business and compliance issues, face the challenge of managing the cost of an increasing number of investigations (even as the amount of available ESI grows significantly). In the case of audit committees who direct independent investigations using outside counsel, the cost concerns are not constrained by a legal departmental budget, but are reflected in the board members' fiduciary duty to manage the shareholders' assets prudently.

Investigation vs. Litigation

A GC's initial response to an investigation may be to eschew outside providers and handle an e-discovery investigation in-house, in the hopes of containing costs. This approach may not, however, be the most cost-effective in the long run — especially if the in-house team is familiar with e-discovery only in the context of litigation. E-discovery in the context of an investigation and e-discovery for litigation can vary significantly, both in terms of the volume of ESI involved and the skill set needed to find high-value ESI.

In litigation, an important goal is to be responsive to opposing counsel or to a subpoena — that is, to satisfy legal requirements. This process entails producing documents that are reasonably accessible (and, depending on the requirements placed on the parties, acknowledging the existence of ones that are not). The GC is under no obligation to provide documents that have not been requested or are not reasonably accessible based on undue burden or cost. Litigation is usually directed by the GC who works with outside counsel who is familiar with the organization.

Regular, frequent and structured communication from the very start of an e-discovery project is critical to cost-effectiveness.

Investigative goals — protection from liability, stemming the loss of assets, finding those who are culpable — are different from the goals of litigation. There is an overarching possibility that someone did something wrong, and investigators (or regulators) are looking for that "smoking gun" document, file or e-mail (or the absence of such a document). Such a situation presupposes an investigation conducted at a much deeper level, and investigators may go to great lengths to find ESI that may have been purposely hidden from view.

Much emphasis during an investigation is placed on documenting the *absence* of ESI (i.e., whether ESI has been concealed or destroyed, when and by whom – with a presumption that such destruction implicates the person(s) who engaged in the attempt or actual concealment or destruction of ESI had something to hide). Typically, an investigation proceeds more quickly than a litigation matter; thus, e-discovery must be conducted by experienced professionals who can maintain chain of custody as well as focus on the most fruitful lines of inquiry during the exceptionally fast pace of an investigation. Investigations may be directed by the GC, but are also frequently directed by the audit committee of the board of directors which hires independent outside counsel (who may not be familiar with the internal operations, IT environment and record retention policies of the organization).

Questions typically involved in the e-discovery aspect of an investigation include:

- Have any documents been deleted?
- Have any documents been hidden through password protection or encryption?
- Did a subject of the investigation bypass corporate e-mail and use social networking sites to communicate?

Answering these questions can mean sorting through billions and billions of bits and bytes to find the contents of documents that someone has gone to great trouble to obscure. Hidden ESI can be detected by focusing on financial and business transactions including metrics which would be expected to show activity, but do not due to a potential fraud. Thus, a consulting team comprised of both computer forensics experts and sophisticated investigators with a background in accounting creates greater efficiencies by concentrating quickly on likely areas for ESI that yield fruitful information for investigations. In addition, regulators look favorably upon an organization that hires an independent provider to conduct the e-discovery portion of an investigation.

The Cost-Effective Investigation

The cost of an e-discovery investigation involving outside consultants can be difficult to estimate. An estimate requires knowledge of the ultimate number of custodians and their associated ESI, as well as specifics about the issues at hand — information that is generally uncovered during the course of an investigation.

Communication Is Key

Regular, frequent and structured communication from the very start of an e-discovery project is critical to cost-effectiveness. A project manager should be responsible for clarifying the deliverables and ensuring that all the stakeholders share their pre-existing and developing pools of knowledge. Communication among GC, outside counsel,

outside e-discovery consultants and other investigation professionals can provide multiple cost benefits, including:

- Detection of relationships among potential custodians (investigation targets who have ESI on their laptops, PDAs, voicemail, shared network files, etc.) such that their ESI can be imaged and processed concurrently to reveal important relationships quickly.
- Identification of gaps and unusual findings, which can be shared rapidly in a structured setting to formalize the investigative "hunches" which arise during review of individuals' ESI.
- Collaboration among e-discovery professionals and investigators on initial interviews, which can lead to development of specific lines of questioning based on ESI (or identification by interview subjects of sources of previously unknown ESI).
- Development of reasonable assumptions about costs for subsequent phases as information is shared during initial steps.

A phased approach, with separate estimates for each phase, also gives investigators, e-discovery professionals and the GC or audit committee counsel time to communicate about the course of the investigation and even to rethink the scope and direction of the investigation and refine the approach as necessary, thereby making gains in efficiency.

Scheduled status updates can help maximize efficiency by raising important issues in the beginning stages of the investigation, thereby minimizing less-productive investigative efforts and focusing in on major risks. Finally, frequent, regular communication provides a structure for the project manager to document the work generated during the project so counsel can show, if challenged, that appropriate efforts were undertaken in the investigation, especially as it relates to securing and evaluating ESI.

The Right People

Communication is but one aspect of running a cost-efficient investigation. The volume of data and the number of custodians contribute to a project's size and complexity, and therefore, its ultimate price tag. Does the e-discovery team need to initially process the ESI for all custodians or just the primary ones? Such important decisions create project parameters that are ultimately reflected in the investigation's total cost.

Putting together a seasoned team of cross-trained e-discovery professionals is therefore paramount. When identifying a team of computer forensics and e-discovery experts, GC or audit committees can contain costs by:

- Employing experienced, certified professionals.
- Avoiding providers who deploy large numbers of inexperienced resources.
- Employing cross-trained e-discovery and computer forensics professionals.
- Identifying a provider with references who can attest to a track record of frequent communication among team members as a basis for strong performance.
- Utilizing providers that are aware of the cost of e-discovery and identify cost-savings opportunities.
- Working with providers that have efficient operating structures — and avoiding providers that have made numerous acquisitions and have large overhead costs which are passed along to their clients.
- Obtaining budgets from the e-discovery provider and monitoring those budgets.

An *inefficient* investigation is an *expensive* investigation. A seasoned investigation and e-discovery team can analyze potential custodians and select the ones that make the most sense to pursue first. An experienced team can also drive the direction of the investigation toward the right places — investigative costs can quickly get out of hand if the wrong direction is pursued, and wasted efforts are, unfortunately, a significant component of many e-discovery endeavors.

A seasoned investigation and e-discovery team can analyze potential custodians and select the ones that make the most sense to pursue first.

Similarly, an experienced computer forensics team can uncover high-value data and avoid expending extraneous efforts searching for ultimately useless information. E-discovery professionals who are knowledgeable about financial reporting objectives, relevant accounting standards and internal and external audit processes and objectives can often direct or redirect the e-discovery process to identify relevant documents.

Using the Right Technology Effectively

A cost-effective e-discovery provider will be familiar with the latest technology. For example, with respect to search

technology, current best practices in an investigation include linguistic- and mathematical-based content analysis to reveal patterns that a straightforward keyword search might miss. Concept searching can be a powerful search tool when individuals are trying to hide their activity. Concept clustering tools — employing a statistical analysis of ESI that identifies similar concepts and contexts and aggregates them in a cluster — also reveal hidden activities and relationships.

While keyword searches are valuable, they should be frequently reviewed and revised as an investigation moves forward. Words can have multiple meanings and can, therefore, be ambiguous. To complicate matters further, in instances of fraud, perpetrators have been known to use code words based on everything from baseball metaphors to fine cuisine in order to mask illegal activities.

Efficiency = Cost-Effectiveness

To maximize the value of communication with stakeholders, counsel requires specific, fact-based analyses of complex accounting issues impacting an investigation and their effect on financial reporting and related disclosures. Developing this information on a timely basis can significantly affect the investigative strategy and direction, confirm that the subjects of the investigation are appropriate and enable an effective strategy of responding promptly to regulatory entities. Engagement teams with deep legal, technical, accounting, technology and investigative knowledge — and a healthy dose of professional skepticism — can respond rapidly to the complex issues that arise during the course of an investigation.

The costs of e-discovery can seem elusive because they are driven by the scope of the investigation: Costs can go beyond initial estimates as the number of subjects or the scope of an investigation increases based on initial findings. GC or the audit committee can reduce exposure to unforeseen costs and maximize efficiency by focusing on frequent, structured communications with e-discovery providers and investigators.

Organizations and their counsel who understand the differences in e-discovery for litigation versus investigations are able to select the most experienced e-discovery providers and communicate with stakeholders about costs, timelines and the impact on daily operations. Combining these techniques with an emphasis on best practices in technology leads to the most efficient — and, therefore, the most cost-effective — e-discovery in an investigation. The "e" in e-discovery can stand for "efficient" — and does not have to stand for "expensive."

Stephanie L. Giammarco *is a Partner in the New York office of BDO Consulting. She advises Fortune 500 clients on the e-discovery processes involved in corporate investigations in the United States and internationally. Leading BDO Consulting's Computer Forensics, E-Discovery and Data Analysis practice areas, Stephanie assists companies by collecting, preserving and analyzing evidence in complex financial fraud investigations, as well as by implementing e-discovery tools.*

Lee M. Dewey *is a Partner in the New York office of BDO Consulting. He assists companies with significant corporate investigations and securities litigation and regulatory enforcement matters, focusing on diverse issues involving generally accepted accounting principles, international tax matters and stock option backdating. Lee has been involved in numerous high-profile engagements, and has been asked to present to boards of directors on auditing topics, including SEC and internal investigation matters, perceived corporate misconduct and internal control violations.*

BDO Consulting
A division of BDO Seidman, LLP