

accountingtoday

THE BUSINESS NEWSPAPER FOR THE TAX & ACCOUNTING COMMUNITY

Finding the smoking e-mail

E-discovery is now a critical part of forensics – and of firm policy >> BY LIZ GOLD

Think you have a lot of e-mails? Those who work within the e-discovery process — the handling of electronic information and documents for litigation purposes — most likely have more.

“Many of the smoking guns in a lot of these cases reside in e-mail,” said Catherine Parente, CPA, ABV, CVA and partner-in-charge of the consulting services department at CPA and business advisory firm Carlin, Charron & Rosen LLP. She added that one of the cases she’s currently working on includes four boxes of records, two of which contain printed out e-mails.

“Years ago, you wrote everything in letters,” she said. “You sent out correspondence and you were very formal in your communication. With the advent of e-mail, a lot has become very informal and quite often [involved parties] will say things that will get them into trouble.”

E-discovery is the inclusion of electronic documents in the pretrial process of discovery, where either side can request documents, ask questions in written form, obtain other evidence or depose individuals.

Once electronic information was included in the discovery phase, large corporations, not surprisingly, were reluctant to cooperate. It was perhaps the 2005 watershed case of *UBS Warburg vs. Zubulake* — a discrimination and sexual

harassment suit where Warburg was ordered to pay an employee \$29 million in compensatory damages for destroying relevant and incriminating e-mails during litigation — that brought the process into the spotlight.

As a result, the Supreme Court began to clamp down on corporations. The Federal Rules of Civil Procedure were amended by the high court and went into effect Dec. 1, 2006, with the intent to scrutinize e-discovery procedures.



Catherine Parente



Ken Neumann



Bill Evert

“They’re really not rocket science,” Parente said about the amendments. “They basically just say that one party seeking discovery of this information has to show good cause and have a reasonable need for those records. You can’t just go in and say, ‘I want to see all your e-mails.’ You have to say, ‘There’s really a reason we think we need to see these e-mails,’ and prove it to the court. The party then has to say, ‘Well, here’s the burden you’re putting on me, if you’re asking for that.’ The courts have a little more guidance of what they look at when they make those decisions.”

FORENSICALLY SPEAKING

Most forensic accounting issues involve the review of some electronic documents, according to Joe Bartling, managing director at Daylight Forensic & Advisory LLC, based in Washington, D.C.

“An example is stock-option backdating, which could include e-mails and other electronic documents that might record minutes of board meetings and then accounting for stock options, grant dates and exercise dates, those kinds of things,”

explained Bartling. “The combination of structured and unstructured data — structured being those accounting transactions and unstructured meaning the e-mail and other documents that might be part of the whole stock-option granting process — may need to be reviewed as part of the forensic investigation.”

Although many people consider computer forensics to be synonymous with e-discovery, there’s a significant distinction.

While e-discovery is about the handling of electronic information for litigation, according to Bartling, computer forensics is a scientific process that includes the identification, collection and examination of computer systems in a forensically sound manner. Computer forensics is not standard in civil litigation, but it’s used in investigations when specific electronic information is needed, such as

news

who sent a particular e-mail or who created a particular document at a specific time.

The starting point of e-discovery is securing electronic information, or what is otherwise known as “bag and tag,” according to Ken Neumann, a partner-in-charge of litigation and forensic technology at forensic accounting firm RGL, in Chicago.

“It’s going in and identifying where electronic data is stored, where it’s being maintained, the architecture that has generated it, looking at the electronic internal systems, and then forensically retaining an image of that data in a format that allows someone to provide testimony that the information extracted is in the same format and without being edited,” he said. “It’s the ability to say [the evidence has] not been tampered with.”

The next step — what Neumann calls e-analysis — is studying the electronic images, extracting what is necessary and telling the story in accordance to the forensic assignment.

“There is software now to allow you to take that physical image and, in fact, replicate it on your own computer in the physical e-discovery lab, run that hard drive like it was the original computer and look at it in the same format as the people who were using it,” Neumann said. “It’s really amazing. That’s really telling the story about the electronic trail of what happened with the data. It’s not necessarily analyzing the data itself.”

Once he has an imaged hard drive, Neumann uses litigation support software applications, such as Summation or LexisNexis’ Concordance, for managing electronic data that includes Excel, Word and PDF files. With the system, users can name, track, code, annotate, redact and highlight data — information that Neumann said has already been certified by somebody as being the original. Aside

from all that, these tools also allow for searches for key words or concepts, types of files and dates.

“Data analysis is using electronic tools to evaluate data, prepare statistical analyses, identification of data patterns,” Neumann continued. “Finally, there is the use of electronic media tools for presentation in court settings.”

YOUR INFO OVERLOAD

The average Fortune 500 company manages between 20 and 500 million document pages, with a 57 percent annual growth in information, according to *The Changing e-Discovery Rules & Roles: The Impact on Forensic Accounting*, a report written by Sy Adler, a CPA at Plante & Moran, along with Michael Harnish and Mary Mack, the chief operating officer and the technology counsel, respectively, at Fios Inc., an electronic discovery management services firm in Portland, Ore.

The report also said that 50 percent of all electronically stored information is stored on local devices such as desktops, laptops and mobile gadgets. But the Fios report also identified a number of ESI sources, such as voice mail, instant messaging, iPods, blogs, thumb drives, third-party e-mail such as Hotmail, and your car computer, as places susceptible to search in cases of litigation.

As a CPA, ask yourself this: Is your records-retention policy updated to include electronic information? And would you be prepared should your firm be faced with a lawsuit?

“It’s a scary thing at any type of a company; they can go after everything,” said Bill Evert, national director of business advisory services at Hein & Associates in Denver. Evert added that his firm has started to mandate encryption on laptops to protect sensitive information. “So you’d better make sure you have

good security and that everybody in your company understands that all of this electronic information is discoverable.”

Evert, who consults with companies on how to incorporate electronic data into their records-retention policies, said that he tries to help companies come up with an overarching policy that will essentially kill two birds with one stone: organizing massive amounts of electronic data while considering an increasingly regulated environment.

“We’re helping our clients structure a lot of their electronic data in a certain form or in a certain database so that a company not only has control over it from an e-discovery standpoint, but also from all these other regulations around this electronic data,” Evert said, pointing to industry-specific legislation such as the Health Insurance Portability and Accountability Act of 1996 and Sarbanes-Oxley.

“Another reason to have a written policy as it relates to electronic information is so if you have a key information technology person leave, their knowledge of where that data resides is not walking out the door,” said Matt Wester, a litigation, valuation and bankruptcy consulting services partner at Hein.

For those who don’t have a records-retention policy, Carlin Charron’s Parente has one simple piece of advice: “Get one!”

“Any company should really use, whether it’s electronic or paper, the same document-retention policies they’ve always had,” she said. “In other words, if you’re a company and in the paper days you used to keep records for seven years, when you’re electronic, you should still keep them for seven years. Obviously, you need to revisit those policies as rules change. CPAs have been doing this for years. They’ve had workpapers for years, they’ve had records and correspondence

files. The only difference is in the old days, you were almost forced to have a good record-retention policy because you had space issues.”

Luckily, for those handling potential evidence for clients, when it’s time for a “technical conference” to coordinate e-discovery activities between litigation parties, only an inventory of materials is required, according to Yigal Rechtman, CPA, CFE, CITP and director for information technology, technology assurance and forensic services at Buchbinder Tunick & Co. LLP in New York.

“[It is] kind of a good thing,” Rechtman said, adding that software for cataloging is

expensive, which deters many smaller firms from making the investment. “You’re not required to give the reams of DVDs or CDs to someone. You’re only required to give a catalogue. Cataloging is a lot easier than actually obtaining it.”

Rechtman described purchasing e-discovery software as the next step up from basic document management — and it often requires an additional server.

“It becomes a challenge,” he said. “Most companies have two parallel systems. One would be what we call a file and print server, that’s where you store your file in Word or Excel or Access; the other one will usually be an e-mail system. Then

there may be a third one, which will be for connectivity such as a Citrix or a VPN [virtual private network] server. There is software out there that will essentially go and catalogue everything. But that’s expensive.”

Still, he said that the new amendments have helped to raise awareness about the importance of acknowledging and having guidance around electronic documents. “The rules of evidence were kind of arcane,” he said. “So it wasn’t clear to judges and arbiters on what needs to be done in order to preserve the integrity of the evidence. Now it’s much clearer and people are more educated.” **AT**