Computer Forensics, Electronic Discovery, and the Power of a Single Email

PINKERTON®

The Pinkerton team finds digital information or evidentiary clues throughout a corporation's electronic infrastructure, enabling its clients to seek appropriate enforcement, whether on a civil or criminal basis.

In September 2004, a single e-mail was used to convict a former New York investment banker of obstruction of justice. In the recovered 22-word e-mail, the one-time senior executive instructs underlings to destroy key documents while the bank is under criminal investigation.

The verdict is expected to result in jail time for the former banker. Such can be the power of a single e-mail.

Increasingly, corporations and their counsel face new demands as the world of litigation becomes digitized. More than ever, discovery requests and internal investigations call for electronic documents—such as deleted e-mails—generated in the normal course of business. As a consequence, more and more in-house and outside counsel are seeking out specialized firms to figure out what data is needed and where to get it. To this end, Pinkerton has expanded, building a new, state-of-the-art, secure Electronic Discovery and Computer Forensics Center in Atlanta.

By recovering and filtering data, the lab helps Pinkerton clients investigate fraud and theft of trade secrets within their organizations, monitor illegal insider trading, and comply with discovery requests for electronic data, such as archived and "deleted" e-mails. While the lab has been a key behind-the-scenes player in a number of high-profile cases, it has also helped companies quietly gauge their own vulnerability as potential plaintiffs and set policy on the preservation of e-mails and other digitized documents.

The lab has three independent networks operating more than 60 production servers, both UNIX and Windows environments, where the majority of processing takes place. In addition, there is a separate forensics area where drive imaging and analysis is conducted. These workstations are compliant with the C2 security level as described by the National Security Agency's Orange Book.

"As our world has become more digitized, our corporate clients have been forced to keep pace," said an executive of Pinkerton. "Where the discovery process and internal investigations once called for parties to collect and review box after box of memos and other documents, it now calls for clients to produce—and be able to filter, sort and analyze—gigabytes of computer-generated data."

Many of Pinkerton's corporate and legal clients find this task too daunting to be done in-house. And it can't be done by firms that specialize in general recovery data for industry, since chain-of-custody, admissibility and attorney-client privilege issues make this type of data recovery different from, for example, restoring data from a failed hard drive.

The lab employs a dozen analysts, technicians and litigation support specialists, who specialize in serving the legal and corporate community. "The key," says the executive, "is employing people with experience in the capture, restoration and vetting of digital data and the skills to organize, analyze and effectively produce massive amounts of digital data."

The manager for the Atlanta lab points out that lawyers often know what they want, but their requests need to be translated into technical terms. "A big part of dealing with clients at the early stages of a project," he says, "is helping them understand the scope of work, developing a costeffective strategy and pinning down a protocol and methodology for the project."

"Our experience in having worked on hundreds of cases," said the manager, "enables Pinkerton to provide tremendous expertise in the business and technical issues associated with large-scale electronic discovery projects."

Of late, the lab has been involved in a project for a major bank that has called for the restoration of more than 70 terabytes of information. That equates to more than 2,000 computer hard-drives, or to put it in another context, more than the contents of the Library of Congress (which comes in at a mere 20 terabytes). The project has involved 2,000-plus back-up tapes and over 30,000 man and computer hours.

During the course of a normal year, the lab works on the recovery of electronic data from dozens of clients equating to tens of millions of e-mails and documents. It advises clients on the burdens and costs of producing electronic evidence; production in "native" and alternative formats; recovery of deleted and backed-up digital material; and re-duplication, filtering and conversion of electronic data. Additionally, the forensic

team works on a national basis with our Securitas Security Services group assisting in numerous internal investigations ranging from diversion of corporate assets to tracking the online illegal distribution and resale of products globally. The Pinkerton team finds digital information or evidentiary clues throughout a corporation's electronic infrastructure, enabling its clients to seek appropriate enforcement, whether on a civil or criminal basis. Many of the team are members of the FBI InfraGuard Program, the High Technology Crime Investigation Association (HTCIA) as well as holding CISSP accreditation.

"The technology team is critical in assisting our clients," said a Pinkerton executive. "It provides an important service to our clients in the area of risk management and investigations."

The lab also helps clients develop digital document and e-mail retention policies, and institute effective procedures for the review and analysis of electronic and digital evidence.

"Sometimes, finding one specific document can be like trying to find the proverbial needle in the haystack," said the exeutive. "But if it's there, our team will usually find computer protocols, experience in similar cases and an array of tools and capabilities."

Because of attorney-client privilege and the high level of confidentiality involved in this type of work, the lab's greatest successes may never be known. A "smoking-gun" e-mail that the lab has uncovered for one of its clients may not be fully appreciated until it has worked its way through the legal system or caused a case to settle months or even years after it was uncovered.

Every now and then, however, the lab's staff can see the immediate result of its hard work.

The executive recalls the case of a company that was under investigation, faced with being de-listed from a stock exchange as its share price plummeted. Rumors of wrongdoing swirled around the company. It was believed that a rogue former executive was at the root of the company's problems, which had blindsided the company's CEO. The CEO asked Pinkerton to recover the former executive's e-mails and other documents stored on back-up tape.

Because of the high level of secrecy, the company's own IT department couldn't be involved. Ultimately, the lab was able to provide the CEO with key e-mails and other data that implicated the former executive and deflected much of the negative attention from the company's current management team.

The lab has three independent networks operating more than 60 production servers, both UNIX and Windows environments, where the majority of processing takes place. In addition, there is a separate forensics area where drive imaging and analysis is conducted.

"Having done due diligence on itself," said the Pinkerton executive, "the company's CEO was able to go to authorities and the financial media and say, 'OK, we've done the research and here's what we've found…' Things soon stabilized for the company and its stockholders, and the company was never de-listed."

PINKERTON®

For more information, please visit our website at www.pinkerton.com or contact us
Email: pinkerton.info@pinkerton.com | Phone: +1 800-724-1616