New Accounting Reform Laws Push For Technology-Based Document Retention Practices

John Patzakis
CEO, Guidance

The Sarbanes-Oxley Act of 2002, which President Bush signed into law last year, represents an ambitious effort by Congress to address many data retention and preservation issues arising from the Enron and Arthur Andersen debacles. In addition to creating a new and apparently powerful Public Company Accounting Oversight Board ("Oversight Board") and addressing corporate responsibility issues, the new law also mandates retention of electronic documents, imposes strict criminal penalties for altering or destroying records, including those kept in electronic form, and mandates production of electronic records and other documents when summoned by the new Oversight Board.

In addition to Congress passing Sarbanes-Oxley, several regulatory agencies, including the National Association of Securities Dealers (NASD), have issued new regulations and guidelines that augment existing document retention requirements. Compliance with these new rules and regulations by public companies and their auditors requires the implementation of systematic protocols and procedures for the recovery of computer-based evidence in the course of the innumerable internal audits and investigations that Sarbanes-Oxley will inevitably spawn.

Computer Forensics as a Standard Practice

Computer forensics, which is commonly defined as the collection, analysis and court presentation of computer-based evidence, is a mandatory process whenever the results of a computer investigation may ultimately be presented in a legal or administrative proceeding. If computer evidence, which is highly malleable and volatile in its native environment, is not properly collected and handled, it will not likely be usable in court.[1] While internal investigations involving the examination of computer media for evidence relevant to a network intrusion, intellectual property theft or other insider misconduct are frequent within the information systems security field, companies often mistakenly

assigned IT experts who are unfamiliar with proper computer evidence handling protocols. The resident computer expert may well find the evidence, but will likely trample all over the electronic investigation scene in the process. Further, if the company's IS team or hired consultant who initially responds to a computer incident cannot establish the integrity of computer evidence at issue, law enforcement likely will decline any request for prosecution.[2] For these reasons, employing proper computer forensic tools and procedures is essential.[3]

In addition to preserving and authenticating computer evidence, computer forensics provides a powerful process to efficiently recover and analyze all available information, including temporary data, deleted files, and remnants thereof. Far from a cumbersome process, the latest generation of computer forensics software offers the easiest and most powerful means to rifle through one or more hard drives to quickly identify and document relevant data.

With the vast majority of information in the enterprise now existing in electronic form, computer forensics is no longer just a promising and specialized field, but a standard practice amongst virtually all levels of law enforcement, large auditing firms and Fortune 100 corporate security departments. However, the feasibility of computer forensics practices, no matter how compelling the need, is largely dependent upon the technology utilized to perform the process of data recovery and analysis. Fortunately, new tools, including enterprise solutions that preview, image and analyze computer drives over networks, are now available to answer the daunting but now mandatory requirement of conducting enterprise-wide computer investigations.

Enhanced Criminal Penalties for Records Destruction Require Response Planning

Sarbanes-Oxley imposes severe penalties for the destruction of records, including electronic data. Section 802 of the new law imposes fines up to $25 million and/or imprisonment of up to 20 years against "whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible

object with the intent to impede, obstruct, or influence" any government investigation or official proceeding.

The deletion, of electronic records relevant to an audit, whether intentional or otherwise, is a critical "computer incident" that necessitates a proper and immediate response in the same manner that network intrusions require instantaneous remedial action. In the Arthur Anderson case, the firm failed, with devastating consequences, to convince federal officials and ultimately a jury that the destruction of electronic records was the unauthorized actions of a few rogue employees and managers and not at least tacitly endorsed by upper management. Other organizations should learn from Arthur Anderson's demise by implementing an immediate computer forensic investigation and response mechanism to preserve computer evidence and recover critical deleted information. In addition to creating peace of mind, forensic tools can help immeasurably in both mitigating the permanent loss of data, and establishing that any destruction was the result of authorized misconduct on the part of an individual.

From even a remote location, the latest computer forensics software will efficiently recover deleted information that remains on the computer while preserving the integrity of the data, thus enabling investigators to accurately reconstruct an incident while preserving the evidence. Further, as is the case with other similar regulatory regimes, including the Graham, Leach, Bliley Act that governs financial institutions, having established response procedures as a matter of due diligence to address such computer incidents will often weigh favorably in the eyes of government regulators.

New Records Retention Requirements

Section 103 of Sarbanes-Oxley requires public accounting firms to "prepare, and maintain for a period of not less than 7 years, audit work papers and other information related to an audit report, in sufficient detail to support the conclusions reached in [the audit report]." Section 104 allows the Advisory Board to "require the retention by registered public accounting firms for inspection purposes of records whose retention is not otherwise required," and a new provision added to the U.S. Code imposes a fine

and/or imprisonment of up to 10 years for failure of any accountant who conducts an audit of a publicly traded company to “maintain all audit and review work papers for a period of 5 years from the end of the fiscal period in which the audit or review was concluded.” (Section 802; amending 18 U.S.C. §1520(a)(1)).

In another related regulatory regime, the National Association of Securities Dealers have promulgated Rule of Conduct 3110, which in its official comment to that rule, the NASD requires that "correspondence with public customers, both written and electronic, be maintained in compliance with NASD rules and the SEC Rules 17a-3 and 17a-4." This means that an employee or other representative of any broker-dealer who engages in "e-mail correspondence with the public relating to the firm's business, generated both at the office and at home, is subject to these provisions." This would include Internet chat conversations, instant messaging, and web-based email.

An important feature of computer forensics software is the ability to create non-invasive physical image backups of drives. Physical drive images capture all the available data, including deleted files that have not been overwritten, allowing investigators to recover information if is later determined that a user deleted data. At the same time, a concise chain of custody of the preserved data is maintained for possible future audits and investigations.

Additionally, image backups could help protect individuals and companies from liability under Sarbanes-Oxley or the NASD and SEC rules in the event that deleted records are later believed to be relevant. For instance, many public companies currently image drives with forensic software whenever an employee leaves the company. That way, all evidence existing on the drive is preserved, which is important as oftentimes an employer will not learn of possible trouble until long after the employee has left the company. An employee engaged in misconduct will typically delete computer files and traditional backup techniques do not capture deleted or temporary data. This practice is even more important in light of the document retention provisions of Sarbanes-Oxley and the severe penalties firms face for destroying or failing to retain required information.

Increased Computer Evidence Discovery

Section 105 of Sarbanes-Oxley authorizes the Oversight Board to conduct broad investigations of auditing firms and "associated persons" and authorizes the Board to "require the production of audit work papers and any other document or information in the possession of a registered public accounting firm or any associated person thereof." Section 105 also authorizes the Board to suspend or bar any individual from association with a registered public accounting firm or to suspend or revoke the registration of any public accounting firm for failure to produce requested documents.

With these broad investigative powers conferred to the Oversight Board largely involving the production of documents (and thus electronic records), firms must have comprehensive and efficient mechanisms to conduct enterprise-wide discovery efforts to retrieve computer-based evidence in response to Oversight Board inquiries. The electronic data preservation, response and information discovery requirements posed by Sarbanes-Oxley are part of a prevailing trend where all internal investigations and discovery efforts are focusing almost exclusively on computer evidence. To address this trend, Enterprise Response, Auditing and Discovery (ERAD) solutions have emerged to provide powerful computer forensics capabilities to the enterprise. ERAD solutions enable examiners to forensically analyze and image any workstation or server connected to the same local or wide area network. Computers connected to a network can be searched and analyzed from a single location at the disk level, enabling non-invasive recovery and analysis of all data, including deleted and temporary files normally invisible to the user. Keyword searches and other automated forms of analysis queries are broadcast throughout the network and returned and organized at an examiner's workstation.

ERAD Case Studies

The ERAD process provides a powerful and instantaneous mechanism to respond to and remediate a wide variety of computer incidents, ranging from unauthorized deletion of critical data, network intrusions, and internal theft of intellectual property. In the case of

one Fortune 100 company, a hacker compromised a mission critical server and deleted several files. The company's IT security team employed computer forensics software to respond to the incident, immediately recover and restore the deleted files, identify installed hacker tools, and determine which files the intruder accessed, renamed and modified. Investigators can employ the same technique to recover files deleted by rogue employees on their workstations or to obtain entire physical images of drives for archival or detailed off-line analysis. Most importantly, ERAD technology allows such examination and recovery to take place remotely from any point on a wide area network, providing instantaneous and cost-effective response to critical incidents.

The ERAD technology also enables internal discovery efforts to conduct broad investigations of legal incidents or to probe suspected but undetermined inside threats and policy violations. In a recent ERAD investigation, the CTO of a large Los Angeles-area company suspected that members of his IT staff might be misusing their access privileges to network servers for some unknown purpose, based upon indications of significant amounts of unusual network traffic. An outside consultant performed a confidential, after-hours investigation of the network, examining network logs and the drives of 60 network machines in only a few hours, without bringing any systems down. The ERAD investigation identified unauthorized web servers that contained more than 20 gigabytes of pornographic material, determined which users had access privileges and had logged onto the rogue machines. An unexpected result of the investigation revealed additional rogue servers were placed above ceiling tiles and were communicating with the network via multiple wireless access points as part of an elaborate Internet pornography distribution scheme.

ERAD solutions also enable an organization to audit and enforce compliance with various computer usage policies. For instance, employee usage of web-based email and instant messaging programs present significant concerns for Wall Street firms seeking to comply with NASD rules that mandate retention of all communications with public clients, including those in electronic form. Many firms address the problem by adopting internal policies that strictly prohibit the use of such means of communication. To ensure

compliance, ERAD technology is employed to conduct automated searches across the network to find web-based email, evidence of instant messaging and Internet relay chat programs, encryption programs and hidden partitions. Hundreds of nodes can be quickly and thoroughly analyzed through automated scripts, GREP queries, and keyword searches that cull information from live network servers and workstations.

Mechanism for Implementation of Best Practices

The advent of the ERAD process is clearly a crucial development in the fields of incident response, internal computer investigations, and liability risk auditing, and will better enable compliance with regulatory regimes such as Sarbanes-Oxley. The comprehensive process also promises to promote effective collaboration between corporate IT security teams, IT auditors, and general counsel to develop and implement concise and effective computer security response and investigation policies to achieve these critical compliance objectives.

NOTES

[1] *Gates Rubber Co. v. Bando Chemical Indus., Ltd.*, 167 F.R.D. 90 (D.C. Col., 1996) is a particularly important published court decision in this area, in which the court ruled that when processing evidence for judicial purposes a party has "a duty to utilize the method which would yield the most complete and accurate results."

[2] "Evidence Compromised in Credit Card Theft Case," by Mike Brunker and Bob Sullivan, MSNBC.COM, June 8, 2000, reports on a recent high-profile case where a law enforcement agency declined to pursue an investigation due to a failure to protect the integrity of the electronic evidence in question.

[3] *State v. Cook*, 777 N.E.2d 882, 2002 WL 31045293 (2002 Ohio App.), is an important case where the court validated the computer evidence in question, expressly noting that it was processed with computer forensics software specifically designed for that purpose.

About the Author

As President and Chief Executive Officer, John Patzakis leads Guidance Software's worldwide operations. Combining his legal and technical expertise, Mr. Patzakis joined Guidance Software as general counsel in January 2000 and is recognized as a leading authority on the admissibility and authentication of computer evidence.

Mr. Patzakis received his Juris Doctorate from Santa Clara University School of Law and was admitted to the California State Bar in December 1992. Prior to receiving his law degree, John received a degree in Political Science from the University of Southern California in 1989. He began his legal career in civil litigation at the firm of Cotkin &

Collins, where he served as an associate in the firm's business litigation department before becoming a Founding Partner of the law firm Corey & Patzakis.

Mr. Patzakis lectures frequently and is repeatedly published on computer forensics and electronic evidence issues. He is the author of the EnCase Legal Journal, a widely read publication distributed by Guidance Software that focuses on legal issues relating to computer forensics and electronic evidence. Mr. Patzakis is a member of the High Technology Crime Investigation Association (HTCIA), and the Information Systems Security Association (ISSA).