

# *Retention of Corporate E-Documents under Sarbanes–Oxley*

Edward H. Freeman

**I**n recent years, the press has reported many high-profile corporate frauds, leading in turn to major bankruptcies. Congressional committees have investigated widespread financial misstatements in some of America's most trusted organizations. Employees saw their pension funds and life savings evaporate after unscrupulous executives pocketed the last remaining assets. The fall of Arthur Andersen, Enron, Tyco, Healthsouth, Global Crossing, WorldCom, and others have cost investors and taxpayers billions.

This column deals with one facet of the Sarbanes–Oxley Act of 2002: how it has affected corporate requirements for document retention. Congress enacted Sarbanes-Oxley “in the wake of vast stock market declines and congressional investigations of widespread financial misstatements and other misconduct in American corporations and in American capital markets.”<sup>1</sup> Its stated goal is to “protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws.”<sup>2</sup>

## **DOCUMENT RETENTION POLICIES**

A *document retention policy* is a published set of guidelines that a company establishes to determine how long it should keep corporate records, including e-mail and Web pages.<sup>3</sup> No legislation or court decision has ever required an organization to maintain all of its documents forever.<sup>4</sup> Premature destruction of documents, however, can lead to penalties in both civil and criminal cases. If an organization is unable to produce pertinent documents in court, a judge or jury is likely to assume that the organization has deliberately destroyed the evidence.<sup>5</sup>

Consequences for improper destruction of relevant information can be severe. A court might penalize an organization by assessing attorneys' fees and other costs. Courts also might draw an adverse inference against the party responsible for the destruction, usually on a finding of willfulness, bad faith, or fault. “The perils of wrongful destruction can include an instruction to the jury that it may infer that the documents would have been harmful to the

---

*EDWARD H. FREEMAN, JD, MCT, MCP (edfreeman@hotmail.com) is an educational consultant in West Hartford, Connecticut. He has written over 50 articles on computer technology, privacy, security, and legal issues and has spoken at a number of professional conferences. He is also an adjunct faculty member at Central Connecticut State University in New Britain, Connecticut, and the University of Connecticut and St. Joseph College in West Hartford, Connecticut.*

*Obstruction of Justice is an attempt to interfere with the administration of the courts, the judicial system, or law enforcement officers and is considered a felony in most states.*

party's case."<sup>6</sup> A court might even award a default judgment against an organization if it destroyed relevant evidence in bad faith and the destruction of evidence prejudiced the other party.

### **OBSTRUCTION OF JUSTICE**

*Obstruction of justice* is an attempt to interfere with the administration of the courts, the judicial system, or law enforcement officers and is considered a felony in most states. Such actions can include threatening jurors or witnesses hiding evidence, impairing the efforts of a court trial, as well as interfering with an audit, assaulting a process server, or resisting an extradition agent. President Clinton was accused of obstruction of justice during the 1999 impeachment trial. The charge stated he attempted to "delay, impede, cover up and conceal evidence" in the Paula Jones sexual harassment lawsuit.

In March 2002, the federal government indicted Arthur Andersen, LLP, for obstruction of justice. At the time, Arthur Andersen was one of the Big Five accounting firms. The indictment alleged that Andersen executives continued to shred documents and delete computer files relating to its audit client, Enron, after it was aware that civil litigation and government investigations were imminent and even after Enron had received an informal request for information from the Securities and Exchange Commission (SEC). According to the indictment, Andersen's destruction of Enron documents ceased only after it was served with a subpoena from the SEC. Arthur Andersen claimed, among other responses, that destruction of the Enron information was performed pursuant to Arthur Andersen's document retention policy. On June 15, 2002, a jury convicted Arthur Andersen. On October 16, 2002, Andersen received the maximum possible sentence,<sup>7</sup> leading to the ultimate demise of the firm.<sup>8</sup>

### **SARBANES–OXLEY ACT**

Partially in response to the Arthur Andersen–Enron, Congress passed the Sarbanes–

Oxley Act of 2002. In a White House press release, President George W. Bush described the act as "the most far-reaching reforms of American business practices since the time of Franklin Delano Roosevelt."<sup>9</sup>

The act requires corporate and accounting reform for public companies and the accounting firms that audit them. Senior management and their audit committees must now assume direct responsibility for the financial statements issued by the corporation. The most important provisions of Sarbanes–Oxley include:

- Accelerated reporting of trades by insiders
- Public reporting of CEO and CFO compensation and profits
- Auditor independence and a prohibition on audit firms offering services that might result in a conflict of interest
- A requirement for companies to have an internal audit function, which must be certified by external auditors
- Certification of financial reports by CEOs and CFOs

Section 1519 of Sarbanes–Oxley deals with the destruction or falsification of corporate documents:

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 the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.<sup>10</sup> (Emphasis added)

When a corporation decides to conduct an internal investigation of alleged fraudulent activity by its employees, it must learn the full extent of any wrongdoing, including the collection of relevant documents. Steps should be taken immediately to preserve and protect any relevant documents. While it may not always be feasible, or even possible, for a large business to identify every

individual who might hold pertinent materials, preservation efforts should be broad enough to ensure that all employees who are potentially connected with the fraud preserve their relevant documents.

The need to preserve documents takes on particular significance in light of criminal penalties that the Sarbanes–Oxley Act imposes. The establishment and enforcement of a written document retention policy is essential. Special care also must be taken to secure any electronic material, including e-mails, until the matter is resolved. This may require purchasing appropriate computer hardware to increase a business’s electronic storage capacity. Although costly, preserving electronic material is essential in today’s world. The government is unlikely to sympathize with a company that, while aware of possible fraud, deleted or lost potentially relevant electronic documents.<sup>11</sup>

To date, no court has explored the legal ramifications of Section 1519 of the Sarbanes–Oxley Act.

#### **DATA RETENTION POLICIES**

A carefully designed records-retention program can save an organization money, space, and time. The possibility of litigation is another reason to set up a records-retention program. Computer records must be available if the government requests them or if other parties subpoena records involved in legal claims. If an organization has no schedule of record retention and destruction, the opposing party may allege that the organization destroyed the computer records to avoid producing them in court.

An appropriate policy for the destruction of documents, adopted in good faith pursuant to industry and governmental standards, may provide valid justification for the company’s inability to produce such documents in later litigation. It should not be adopted for preventing damaging documents from becoming available if required in future litigation.

As an example, many e-mails are written for internal use and may contain erroneous information, personal opinions, or offensive remarks. Such documents might prove embarrassing or damaging if they are ever disclosed. The retention of documents that do not need to be retained exposes the company to unnecessary risk.<sup>12</sup> “By using a policy that is consistent in its application rather than selectively applied, a preexisting policy appears to eliminate the specific intent for impeding the administration of justice because the policy is not intended to impede a specific proceeding.”<sup>13</sup>

Before establishing a formal records-retention program, an organization should compile a data inventory. This inventory will identify which records exist, where they are located, and who has access to them. The organization should then establish a records-retention schedule, considering the following factors:

- Industry standards.* If possible, competitors should be contacted to compare retention policies. Industry organizations are often a useful source for standardized document retention policies.
- Governmental requirements.* As an example, the Internal Revenue Service can audit tax records for up to seven years. All tax-related documents should be stored for at least that length of time.
- Foreseeability of legal action.* If an organization is aware that its products might be the basis for product liability litigation, appropriate records should be kept for a reasonable time period.
- Cost and space requirements.*

The courts do not expect that organizations will retain records indefinitely. In particular, an organization need not keep detailed records of daily transactions for an extended time period. However, the courts do expect that appropriate business records and computer data will be available for a reasonable amount of time. The appropriate period for a specific type of organization should be a matter of formal company policy. The courts disapprove of premature

*If an organization has no schedule of record retention and destruction, the opposing party may allege that the organization destroyed the computer records to avoid producing them in court.*

destruction of records, especially when such actions create roadblocks to discovery.

When old data is destroyed, the organization should be careful to record exactly what was destroyed, as well as when and how the removal took place. Such a recording will help rebut charges of impropriety if its decision to destroy old data is challenged in future litigation. Special care should be taken when reusing backup tapes or zip drives, so that old data is not accidentally overwritten by new backups.

### RECOMMENDATIONS

The goal of an organization's document retention policy is to preserve valuable business information in usable, retrievable form. Some documents, such as contracts, real estate transactions, and financial statements, should be retained indefinitely. Other items can be discarded after a year. All retained documents should be filed systematically to allow for easy retrieval. For e-mail retention specifically, a useful motto is "Keep it only while you need it, destroy it when you don't, and don't destroy it if you've been ordered by the court to retain those records."<sup>14</sup>

Organizations should have a clear written policy for document retention. An experienced computer lawyer should be brought in when the document retention policy is created or modified. This policy should be based on industry standards *and* government requirements. All employees dealing with computer records must be aware of the scope of the policy. When a document is legitimately deleted in accordance with corporate policies, all copies should be destroyed. An organized approach to document retention and deletion can save large amounts of money if a request for discovery is presented. A management team should be appointed to monitor compliance with the corporate policy.

If the organization is even remotely aware that a certain electronic document might be the object of a discovery request, that document should not be destroyed under any circumstances. If such documents

are destroyed, the organization is opening up itself to the possibility of sanctions for the spoliation of evidence.

A documentation retention policy need not be a major document. It can contain a few paragraphs or two pages, but should clearly spell out the organization's policies. Appropriate fundamentals should include:

- Clearly defined retention policies and times for paper and electronic records, as well as voice mail and e-mail
- Methods for destruction of records when their retention period has expired (is it automated or are users responsible?); documents should be destroyed as soon as they are eligible for destruction
- Procedures for suspension of the policies when a lawsuit is anticipated or an investigation is underway
- Personnel policies clearly defining who is responsible for enforcing and updating the policy and what penalties will be imposed if the policies are violated

If an electronic document is deleted pursuant to corporate and governmental policy, great care must be taken to ensure that the document has actually been deleted. When a computer file is deleted from a hard drive, the space occupied by the file is not erased, but is made available for overwriting when needed. Overwriting can occur at any time in the future, depending on the size and utilization of the drive. There are software products that will wipe a storage medium clean as soon as the delete command is executed. Such a program should be used whenever documents are deleted.<sup>15</sup>

The science of computer forensics is based on the ability of specially trained personnel to recover electronic documents that were "deleted" or destroyed but are still accessible from a hard drive. Such documents may still be subject to production during discovery. A company must implement a routine destruction schedule that completely erases all copies of the information.<sup>16</sup>

Senior personnel should review and update the document retention policy on a

regular basis. It should be part of the employee handbook. Employees should acknowledge in writing that they have received and understand the policy.<sup>17</sup>

## CONCLUSION

Courts will show no sympathy to an organization if there appears to have been impropriety in the discovery process. If there is even a possibility that electronic data was deliberately destroyed before discovery, courts will impose severe sanctions on the offending party, including severe fines and even forfeiture of the case. Organizations are wise to develop and enforce strict document retention policies and never to destroy documents that may be the subject of future discovery.

The Sarbanes–Oxley Act is a powerful piece of legislation that will significantly alter the manner in which today’s companies do business. All business owners, executives, managers, line supervisors, and human resources professionals should become familiar with the implications of the act regarding document retention. It could save a great deal of money and bad publicity. ■

## Notes

1. Lewis D. Lowenfels and Alan R. Bromberg, Implied Private Actions under Sarbanes-Oxley, 34 *Seton Hall Law Review*, 775 (2004).
2. 18 United States Code, 1503 (2002).
3. Barbara Weil Gall, Document Retention Policies: Legal Reasons to Keep E-Mail, Web Pages and Other Records, [www.gigalaw.com/articles/2000-all/gall-2000-09-all.html](http://www.gigalaw.com/articles/2000-all/gall-2000-09-all.html). (Accessed February 16, 2005.)
4. *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003).
5. Christopher R. Chase, To Shred or Not to Shred: Document Retention Policies and Federal Obstruction of Justice Statutes, 8 *Fordham Journal of Corporate and Financial Law*, 721 (2003).
6. Einar Rowan, Document Management in the Digital Age; When Formulating a Document Retention Plan, Remember that Documents Today Are Not Always on Paper, *Legal Times*, May 17, 2004, p. 18.
7. Document Retention and Destruction Post-Arthur Andersen What Can You Destroy?, [http://www.perkinscoie.com/content/ren/updates/bc/doc\\_retention.htm](http://www.perkinscoie.com/content/ren/updates/bc/doc_retention.htm). (Accessed March 14, 2005.)
8. Jennifer Smith Finnegan, Ten Steps to an Effective Document Retention Program, Product Liability Law and Strategy, *Product Liability Law and Strategy*, December 30, 2004, p. 1.
9. David A. Kotler and Rick Swedloff, Sarbanes–Oxley’s Impact on State Corporate Governance, 13 *Washington Legal Foundation Legal Opinion Letter*, 16, July 25, 2003.
10. 18 United States Code Annotated §1519 (Supp. 2003).
11. Lanny Breuer and Alan Vinegrad, In-House Counsel — Focusing in on Fraud — Seven Steps for Detecting and Preventing Fraud, *New York Law Journal*, October 27, 2003, p. 20.
12. Steven Schoenfeld and Rosean P. Rasalingam, Document Retention Policies Have Long-Term Benefits: Goal is to Ensure Important Information is Kept as Long as Necessary and No Longer, *New York Law Journal*, November 18, 2002, p. 1.
13. John M. Fedders and Lauryn H. Guttenplan, Document Retention and Destruction: Practical, Legal and Ethical Considerations, 56 *Notre Dame Law Review*, 5 (1980).
14. Roberta Fusaro, Cases Highlight Need for E-Mail Policies, *Computerworld*, October 5, 1998, p. 20.
15. Einar Rowan, Document Management in the Digital Age: When Formulating a Document Retention Plan, Remember that Documents Today Are Not Always on Paper, *Legal Times*, May 17, 2004, p. 18.
16. Marilee S. Chan, Paper Piles to Computer Files: A Federal Approach to Electronic Records Retention and Management, 44 *Santa Clara Law Review*, 805 (2004).
17. Sharon D. Nelson and John W. Simek, Law Firm Document Retention Policies: “The Future Ain’t What It Used to Be,” 12 *Nevada Lawyer*, 14 (May 2004).

*Organizations are wise to develop and enforce strict document retention policies and never to destroy documents that might be the subject of future discovery.*

The views presented in this journal are those of the authors and do not necessarily reflect the views of the publisher or of the journal’s board of advisers.

*Information Systems Security* (ISSN 1065-898X) is published bi-monthly by Auerbach Publications, Taylor & Francis Group, 6000 Broken Sound Pkwy NW, Suite 300, Boca Raton, FL 33487. Editorial offices: Auerbach Publications, 270 Madison Avenue, New York, NY 10016. Subscription rates: \$175/year in the U.S., U.S. possessions, and Canada. For prices elsewhere, please inquire. Periodicals postage paid at Boca Raton and other mailing offices. Printed in U.S. Copyright © 2005 Taylor & Francis. All rights, including translation into other languages, reserved by the publisher in the U.S., Great Britain, Mexico, and all countries participating in the International Copyright Convention and Pan American Copyright Convention. Product or corporate names may be trademarks or registered trademarks, and are only used for identification and explanation, without intent to infringe. This journal contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or the consequences of their use. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated in any information retrieval systems without the written permission of the copyright owner. Authorization to photocopy items for internal or personal use, or the personal or internal use of specific clients, may be granted by Taylor & Francis, provided that \$20.00 per article photocopied is paid directly to Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923 USA. The fee code for users of the Transactional Reporting Service is ISSN 1065-898X/05/\$20.00+\$0.00. The fee is subject to change without notice. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged. Postmaster: Send address changes to *Information Systems Security*, 6000 Broken Sound Pkwy NW, Suite 300, Boca Raton, FL 33487.