Chapter 7
Securing Information Systems

LEARNING TRACK 2: THE SARBANES-OXLEY ACT

Reacting to corporate accounting and governance scandals that made headlines in the early days of the twenty-first century, the United States Congress enacted legislation to protect investors from fraudulent corporate accounting and restore public confidence in corporate America. The legislation, known officially as the Public Company Accounting Reform and Investor Protection Act of 2002, acquired the common name of the Sarbanes-Oxley Act (alternatively SOX or Sarbox), so named for the members of Congress who sponsored the bill, Senator Paul Sarbanes (D-MD) and Representative Michael G. Oxley (R-OH).

The scandals in question, including Enron, WorldCom, and Tyco, resulted in bankruptcy and, in some cases, the complete collapse of major public corporations. Hundreds of thousands of shareholders lost millions of dollars due to the unethical actions of a handful of executives and faulty accounting practices. In general, high-ranking company officials allowed earnings to be misstated and investors to be deceived. In less serious cases, companies were forced to restate their earnings to the detriment of shareholders because accounting practices did not provide accurate records of income and expenses.

SOX forces companies to ensure the accuracy of their financial records though internal accounting controls. All internal audits must in turn be certified by an independent external auditor. The importance of an independent external auditor is underscored by the fact that Enron's accountant, Arthur Andersen, also relied on income from Enron for consulting services. This conflict of interest influenced the accounting firm to, at best, tacitly approve inaccurate records. SOX declares that outside auditors may not furnish actuarial, legal, or consulting services to their audit clients. In addition to mandating the independence of auditors, SOX enforces compliance to the following:

- Financial reports must not contain any misrepresentations
- CEOs and CFOs of corporations must review all financial reports and are responsible for their veracity, as well as the internal accounting controls that ensure them
- High-level executives are prohibited from asking for or accepting loans from their companies
- Companies must fully disclose the compensation of the CEO and CFO
- Companies must report insider trades more expeditiously
- Companies must offer protection for whistleblowers
- Companies must disclose material changes in their financial state or operations promptly
- CEOs and CFOs are compelled to report deficiencies in internal accounting controls, fraud related to management of internal accounting controls, and material changes in internal accounting controls

Companies, and executives, that fail to comply with SOX regulations are subject to a variety of penalties, ranging from criminal and civil actions for securities violations to

lengthy jail terms and hefty fines for executives who purposefully misstate financial records. SOX also criminalizes the corrupt alteration, destruction, mutilation, or suppression of documents for the purpose of devaluing them or evading disclosure in official proceedings.

Along with heavy consequences for violations, SOX compliance carries financial burdens for implementing the necessary controls. The cost of installing adequate internal auditing controls and having those controls certified by an outside auditor is on average $4.3 million for companies with revenues of at least $5 billion. Even larger companies may spend $30-$40 million annually on SOX compliance.

While the burden of proof of SOX compliance falls on executives and the auditors they hire, the burden of implementation falls largely on IT departments. SOX does not outline requirements for IT security, in fact the text of the law makes no explicit mention of IT, but the vast majority of internal auditing and reporting controls rely on IT installations. Without the IT department, SOX compliance has virtually no chance of occurring.

The terms of SOX mandate the long-term storage and protection of financial records, as well as the rapid availability of such records in case an oversight agency or subpoena requests them. Interference with the proper retention of records, including destruction, alteration, and falsification, carries harsh criminal penalties mentioned earlier. Records that need to be retained include not only transactions that account for income, expenses, liability, etc., but also communications, such as e-mails and instant messages. Penalties for deleting an e-mail with the intent to hinder a federal investigation may be as severe as a $1,000,000 fine and 20 years in jail. While all e-mails and IMs may not be relevant to compliance, best practices suggest archiving practically all electronic communications, including phone calls.

SOX stipulates that companies and their accountants must retain records of their audits for at least seven years, and that accountants auditing companies that issue securities must retain audit work papers for at least five years, SOX has created the need to store and protect data for longer periods with secure, duplicate backups. Storage repositories must feature an easily navigable index to facilitate the satisfaction of record requests. And companies must be able to record and report any attempts to access, modify, or delete the records they have retained. To comply with these provisions, companies are investing in IT: new storage devices and media, software, and record management controls.

A popular solution for managing record retention is write-once, read-many server technology, commonly known as WORM. WORM technology employs magnetic tape, specially enabled drives, and WORM data cartridges to serve a "backup, duplicate, and archive everything" strategy effectively. This is especially important in an era when even individual employee workstations must be added to the aggregate official record.

WORM media prevent overwriting or deleting data once they have been recorded as a result of the write-once technology. These media are also high-performance and high-capacity solutions at a reasonable cost. Technologists have used magnetic tape reliably to store data for decades. Its traditional strengths, including capacity, cost, transfer rates, durability, and portability, combine with the security of WORM technology to satisfy the SOX-compliance needs of many businesses.

Creating unalterable, long-lasting data records is not the end of the information security process. Full Sox compliance requires that the media and their duplicates be physically secure as well. To prevent loss from damage, best practices indicate storing duplicate copies in different locations. To prevent unauthorized access, these locations must be subject to strict controls so that all interactions with the records are properly documented.

SOX compliance is a complex undertaking. The following guidelines may be helpful to any business that has questions about their strategy for storing and securing

data:

- Do you have the ability to store data and prevent them from being altered for the appointed retention period?
- Is the technology you are using flexible enough to be updated so that access to stored data remains possible years from now?
- Does your current technology permit rapid retrieval of financial records by authorized personnel in the face of an oversight request?
- Is the technology you are using scalable so that it will support increased storage and security demands if your organization grows?
- How well does your SOX-compliance technology solution work with the business process technologies that produce the critical data that are subject to the legislation?

By answering these questions appropriately, executives may find that they have blessed their companies with improved operational processes and new competitive advantages.

Sources: David Breisacher, "S-OX & Storage-The ABCs," Sarbanes-Oxley Compliance Journal, December 6, 2004; Bernie Goulet, "The Best Defense is Being Proactive About Email Retention," Sarbanes-Oxley Compliance Journal, June 1, 2006; "What is the Sarbanes-Oxley Act?" www.allbusiness.com, accessed August 29, 2007; "Sarbanes-Oxley Cheat Sheet," Silicon.com, accessed via CNET News.com, August 29, 2007; "Sarbanes Oxley Summary," www.sarbanes-oxley-101.com, accessed August 29, 2007; Mark Rasch, "Sarbanes Oxley for IT Security?" The Register, May 3, 2005; Randy Brasche, "Sarbanes-Oxley Is an IT Responsibility and Business Opportunity," DM Review, December 2004; Courtney Macavinta, "Save Often," Dell Insight, January 2005.