

Information control with Sarbanes-Oxley: Is your business compliant?

A Sophos white paper

May 2005

SUMMARY

This white paper discusses the role of security and record retention within the context of the Sarbanes-Oxley Act, and the steps businesses must consider to ensure compliance. The sections of the Act relevant to security and record retention are reviewed, followed by company interpretations and their actions related to compliance.

Introduction

The Sarbanes-Oxley (SOX) Act of 2002 is a broad piece of US legislation that covers a range of topics. Developed to protect investors by improving the accuracy and reliability of corporate disclosure, the Act covers Analyst Conflict of Interest, Auditor Independence & Reporting, and Corporate Responsibility, as well as the creation of a Public Company Accounting Oversight Board.

While introduced as law in July 2002, the governing Securities and Exchange Commission (SEC) designed a rolling set of deadlines that continually increase the requirements on those affected, including auditors, executive management, audit committees, legal counsel and financial service firms.

Current status of compliance

The latest deadlines for most public companies are financial reporting and certification mandates for any end-of-year financial statements filed after November 15, 2004. Foreign companies and smaller companies – those with a market capitalization of less than \$75 million – must meet

The Sarbanes-Oxley Forum reported that almost half of US businesses have not created plans or implemented actions to comply with the SOX Act.

September 2004

these requirements for any statement filed after July 15th, 2005. With little time remaining before most publicly traded companies must begin to comply with the SOX Act, confusion reigns.

In September 2004, the Sarbanes-Oxley Forum reported that almost half of all US businesses still had not created plans, let

alone implemented actions, to comply with SOX, as evidenced in the following:

- Greater than 15% have not started.
- Greater than 65% have made no changes.
- Fewer than 5% consider themselves fully compliant.

Why is this?

Firstly, because the legislation covers a range of topics and is substantially broad, a number of actual rules have been issued by the SEC through the mechanism of final rules releases that attempt to clarify earlier language. Secondly, language within the Act demonstrates an allowance for broad interpretations.

For example:

- Executive officers of corporations are responsible for establishing and maintaining internal controls (no definition of internal controls provided).
- Each issuer reporting shall disclose to the public on a rapid and current basis information concerning material changes (no definition of rapid or material).

It is understandable how some issues – particularly security and record retention – can get lost in the confusion. The rest of this paper looks at Sophos's view of these issues within the context of Sarbanes-Oxley, and the steps necessary to achieve compliance.

The role of security and record retention in Sarbanes-Oxley

Two themes concerning information integrity dominate the language and tone of SOX:

The first, internal controls, calls attention to issues around design, operation, audit ability, management assessment and reporting. References to internal controls can be found in three sections. Section 103 pertains to auditors'

responsibilities in evaluating their clients' internal controls. Sections 302 and 404 describe corporations' responsibilities regarding internal controls.

The second, record retention, addresses the rules around retention of documents (including electronic) that are created, sent or received relating to an audit or review.

Internal controls

Evaluate asset protection

As companies review their networks, protecting all assets should be a focus. This has received particular attention based on a Securities and Exchange update specifying the rules

Companies are uncertain how to keep email compliant under Sarbanes-Oxley standards, and are choosing to save everything, putting themselves at increased risk.

around Section 404. The new rules define the term "internal control over financial reporting" to include:

- Company management must provide reasonable assurance regarding the prevention or timely detection of unauthorized acquisition, use or disposition of the registrants' assets that could have a material effect on the financial statements.

As an example, one Sophos customer, an IT manager of a Fortune 500 Company, reviewed his entire network prior to an upcoming internal audit. During the review, the IT manager decided that Section 404 of the Act meant that all file servers in their network that managed financial information, even UNIX servers not particularly susceptible to viruses, needed anti-virus protection.

Specifically, companies are taking another look at their UNIX/Linux servers for two reasons:

- 1 People have pointed to the limited number of viruses written for UNIX/Linux. However, companies must acknowledge that viruses intended to attack these operating systems do exist.
- 2 A UNIX/Linux file server can be a host for a virus, and Windows machines that interact with the box can be infected as they retrieve/store files on the machine.

From Sophos's perspective, as we continue to see greater sophistication in viruses, and as virus writers themselves are learning non-Windows operating systems, it is likely that the number of viruses will increase.

Record retention

Many companies are uncertain how to keep documents, particularly email, compliant under SOX standards. The reality is that companies are choosing to save everything. The issues with that approach include the following:

Security theme	Relevant section of the Sarbanes-Oxley Act
Internal controls	Section 103: Auditors must describe the testing of the control structure and procedures of the company Section 103: Auditors must describe any weakness in the company's internal controls Section 302: Officers are responsible for establishing, designing, evaluating and maintaining internal controls Section 302: Officers must disclose any deficiencies and significant changes Section 404: Annual reports must contain a control report stating the responsibility, assessment, and evaluation of internal controls
Record retention	Section 802: Rules and regulations on record retention

Table 1: Security/Record retention and Sarbanes-Oxley relevant sections

- 1 Keeping all email puts companies at undue risk. As Michele Lange of the National Law Journal writes, “Outdated email, antiquated files and data are often kept past their useful life. Case law reveals that unwieldy preservation of all electronic data can come back to haunt a corporation when litigation ensues”.¹
- 2 Retention is not just about archiving, but also about retrieval. Saving all correspondence leads to obstacles when asked to deliver only relevant documentation.
- 3 The costs of retaining and maintaining this documentation overwhelms the cost of implementing a policy framework to retain documents selectively.

A policy framework is critical – businesses should consider the enhanced policy management included in Sophos's gateway solution.

A policy framework is a critical element of an overall compliance architecture, and businesses should consider a gateway solution that includes enhanced policy management.

Your audit firm determines compliance

Whether it's concern over what an audit committee might view as **“reasonable assurance regarding prevention or timely detection”** or the fact that they simply need to check the box – compliance is a focus area. Many audit firms are not technically savvy and don't have detailed understanding of the implications, which confirms the need for a conservative approach.

Customers should not assume that a discussion with their audit firm around the low potential of corrupted or lost data will be straightforward. Corporate management must understand that the audit firms themselves are subject to as much, if not more, regulation as the companies they serve. New rules produced by the SOX Act will make any audit firm particularly sensitive during the initial rollout of any new rules.

Sophos's support of Sarbanes-Oxley

At Sophos, we understand business because that is our only focus. Incorporated in 1985, Sophos serves over 35 million users from organizations of all sizes in more than 150 countries.

Asset protection

Sophos Anti-Virus is a recognized product leader in the market:

- 1 Sophos Anti-Virus™ has the broadest coverage for the UNIX and Linux operating systems of any of the major vendors.

- 2 Sophos IDE files are the smallest in the industry, resulting in the fastest download and shortest deployment times.
- 3 Linux/UNIX platforms can be centrally and automatically updated using EM Library.

Companies must acknowledge the increasingly important roles of regulation and compliance and the potentially damaging effects of non-compliance.

Record retention

Sophos PureMessage™ provides leading gateway capabilities that address Sarbanes-Oxley:

- 1 By filtering out spam and malicious content, PureMessage policy controls for inbound/outbound email management reduce the volume of email that compliance scanning, archiving and encryption systems handle. This increases efficiency and reduces the resources required.
- 2 PureMessage policy controls can look for common patterns and “watermarks” (combinations of keywords) that suggest a message might require retention.
- 3 PureMessage includes detailed reporting on message flow and policy triggers, providing information that can help you meet internal control documentation requirements.

Summary

All companies must acknowledge that regulation and compliance are playing increasingly important roles in how business is conducted. Non-compliance can have many impacts on a company, some of which could be damaging, including:

- 1 A decrease in the perception of the company and investor confidence. The Sarbanes-Oxley Act is heavily publicized, and after November 15, 2004 there are likely to be negative reports in the media on companies who miss full compliance.
- 2 Penalties are written into the Act and disclosures are made to the Securities and Exchange Commission. For public companies that do not meet compliance by the appropriate time, the Sarbanes Oxley Act provides specific details.

The challenge of Sarbanes-Oxley and other regulations are that they are not easy to understand and the final rules continue to be written. That is one reason why many companies consider

using a software approach rather than an appliance, as this is inherently more flexible. As more companies and their auditors go through compliance, there is likely to be greater consensus. In the interim many companies are taking a conservative approach to ensure that they meet the requirements of the new regulations.

For more information on how Sophos can help with your compliance initiatives, call toll-free on 1-866-866-2802, email nasales@sophos.com or visit www.sophos.com.

Sources

- 1 Sarbanes-Oxley has Major Impact on Electronic Evidence, The National Law Journal (law.com), Michele C S Lange, 01/2003