A PRACTICABLE ANALYSIS OF THE SAXBANES-OXLEY IMPACT ON DOCUMENT RETENTION & MANAGEMENT

Background

Many publicly traded corporations have a strong grasp of the administrative and managerial accounting requirements for SOX compliance reviews. However, even now, after almost 3 years of compliance auditing reviews, most organizations still have not assessed the impact of SOX compliance on document management and retention.

In most information technology departments, documentation management and controls have, historically, been an after thought to the development, testing and maintenance of applications. In fact, with the exception of the public sector, very little attention has been given to this aspect of business maintenance and survival.

This white paper is based on both my research and the contributions of the other members of my SOX FTP Online Resources Group. Specifically related to document retention, the Sarbanes Oxley Act states the following:

- A failure to maintain audit or review of work papers for at least five years is punishable by up to five years in prison, and/or an unspecified fine amount.
- Corruptly altering, destroying, or concealing records or documents in order to compromise the integrity of the record for use in an official proceeding is punishable by up to 20 years in prison, and/or an unspecified fine amount.
- The alteration, destruction, or concealment of any records with the intent of obstructing a federal investigation carries an unspecified fine amount, and/or jail time of up to 10 years.

General legal discovery

Legal discovery rules require any company involved in legal proceedings, regardless of size or industry, to produce evidence contained in electronic communications. The typical process can be exhaustive and expensive.

It's true that paper trails can do a good job of protecting organizations from fraud and error by providing evidence that is acceptable in court. But what happens when interactions and records exist only in electronic format, as is more and more often the case? Many companies, unfamiliar with the concept of treating e-mail messages as business records, have been accustomed to deleting them automatically after a certain time period (usually 90 days or so). Subsequently, if any of these messages are needed as evidence in legal proceedings, these companies are often out of luck.

As regulatory and legal discovery pressures continue to increase, however, the corporate world is learning its lessons. "Most large companies," says Andrew Rathmell, CEO of the Information Assurance Advisory Council, "now recognize that they can be crippled overnight if their reputations are harmed by failure to protect their information assets." That underscores the importance of ensuring that business-critical e-mail messages and their attachments are efficiently captured, classified, archived, retrieved, and also destroyed when they've finally outlived their usefulness.

Building the foundation for e-mail-related regulatory compliance

The requirement: An efficient and affordable compliance solution that preserves maximum evidential weight. While regulations can be very strict about how archived messages should be treated, these rules refer only to relevant messages that have to do with client and partner communications, or contain internal sharing of important information. None of the regulations, so far, has required companies to archive absolutely all messages passing through the system.

At the same time, archiving absolutely all messages is often seen as the easiest and lowest-risk route to compliance. While today this may still be the safest choice, these companies will face the difficult task of managing an enormous volume of messages in two to three years, which not every archiving solution may be able to handle. Given this, it's critical that you select a solution that is ideally suited for corporate-wide e-mail capture and archiving based on key words/phrases, individuals, roles, or other customizable identifier—while maintaining long-term security, efficiency, and economy related to storage requirements.

Beyond backup and more than mail store management

Distinguishing between e-mail backup and e-mail archival is critical if regulatory problems are to be avoided. E-mail backup systems are designed to provide wholesale recovery of the e-mail server, should a disaster befall the production environment. These systems are not designed for compliance or legal discovery-related record retention.

Simple e-mail system backups have no provision for the review of individual e-mail records. Backup processes format the data to reduce storage space and speed future recovery processing. This formatting works against attempts to review and retrieve individual messages.

A true e-mail archiving and retention system ensures, at a minimum, that companies have ready access to any given e-mail record, whenever it is needed. Maximizing the evidential weight of e-mail records also requires a secure audit trail capable of tracking every action against every archived e-mail message.

Look for security and scalability

A good approach to e-mail archiving will capture every e-mail and attachment and compress the data. A better approach ensures that a unique key is generated and encrypted, and that the message is digitally signed. The compressed, encrypted, and signed messages and attachments, normalized for single-instance, should then be written to a highly scalable relational database. Only after the archived message is successfully stored in the database should it be deleted from the archive inbox.

Keep in mind that solutions that scan mail servers for messages may not provide the best approach. Some products process mail messages as they pass through the server. This real-time processing provides airtight auditing and leaves no window for the messages to be tampered with prior to being encrypted and archived. A distributed configuration for the archiving application, which may run as a Windows service, can also eliminate the potential for degraded mail server performance due to archiving. Look for a solution that is able to run multiple archive processes simultaneously, each accessing a different mail server. This will aid in scalability as the flow of e-mail increases.

True compliance means maintaining the audit trail

The best e-mail archiving solutions will perform comprehensive auditing of every event in the life cycle of an e-mail message. Each time a message is stored, viewed, retrieved, or deleted, the audit system tracks the change, logging the activity in a secure database. Any changes made to policy configurations affecting an archived message should also be audited.

The encryption and digital signing of all e-mail and attachments, as soon as they enter the archiving process, eliminates any possibility of the audit trail being circumvented. Without comprehensive encryption, this guarantee cannot be made. The combination of strong encryption and a bulletproof audit trail allows administrators to vouch for organizational compliance with auditing requirements and SOX regulations with confidence.