

Sarbanes-Oxley and Email Archiving

An ArcMail Technology Research Paper



Organizations are faced with an increasing number of industry and government regulations that have made compliance a full-time position at many companies. While much of the compliance falls on the shoulders of publicly traded organizations, the standards established by legislation such as HIPAA, Gramm-Leach-Bliley Act and Sarbanes-Oxley are having far reaching impacts across both private and public organizations. A common requirement for many companies today in order to meet certain guidelines and to ultimately protect themselves is the concept of archiving. The truth is most industries from retail to health care to higher education are overwhelmed with the growing amount of data they have to manage. While the data is coming from a variety of sources, email is one of the main reasons why organizations have to add more storage capacity to their networks or look for archiving solutions specifically to manage email.

“E-mail archiving shows up as the tip of the iceberg when it comes to managing, securing, and exploiting the unstructured data within an organization.”ⁱ

According to a report by International Data Corporation, “The introduction of legislation such as the Sarbanes-Oxley Act of 2002 and the Health Insurance Portability and Accountability Act [HIPAA] has significantly increased the importance of managing, securing and storing all information within the enterprise. More specifically, because of regulations such as SEC Rule 17a-4 that are very prescriptive for the retention for email, and the numerous and very costly public lawsuits in which an email has been the deciding factor, email has emerged as one of the most important content types that need to be retained.”ⁱⁱ

The Sarbanes-Oxley Act of 2002 was passed in response to several extremely high-profile corporate financial scandals, such as those involving Enron and WorldCom. The Act, which is administered by the Securities and Exchange Commission, was designed to help protect shareholders from fraudulent activities and accounting blunders by making corporate executives ultimately responsible for their filed financial reports. In reality, SOX is having far-reaching effects on the entire organization. While the accounting department and c-level executives are responsible for the financial compliance of the act, all employees are being required to change their email and document storage habits, while the IT department is responsible for making sure the company complies with the electronic records storage requirements outlined the legislation.

The remainder of this paper will focus on the three rules of data storage described in SOX Section 802(a) and how email archiving solutions can help organizations meet compliance standards.

Rule 1

The first rule regarding document storage found in section 802(a) outlines the punishment of destroying, falsifying or altering records:

“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.”

Email has become one of the most important methods of communicating internally and externally because of its speed, flexibility and informal nature. Email is being used to negotiate contracts, collaborate with team members, document communications and store files that are used for all aspects of business.

A recent article in KM World magazine reported, “Twenty years ago, no permanent records existed that weren’t physically printed on paper, due to legal precedents. Now 60 to 70 percent of business critical data is, at some point, contained in email, so the need to manage, store, search and retrieve those electronic records is paramount. Email Management is now mission-critical.”ⁱⁱⁱ As a result of

its growing importance and how it is being used, in terms of SOX and the SEC, email is treated like any other electronic record. In the event of litigation or compliance audits, companies are being required to produce email correspondence, often more so than other documentation, either in support of their case or in response to a plaintiff's request.

In the Enron case, company auditors from Arthur Andersen were found guilty of sending emails requesting that employees shred documents related to Enron's financial and accounting irregularities. It was the evidence found in the emails that ultimately led to the demise of 82-year-old accounting firm. In September 2007, Morgan Stanley was forced to pay a \$12.5 million fine because it did not provide emails requested by the plaintiffs, instead falsely claiming the emails were destroyed in the 9/11 attack on the World Trade Center. Morgan Stanley was also fined \$15 million in 2005 to the SEC for failing to produce emails related to a research probe.

The list of companies being fined for deleting emails or not being able to produce documentation is growing, while retention practices of data, including email archives are being continually scrutinized. Email archiving solutions such as the ArcMail Defender automatically capture all original inbound and outbound emails and their attachments. Once the emails are stored on the device, they cannot be altered, destroyed or deleted.

Rule 2

Section 802(a)(1) outlines the amount of time companies are required to store files:

"Any accountant who conducts an audit of an issuer of securities to which section 10A(a) of the Securities Exchange Act of 1934 (15 U.S.C 78j-1(a)) applies, shall maintain all audit or review workpapers for a period of 5 years from the end of the fiscal period in which the audit or review was concluded."

According to a survey conducted by the Enterprise Content Management Association of the Association for Information and Image Management (AIIM), "storage consumers are basically ignorant when it comes to archiving." The ECMA survey 1,000 organizations, and the corresponding report said that "most organizations consider archiving as a collection of massive .pst backup files." In addition 46 percent of those surveyed considered archiving the responsibility of individual employees while only 26 percent considered it part of an overall information management strategy.^{iv}

One of the main differences between traditional back-up practices versus archiving is time. When companies backup information, they are confident that the information is being replicated. Archiving, on the other hand, is putting something in storage with the anticipation that it will be used again. Most emails programs have a built-in capability of backing up .pst files at a specific point in time. These programs simply take a snapshot of the inbox and other folders. When emails are deleted from the inbox, they are also deleted from the next back-up. An email archiving solution takes data protection to another level by automatically capturing and indexing all emails, including subject line, body contents and attachments, as they are sent or received. Archived data is being stored for the long-term so it is captured in such a way that it can be searched, retrieved and restored quickly.

Section 802(a)(1) indicates that information should be restored for a period of five years. A back-up file is for the short-term and can be overwritten, while archiving is about preservation. In solutions such as the ArcMail Defender, archiving policies can be established and enforced to meet the specific guidelines of SOX and other regulations.

Rule 3

Section 802(a)(2) outlines the types of information that need to be stored.

"The Securities and Exchange Commission shall promulgate, within 180 days, such rules and

regulations, as are reasonably necessary, relating to the retention of relevant records such as workpapers, documents that form the basis of an audit or review, memoranda, correspondence, communications, other documents, and records (including electronic records) which are created, sent, or received in connection with an audit or review and contain conclusions, opinions, analyses, or financial data relating to such an audit or review.”

“About 40% of companies cite the Sarbanes-Oxley Act as the biggest factor in archiving more of their email, with the Health Insurance Portability and Accountability Act and other healthcare regulations also triggering adoption.”^v

The SEC is treating email like any other document. With the growing dependence upon electronic communications, email has become “a prime candidate to look for a ‘smoking gun,’” during the litigation discovery and auditing processes. As a result, email retention and archiving policies and procedures should be constantly reviewed to ensure that they are meeting the needs of the various areas of the organization, from legal to accounting to IT. Unfortunately, according to a study conducted by the American Management Association and The ePolicy Institute, more than 66 percent of organizations do not have policies for saving, purging and managing e-mail. This despite the fact that among the companies surveyed, 24 percent had electronic messages subpoenaed by lawyers or regulators in 2006, compared to 14 percent in 2003.^{vi}

Driven by the growing number of legal concerns and compliance issues, the email archiving market continues to experience tremendous growth. IDC reported that the market grew by 45 percent in 2006 and expects the archiving applications market to reach \$1.4 billion by the 2011.^{vii} The Radicati Group expects the total email archiving market, including on-premise archiving systems and hosted services, to reach \$6 billion by 2010.^{viii}

According to IDC, “customers are increasingly demanding integrated workflows to support discovery and auditing. This coupled with aggressive reductions in the cost of connectivity and storage combined and rising awareness of new legal obligations is leading growth in the SMB and mid-market segments.”^{ix}

Finding emails on traditional tape drives and back-up applications can be difficult and expensive. With the limited amount of time allowed under SOX guidelines to respond to document requests, it is important that organizations have an email management solution that will help to retrieve all the necessary and correct emails quickly and easily. The ArcMail Defender makes it easy for administrators or end users to find and retrieve the information organizations need to comply with requests and defend their positions. The appliance automatically indexes all emails and the solution’s Web-based interface offers access to archived email from anywhere there is a Web connection while providing advanced search features, including full-text and wild-card searches.

Conclusion

SOX has made it clear that email correspondence must be securely archived for up to five years. Experts suggest that the best policy for email archiving is to capture anything and everything so that in the event of litigation or a compliance audit, organizations can have confidence in their storage strategies and make it easier for internal and external auditors to review the “virtual paper trail.”

The first step in solidifying an email archiving strategy is to establish an archiving policy and then find a solution that will help to enforce the policy. ArcMail Defender combines on-board storage, comprehensive archiving, data compression, disk management software, and easy to use web-based search and retrieve functions in one network appliance. Through Defender, organizations can enforce their archiving policies by eliminating one of the biggest challenges in the email retention process, people. Defender manages the entire archiving process and eliminates the need for manual back-ups. Defender also automatically captures all email messages and stores them

in such a way that they can be quickly tracked, reviewed, searched and restored by end-users, IT administrators or an attorney.

According to a recent survey by Osterman Research, IT departments receive an average of 36 business requests, 24 regulatory or audit-related requests, and 108 end-user requests annually.^x The average request for "retrieving raw email data for a single legal discovery request takes almost a month."^{xi} Companies can reduce the amount of time and costs associated with email storage and discovery by integrating an email archiving solution. The reliance upon email correspondence is only going to continue to increase, which makes email archiving a business critical process for all sized organizations, particularly in an era with more litigation and strong regulatory compliance standards.

ⁱ http://www.infostor.com/display_article/305936/23/ARTCL/none/none/1/Focus-On:-E-mail-management-and-archiving/

ⁱⁱ <http://accounting.smartpros.com/x46588.xml>

ⁱⁱⁱ <http://www.kmworld.com/articles/PrintArticle.aspx?ArticleID=15409>

^{iv} <http://computerworld.co.nz/news.nsf/news/DDA38125EE52836FCC25723E00071A25>

^v http://searchcio.techtarget.com/tip/0,289483,sid19_gci1188687,00.html

^{vi} <http://www.baselinemag.com/article2/0,1540,1998112,00.asp>

^{vii} <http://www.idm.net.au/story.asp?id=8496>

^{viii} http://aiimknowledgecenter.typepad.com/weblog/2007/05/the_email_archi.html

^{ix} <http://www.idm.net.au/story.asp?id=8496>

^x http://www.darkreading.com/document.asp?doc_id=133079

^{xi} *ibid*