



Achieving Regulatory Compliance With Email and Internet Content Security Policy Enforcement

By Ferris Research

EXECUTIVE SUMMARY

The maze of laws and regulations governing the treatment of electronic data has never been greater or more complex. Various regulatory bodies, as well as international, regional, and national governments, have different requirements for handling electronic data.

Many high-profile compliance cases illustrate the painful consequences of noncompliance. Organizations and their board members, executives, and administrators face lawsuits, fines, jail time, public embarrassment, loss of good will in the community, loss of revenue, and ultimately, the loss of customers.

In automating policy enforcement, organizations need to consider the distinction between regulatory compliance and corporate governance. Compliance refers to the complexities of obeying multiple legislative, regional, and global regulations and is litigated by the court system. Corporate governance requires following internal guiding principles as stated in acceptable use policies (AUPs) and is enforced by the organization. This distinction is important because AUPs create sound business practices that enable organizations to become compliant. Compliance is the next driver for content security.

This Ferris report focuses on compliance and regulations, particularly Sarbanes-Oxley (SOX), that impact IT managers, and suggests best practices for achieving compliance for electronic messaging content.

Those key best practices are:

- Protecting data from malware.
- Monitoring outbound email.
- Archiving electronic messages and content.
- Encrypting data during transport.

The report also looks at two products—MailMarshal and WebMarshal—which together serve as a platform for managing and enforcing electronic content security policies.

KEY ACTS AND REGULATIONS

The primary regulations of concern to IT managers are those covering privacy, records retention and disposition, monitoring for compliance, and the recovery or discovery of information in response to litigation or court orders. Organizations should communicate usage policies and compliance efforts to employees, customers, vendors, and other stakeholders.

The regulations listed below are applicable in the United States, Canada, and Europe, and represent an important subset of government and industry regulations for electronic mail, record keeping, and IT controls.

Privacy

Gramm-Leach-Bliley (U.S.)

The Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLB), controls the manner in which financial institutions handle customer information. The act contains several provisions relating to the privacy of consumer financial data, including a definition of privacy and information disclosure policies.

HIPAA (U.S.)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets requirements for health care and related organizations concerning the electronic communication of patient information. For example, hospitals cannot send private patient data via open email channels. The information must be transmitted securely, typically using encryption. HIPAA defines the types of data used to uniquely identify a patient. This includes names, birth dates, admission dates, telephone/fax numbers, Social Security numbers, medical record numbers, health plan beneficiary numbers, and biometric identifiers like fingerprints.

PIPEDA (Canada)

The Personal Information Protection and Electronic Documents Act (PIPEDA) protects personal information from improper disclosure during commercial transactions, activities involving federal work, and business dealings within Canada as well as internationally. The act also provides guidelines for the gathering, use, and storage of data.

Basel II Accord (EU)

Basel II is a global standard for risk management in financial institutions. The accord seeks to ensure the privacy of financial information when transferred across international borders. It also presents guidelines on the disclosure of private information.

Retention

Sarbanes-Oxley (U.S.)

The Public Company Accounting Reform and Investor Protection Act of 2002, also known as the Sarbanes-Oxley Act (SOX), was drafted principally in response to the corporate corruption and financial scandals rampant at the turn of the millennium. Also known as the “Enron Law,” Sarbanes-Oxley provides severe criminal penalties, including prison sentences, for corporate executives who destroy documents and business information. The act also specifies a records retention period of seven years and defines record types, such as physical and electronic documents and correspondence.

SEC Rule 17a-4 (U.S.)

The U.S. Securities and Exchange Commission (SEC), which regulates financial organizations, has implemented a comprehensive and specific set of rules for the management of electronic communication. These mandates include SEC Rule 17a-4, which requires storage of duplicate copies and maintenance of indices. The rule also mandates the ability to present stored messages for inspection and review within a reasonable time frame, typically 24 hours.

The SEC regulations and SOX overlap in that both address auditability and accountability of financial organizations, as well as record keeping and the protection of investors’ private information.

Title 21 Code of Federal Regulations (U.S.)

Part 11 of Title 21 of the Code of Federal Regulations (CFR) for the Food and Drug Administration focuses on electronic records and signatures relevant to the pharmaceutical industry. The code specifies criteria for acceptance of electronic records, signatures, and handwritten signatures affixed electronically to documents.

Data Protection Act 1998 (U.K.)

The United Kingdom’s Data Protection Act 1998 specifies that personal information held electronically must be secured and retained for defined periods, after which it must be destroyed. It also includes rules on the transfer of personal data.

ISO 15489 (Worldwide)

The International Organization for Standardization (ISO) has released ISO 15489—Information and Documentation, Records Management. This standard offers guidelines on the classification, conversion, destruction, disposition, migration, preservation, tracking, and transfer of records.

FSA (U.K.)

The Financial Services Authority (FSA) sets policies and standards for records management concerning the review, retention, and destruction of documents, computer files, email, and web pages. The FSA defines retention schedules for various financial records, ranging from three years to

indefinitely. FSA also draws a distinction between emails that contain information about business transactions (records) and those that contain no business information (ephemeral), and establishes storage and retention guidelines for both.

Monitoring

NASD Rule 3010 (U.S.)

The National Association of Securities Dealers (NASD) Rule 3010, as applied to email, requires that management be able to perform routine sampling and inspect customer communications to ensure that they are in accordance with regulations.

RIPA (U.K.)

The Regulation of Investigatory Powers Act (RIPA) 2000 addresses the interception of electronic communications as part of an investigative action and under what circumstances this information would be disclosed.

PCI DSS (U.S.)

The Payment Card Industry (PCI) Data Security Standard (DSS) provides guidelines for the protection of credit card holder information, including the use of encryption, the storage of secure data, and access control methods.

E-Discovery

FRCP Rules 26 and 30(b) (U.S.)

In December 2006, the Federal Rules of Civil Procedure (FRCP) were amended to include regulations concerning the processes for electronic discovery (e-discovery) and the implementation of a legal hold on email. According to Rule 26, organizations now must confer with the opposing party much earlier in the litigation process, and they must plan the way that electronic evidence will be collected, preserved, produced, and transferred. As part of this rule, IT staff must determine the accessibility of the data and develop a map of all data sources. FRCP Rule 30(b) calls for an expert IT witness to be designated.

Notifications

SB 1386 (U.S.)

The California Information Practices Act, SB1386, mandates that companies must notify consumers when they suspect or know that unencrypted personal information has been improperly disclosed, stolen, or lost. The company must notify those California customers directly affected as well as organizations doing businesses with customers in the state. Proper notifications of any suspected or actual improper disclosure include emails, web postings, and media alerts. If all the information disclosed was encrypted, then notifications are not required. As of October 1, 2006, 34 states have implemented similar legislation to protect their citizens.

MORE ABOUT SARBANES-OXLEY

The SEC is responsible for enforcing the corporate financial reporting procedures within the Sarbanes-Oxley Act. The SEC established a private, nonprofit organization, the Public Company Accounting Oversight Board (PCAOB), to develop regulations for implementation and enforcement.

SOX specifies the retention of financial records. Therefore, it is prudent for an organization to first identify all of its financial custodians and then design the security and archiving tools to address this group. Information technology is not explicitly mentioned by name in SOX. However, since the focus of the act is on financial reporting processes in publicly held companies, the IT impact is implicit: No public company is likely to prepare financial reports without the use of software, email, and other information technology.

The Purpose of the Act

The focus of SOX is to establish and manage controls and processes for financial reporting as an ongoing process. The key test for SOX compliance is whether the processes are deemed to be repeatable and sustainable. Processes used to produce financial reports must be shown to be consistent, reliable, secure, and accurate.

Time Frames for Compliance and Enforcement

External auditors are required to assess their clients' compliance with SOX as part of the audit process, beginning in the first fiscal year following the compliance deadline. The deadline for public companies with market capitalizations over \$75 million was November 15, 2004. The deadline for those valued at less than \$75 million was July 15, 2005. While SOX Section 404, Management Assessment of Internal Controls has been ratified, specific guidance on IT controls has not been published. Auditors are currently forced to rely on accepted practices and best judgment to assess the effectiveness of IT controls.

The Impact of SOX on Messaging and Collaboration

Large numbers of individuals are likely to be involved in developing financial reports in public organizations. They typically collaborate on the reports and create the content using various electronic technologies. SOX requires electronic collaboration to be documented and stored. Communication about corporate finances can no longer be an ad hoc process. Creating policies is not enough. Companies must also be able to demonstrate their practices for creating financial reports.

KEY STEPS IN SOX COMPLIANCE

Several aspects of SOX will be particularly challenging for messaging and collaboration systems. For example, SOX requires that organizations retain records related to the development of financial reports for seven years. This is challenging because hardware, software applications, formats, and storage media change over time, which may hinder an organization's ability to retrieve stored information.

Other aspects of the act, such as the requirement that internal audit committee members be able to receive anonymous comments from employees, force organizations to expand the

features of their messaging applications. Finding email systems with the ability to send anonymous messages may restrict the choice of vendors.

Apply Policy to Unstructured Communication

Email, instant messaging (IM), and other types of unstructured electronic collaboration tools are held to the same standards as other components of the financial reporting process. That means they must be consistent, reliable, secure, and accurate. For example:

- Senders and recipients of messages must be positively verified.
- The system should maintain an adequate log of the messages sent and received, with such details as time/date stamps, delivery status, read receipts, and where retained.
- It must be possible to protect messages from tampering during transmission or storage.

Establish Data Archives and Content Security Monitoring

SOX mandates a records retention period of seven years. That does not, however, apply to all email—only email included in the documented financial reporting process. Some customers estimate that half of their email need not be retained. The difficulty is in determining which half to keep.

Technology that helps differentiate between negligent and fraudulent behavior will also be particularly useful. For example, software could detect and report repeated attempts by an individual to violate policies. Nearly 90% of noncompliant activity is negligence. The purpose of SOX is to prevent fraud.

Document Process and Apply Technology to Limit Costs

The main costs of SOX compliance are in consulting, employee training, remediation of noncompliant content, data capture/retention, and handling retrieval requests. Technology will be most useful in controlling the cost of the latter two issues. Keeping all records forever won't achieve compliance if organizations cannot quickly find their records. Retrieval requests will become more costly if organizations don't have a well-defined and easily executed process for responding. Better metadata will help, but systems must generate this metadata automatically. Users shouldn't be trusted to reliably and consistently create it themselves.

Public IM and Webmail Must Identify Senders

Public instant messaging and Webmail do not ensure verifiable identity. Such anonymous communication is a problem under virtually all recent regulations. That's because a fundamental aspect of control is the ability to unambiguously identify people.

MAILMARSHAL AND SOX

Sections 302 and 404 of SOX discuss the requirements for organizations to document their internal processes for handling financial reports. However, these sections don't specify the steps necessary to fulfill the requirements. Organizations must

determine their own methods for meeting the requirements in a manner acceptable to their auditors and regulators. The following suggestions may be used as general guidelines for creating SOX policies, as well as many of the other rules governing electronic data.

Protect Data From Spam and Viruses

Spam can hurt the reliability of email as a communication mechanism, while malware (viruses, bots, and spyware) can expose confidential data. In extreme cases, spam can affect the performance of the email system by delaying message delivery. It's important to ensure that the email system is secure so that communication is maintained and data protected. An obvious first step to doing that is by blocking spam and malware.

MailMarshal, for example, is a content security solution for email that works with Microsoft Exchange, IBM Lotus Domino, and many other systems to protect against spam and malware at the Internet perimeter. It allows administrators to create and implement rules that block the majority of spam messages.

MailMarshal includes a proprietary technology known as SpamCensor that examines incoming messages. SpamCensor includes heuristic and message composition analysis to determine likely spam. SpamCensor Zero Day can be used to ensure prompt updates to virus signatures. URLCensor is an additional layer of spam detection that looks up URL links in email messages to see if they are listed as suspected sites. MailMarshal can then quarantine suspicious email in server-based, user-managed folders.

MailMarshal supports third-party Realtime Blackhole Lists (RBLs) such as SpamCop or Spamhaus. Using these services, administrators can block email from domains that have been known to send spam. MailMarshal also allows administrators to build their own rules to examine messages for inappropriate or dangerous content.

As a content security solution, MailMarshal allows administrators to define rules that block potentially dangerous content, such as executable file attachments. The TextCensor feature performs a lexical analysis to identify malicious and predefined keywords and phrases in email. Integration with the PestPatrol and CounterSpy modules enables organizations to prevent spyware threats.

MailMarshal also works with the virus scanning engines provided by leading vendors. MailMarshal is available with an optional McAfee or Norman solution. Alternatively, administrators can use a scanning engine such as one sold by Symantec, Frisk Software, Sophos, Panda, and others to provide an additional layer of protection.

Monitor Outbound Email and Content

SOX requires that the confidential corporate data used to develop financial reports, as well as the reports themselves, be protected from intentional or accidental disclosure.

Administrators can block both deliberate and inadvertent disclosure by using MailMarshal's outbound rules. Like inbound

rules for spam and virus protection, outbound rules define how outgoing messages and attachments are screened before they leave the organization.

Typically, administrators define rules that search for keywords relating to confidential data that could be contained in financial reports. Additionally, organizations may be required to protect customer information such as account numbers or Social Security numbers from disclosure. MailMarshal also protects against porn and offensive content.

Administrators can build outbound rules using text strings, natural language expressions, image analysis, or document fingerprinting to examine message content. For example, an organization may use fingerprinting to identify documents that have a format like that of an earnings statement, by comparing the hashed image of the document against that of a sample earnings statement. Or it may prohibit any message containing the word "earnings" from being sent before the earnings announcement. Using MailMarshal, administrators could build a rule that would look for variations on the word "earnings." Messages caught by the outbound rule can be quarantined or sent to an administrator, where they can be reviewed before being allowed to continue.

MailMarshal's TextCensor adds another layer of content control by assigning weights associated with the number of times that a word or phrase is detected within a message. These values can then be used to indicate the severity of the breach.

By integrating with an organization's directory—usually Microsoft Active Directory or LDAP—MailMarshal can support a range of role-based rule options to apply or exclude different policies to individuals, groups, or the entire organization. MailMarshal can also add message disclaimers, controls, and alerts on questionable email activity that can assist with legal and regulatory compliance. These alerts can be monitored and reported by severity level to management applications like HP OpenView, IBM Tivoli, and NetIQ AppManager, and through Microsoft Operations Manager (MOM) using MailMarshal's SMTP MOM Management Pack.

Archive Email for Seven Years, Then Delete

Increasing legal discovery requests prompted organizations to implement email archiving even before SOX made it mandatory. All communication relating to the creation of financial statements and reports must be archived and maintained for seven years. The communication must also be verifiably original, meaning that users cannot be allowed to alter their messages.

SOX requires that only messages relating to financial records be retained. However, organizations are likely to archive more content, rather than less, given the severe penalties for noncompliance. Therefore, it is extremely important to delete content when the retention period has expired.

Organizations should first determine what they are required to archive and then build the appropriate environment and storage capacity. They should take care to configure their archiving systems with sufficient storage space to accommodate data from a variety of sources and for growth.

The content filtering solution should then be placed in front of the email archive to scan and store business email and ignore casual messages.

MailMarshal can archive all inbound and outbound messages on the fly as permanent records. These archived messages can be stored in a repository of the administrator's choice, such as network or optical storage, or a database.

Organizations that do not wish to archive all email can configure MailMarshal to archive messages based on specific business rules. MailMarshal can archive messages based on the sender's or recipient's email address, and can use a company's internal directory for group-based policies. This allows an organization to archive all messages to and from the finance or executive groups, for example. MailMarshal can also archive messages that contain keywords or phrases.

Monitor Internal Email Traveling Between Mailboxes

Full compliance with SOX archiving regulations requires organizations to archive internal messages as well as messages that involve external parties. MailMarshal for Exchange is designed to archive messages sent internally on Exchange servers. (Organizations using other messaging systems such as IBM Lotus Notes or Novell GroupWise must use an alternative internal archiving solution to achieve full compliance.)

Encrypt Data During Transit

An important objective of SOX and other regulatory initiatives is data protection. Although SOX does not require encryption, organizations must ensure that confidential data is protected both internally and during communications with external partners.

Since SMTP email is typically sent in a human-readable, plain-text format, organizations should employ strategies to protect email messages while in transit or in storage. However, message security and encryption systems have not been widely used because of the cost and complexity of implementing and managing them.

For example, most of these systems rely on complex message-signing and encryption procedures that involve maintaining both "public" and "private" security keys. Administrators must manage the process of generating, validating, and renewing these keys for users. Organizations must also ensure that their encryption systems are compatible with their business partners' systems.

Easier encryption solutions are appearing, however. Transport Layer Security (TLS) is integrated into MailMarshal SMTP 2006. Additionally, MailMarshal Secure is an email encryption and decryption system that provides an automated process for encrypting messages. It reduces much of the complexity associated with message encryption between organizations. MailMarshal Secure is fully compliant with the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard for public key infrastructure (PKI).

Organizations can implement selective encryption by creating policies governing how outbound messages are handled.

Messages that are destined for specific domains can be automatically encrypted and signed by the MailMarshal server. Users do not have to manually sign or encrypt their email.

For example, a manufacturing company is in the process of developing its financial reports and is working closely with its external auditing firm. As part of this process, the company exchanges confidential information that needs to be protected while in transit. The manufacturing company implements MailMarshal SMTP, which allows it to build a rule that automatically encrypts any messages destined for the audit firm. Once the message arrives at the audit firm, the message is decrypted and becomes readable. MailMarshal prevents users from accidentally sending confidential information in an unprotected, open format. Policies can also be deployed based on message content, which protects messages containing keywords/phrases, Social Security numbers, account numbers, patient information, or other confidential data.

WEBMARSHAL AND POLICY MANAGEMENT

As part of corporate governance, most organizations have developed Internet, email, and company resources acceptable use policies as a means of improving productivity and reducing risk. These policies set the standards and expectations that employers have of appropriate Internet use within the workplace. Organizations need a way to manage and enforce these policies. WebMarshal is a solution for employee Internet management that enables organizations to define and use rule-based access policies.

Policy management of web browsing is about enforcing AUPs as it relates to company-enabled Internet access. This involves ensuring that work-related Internet access is safe from offensive material and dangerous content. It also involves ensuring that personal Internet use is moderated and does not pose a risk to the company. This risk includes lost productivity, exposure to legal liability, and loss of company confidential information.

Unmanaged Internet access can be a serious drain on productivity and can be more difficult to detect than excessive personal phone calls. It also has the added risks of providing a vulnerable entry point for viruses, spyware, and pornography, as well as a conduit for data leakage.

Organizations must secure their data assets from a regulatory compliance perspective. In addition, intellectual property leaks must be prevented to safeguard the company's brand and competitive position from improper disclosure. Managing Internet access enables an organization to thwart both malicious and inadvertent transmission of sensitive, proprietary, or private information.

WebMarshal acts as a gateway between the Internet and the network, allowing or denying access to the Internet based on predefined company policies. It supports virus scanning, quota management, URL blocking, and real-time content analysis of web pages. The product uses artificial intelligence to categorize content dynamically on the fly and to create lists based on detected content; or, organizations can create their own customized categories.

WebMarshal can protect against the risk of legal liability by preventing employees from browsing offensive content or downloading copyrighted or inappropriate material. WebMarshal monitors Webmail accounts to ensure that email traffic to and from websites is held to the same standard as email entering or leaving the corporate gateway.

WebMarshal also prevents viruses from entering the network through web-based email accounts and files downloaded from the web. In addition, it can protect confidential information by ensuring that private data is not intentionally or accidentally uploaded to public websites.

M86 SPONSORSHIP OF THIS WHITE PAPER

M86 Security commissioned this white paper with full distribution rights. You may copy or freely reproduce this document provided you disclose authorship and sponsorship and include this notice. Ferris Research independently conducted all research for this document and retained full editorial control.

FERRIS RESEARCH

Ferris Research is a market research firm specializing in messaging and collaborative technologies. We provide business, market, and technical intelligence to vendors and corporate IT managers worldwide with analysts located in North America, Europe, and the Asia-Pacific region.

To help clients track the technology and spot important developments, Ferris publishes reports, white papers, bulletins, and a news wire; organizes conferences and surveys; and provides customized consulting. In business since 1991, we enjoy an international reputation as the leading firm in our field, and have by far the largest and most experienced research team covering messaging and collaboration.

Ferris Research is located at 408 Columbus Ave., Suite 3A, San Francisco, Calif. 94133, USA. For more information, visit www.ferris.com or call +1 (415) 986-1414.

Ferris Research White Paper. Report #685. January 2007.
© 2007 Ferris Research, Inc. All rights reserved. This document may be copied or freely reproduced provided you disclose authorship and sponsorship and include this notice. For subscriptions, contact us at +1 415 986 1414 or info@ferris.com.

Free News Service

Ferris Research publishes a free daily news service. It provides comprehensive coverage of the messaging and collaboration field, and is a great way to keep current. Topics include spam, email, email retention/archiving, mobile messaging devices, consumer messaging services, web conferencing, email encryption, email migrations and upgrades, regulations compliance, instant messaging, ISP messaging, and team workspaces.

The news is distributed daily. To register, go to www.ferris.com/forms/newsletter_signup.php. In addition, you will receive one or two emails every month announcing new Ferris reports or conferences. To opt out and suppress further email from Ferris Research, click on the opt-out button at the end of each news mailing.

ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.com.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters

828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters

Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Asia-Pacific

Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Auckland, New Zealand

Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 09.01.09