

Using Content Security To Achieve Regulatory Compliance

A White Paper by Ferris Research

April 2005. Report #540

Contents

Using Content Security To Achieve Regulatory Compliance	2
Executive Summary	2
Key Acts and Regulations	2
Gramm-Leach-Bliley (Privacy)	2
HIPAA (Privacy)	2
Sarbanes-Oxley (Retention)	2
SEC Rule 17a-4 (Retention)	3
NASD Rule 3010 (Monitoring)	3
About Sarbanes-Oxley	3
The Purpose of the Act	3
Time Frames for Compliance and Enforcement	3
The Impact of SOX on Messaging and Collaboration	3
Key Challenges in SOX Compliance	4
Apply Policy to Unstructured Communication	4
Establish Data Archives, Security Monitoring	4
Documented Processes, Plus Technology, Limit Costs	4
Public Instant Messaging Presents a Unique Challenge	5
MailMarshal and SOX	5
Protecting Against Spam and Viruses	5
Protecting Content Against Disclosure	6
Archiving	6
Encryption	7
Marshal, MailMarshal, and WebMarshal	8
About Marshal	8

WHITEPAPER - Using Content Security To Achieve Regulatory Compliance

Executive Summary

This document reviews the current regulations that impact IT managers. It provides suggested practices that administrators should follow when developing internal controls over their record-keeping systems and processes. It also looks at Marshal's MailMarshal, which provides a platform that administrators can use to enforce many of the content security policies required under current regulations. By deploying a solution at the Internet perimeter as well as on internal email servers, administrators can unify the creation and management of content security policies.

Thanks to high-profile accounting scandals in the United States and other countries, businesses today are more regulated than at any other time in recent memory. The latest regulatory initiatives enforce standards for electronic messaging, record keeping, and related processes. The IT manager must respond to these regulations by implementing policies and procedures to protect and retain electronic data. At the same time, the manager must also support the business's needs for efficient communication and collaboration.

Regulations like the Sarbanes-Oxley Act require strong content security policies for email, including archiving and encryption. Administrators are tasked with ensuring not only that their email systems are highly available and free from spam and viruses, but also that data is secure both internally and when shared with partners. They must also implement plans for keeping a full record of relevant communication, including email messages, Webmail, and instant messaging (IM) conversations.

Key Acts and Regulations

The main regulations of concern to IT managers have to do with privacy, records retention and archiving, monitoring for compliance, and the recovery or discovery of information in response to litigation or court orders. The regulations listed below are applicable in the United States and represent an important subset of government and industry regulations for electronic mail. Similar regulations exist in many other countries.

Gramm-Leach-Bliley (Privacy)

The Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act, incorporates a number of provisions related to privacy of consumer financial data, including a definition of privacy policies and policies for disclosure of information.

HIPAA (Privacy)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) places specific requirements on healthcare and related organizations covering how they manage electronic communication with, and about, patients.

Sarbanes-Oxley (Retention)

The Public Company Accounting Reform and Investor Protection Act of 2002, also known as the Sarbanes-Oxley Act, was drafted largely as a legislative response to the corporate corruption and financial scandals rampant at the turn of the millennium. Also known as the "Enron Law," it provides severe criminal penalties, including



WHITEPAPER - Using Content Security To Achieve Regulatory Compliance

potential prison sentences, for corporate executives who destroy documents and business information.

SEC Rule 17a-4 (Retention)

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

NASD Rule 3010 (Monitoring)

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

About Sarbanes-Oxley

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

SOX is all about establishing and managing controls and processes for financial reporting. It is not a one-time event, but an ongoing process. A key test for SOX compliance is whether the processes are deemed to be 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 their audit process, beginning at 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 is July 15, 2005.

The Impact of SOX on Messaging and Collaboration

Development of financial reports in publicly held organizations not only requires technology, but also collaboration. That's because large numbers of individuals are likely to be involved. While financial reporting is inherently collaborative, SOX says it can no longer be adhoc. Organizations are required to "document what they do and do what they document."

Other recent regulations from organizations such as the SEC and NASD have

WHITEPAPER - Using Content Security To Achieve Regulatory Compliance

specifically included technologies such as email and instant messaging. History indicates that SOX IT assessment guidelines are likely to follow these established precedents.

Key Challenges in SOX Compliance

There are aspects of SOX that will be particularly challenging for messaging and collaboration software. For example, SOX requires that records related to the development of financial reports be retained for seven years. Other aspects of the act, such as the requirement that internal audit committee members be able to receive anonymous comments, will force organizations to expand their use of messaging technology. If email, instant messaging, or other collaboration tools are applied to the development of financial reports, they will be held to the same standards of consistency, reliability, security, and accuracy as any other component of the process. 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.

Apply Policy to Unstructured Communication

Denying access to messaging and collaboration tools to comply with SOX is not an option for most public companies. Organizations use unstructured communication tools like email and instant messaging because they need to be responsive and agile. Eliminating communications technology is unacceptable. Therefore, organizations must find ways to impose controls over these unstructured forms of communication.

Establish Data Archives, Security Monitoring

SOX mandates that records be retained for 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 for business reasons. The difficulty is in determining which half to discard.

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 non-compliant activity is negligence. The purpose of SOX is preventing fraud.

Documented Processes, Plus Technology, Limit Costs

The main costs of SOX compliance are in consulting, employee training, remediation, 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 will not achieve compliance if organizations cannot find the records they need. Retrieval requests will be more costly if organizations don't have a well-defined and easily executed process for responding. Better metadata will help, but systems must

WHITEPAPER - Using Content Security To Achieve Regulatory Compliance

generate this metadata automatically. Users shouldn't be trusted to reliably create it themselves.

Public Instant Messaging Presents a Unique Challenge

Public instant messaging does not ensure verifiable identity. Such anonymous communication is a problem under virtually all recent regulations. That is because a fundamental aspect of control is the ability to 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 to regulators. The following suggestions may be used as general guidelines for creating SOX policies.

Protecting Against Spam and Viruses

Much of the process of creating financial reports is conducted over email. Using email, employees collect information and share it internally. They also communicate with external groups like the company's auditors or accountants. In addition, employees frequently store critical data in their corporate mailboxes or shared folders. Spam can impact the effectiveness of email as a communication mechanism, while viruses and spyware can expose confidential data. In extreme cases, spam can impact a messaging system by delaying timely message delivery. It's important to ensure that the email system is safe and secure so that communication is maintained and data is protected. An important way to do that is by blocking spam and viruses.

MailMarshal's MailMarshal, for example, provides protection against spam and viruses at the Internet boundary. It allows administrators to implement rules that block the majority of spam messages. MailMarshal includes a proprietary technology known as SpamCensor that can examine messages as they are received by the system. SpamCensor includes heuristic and message composition analysis to determine likely spam messages. URLCensor is an additional layer of spam detection that performs a site lookup against any URL links in mail messages. MailMarshal can then perform actions based on the outcome of the lookup. Messages that are identified as spam can be quarantined in server-based folders. Users can periodically review their spam quarantine and release messages without requiring assistance from an administrator.

MailMarshal supports third-party Realtime Blackhole Lists (RBLs) such as SpamCop or Spamhaus. Using these services, administrators can block messages 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. MailMarshal protects against viruses in several ways. First, as a content security solution, administrators can define rules that block potentially dangerous content. For example, administrators might implement a rule that blocks all executable file attachments. 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 from Symantec, Frisk Software (F-Prot), Sophos, Panda, or others. This allows administrators to provide an additional layer of protection.



WHITEPAPER - Using Content Security To Achieve Regulatory Compliance

Protecting Content Against Disclosure

The corporate data used to build financial reports, as well as the reports themselves, are highly confidential. Even before SOX was enacted, it was in a company's best interests to protect confidential data from intentional or accidental disclosure. Now it's mandated by law.

In most cases, disclosure of confidential information isn't intentional. Most disclosure happens by accident. For instance, it's easy to mistakenly address an email so that it's sent to the wrong person. Features like Outlook's AutoComplete contribute to addressing mistakes. Or, users might choose "Reply All" rather than "Reply" when responding to a message. Administrators can block both intentional and unintentional disclosure by using MailMarshal's outbound rules. Similar to the inbound rules that are used to examine messages for spam and viruses, outbound rules are used to examine messages for specific content before they leave the organization. Administrators can define rules that search both messages and their attachments.

Commonly, administrators would define rules that search for words relating to confidential data, such as financial reports. Other organizations may have a mandate to protect customer information such as account numbers or Social Security numbers from disclosure. Administrators can build outbound rules using text strings or more powerful regular expressions to examine message content. For example, a financial firm may want to prohibit any message that mentions "earnings" from being sent before the earnings announcement. Using MailMarshal, administrators would build a rule that looked for variations on the word "earnings." Messages that are caught by an outbound rule can be quarantined or sent to an administrator, where they can be reviewed before being allowed to continue.

Archiving

Even before SOX became effective, organizations began implementing message archiving solutions as a response to increasing legal discovery requests. However, SOX makes message archiving a requirement. 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. For example, a user shouldn't be able to send a message, and then go back into his or her sent mail folder and alter a sentence or other message properties, like the sent time.

SOX doesn't require that organizations archive every email message or instant messaging conversation. Only messages relating to financial records must be retained. However, organizations are likely to archive more content, rather than less, given the regulatory requirements and the severe penalties for failure. MailMarshal can archive all incoming and outgoing messages 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 or recipient email address, and can use a company's internal directory for group-based policies. This allows an organization to archive all messages to or from the finance or executive groups, for example. MailMarshal can also archive messages that contain keywords or phrases. To fully be compliant with



WHITEPAPER - Using Content Security To Achieve Regulatory Compliance

SOX archiving regulations, organizations must archive internal messages as well as messages that involve external parties. Since MailMarshal is an Internet perimeter solution, organizations will have to employ an internal archiving solution to achieve full compliance.

For organizations that use Microsoft Exchange, Marshal has a product called MailMarshal Exchange that performs functions similar to MailMarshal, but for internal Exchange servers. Organizations that are not using Exchange will have to implement an alternative solution.

Encryption

An important objective of SOX and other regulatory initiatives is data protection. Organizations must ensure that confidential data is protected both internally and during communications with external partners. In the case of SOX, confidential information means financial reports and the data used to create these reports. In other regulatory scenarios, confidential information could include patient medical data, customer financial data, or privacy-related data such as Social Security numbers and account numbers.

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 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, such systems rely on complex message-signing and encryption procedures that involve maintaining both “public” security keys 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.

MailMarshal has an add-on product called MailMarshal Secure that reduces much of the complexity associated with message encryption between organizations. MailMarshal Secure is an email encryption and decryption system that provides an automated process for encrypting messages. MailMarshal Secure is fully compliant with the Secure Multipurpose Internet Mail Extensions (S/MIME) standard for public key infrastructure (PKI).

Administrators can define policies governing how outbound messages are handled. Messages that are destined for specific domains can be automatically encrypted and signed by the MailMarshal Secure server. Users don’t have to manually sign or encrypt their email.

For example, a manufacturing company is in the process of creating its financial reports and is working closely with its external auditing firm. As part of this process, the company exchanges confidential information that it wants to protect while in transit. While the company could implement a manually operated encrypting and signing service, it might be prone to error and difficult to maintain.

The manufacturing company implements MailMarshal Secure, 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 read using standard technology. The MailMarshal Secure service prevents users from inadvertently sending confidential information in an unprotected, open format.



WHITEPAPER - Using Content Security To Achieve Regulatory Compliance

Policies can also be deployed based on message content, which protects messages containing Social Security numbers, account numbers, or other confidential data.

Marshal, MailMarshal, and WebMarshal

About Marshal

With new threats disrupting business, productivity and wrecking reputations every day, Marshal's content security solutions take a proactive approach to identifying email and web vulnerabilities to protect over seven million international users from the risks of email and Internet threats.

Marshal's flagship and award-winning product MailMarshal has offered businesses of all sizes more security enhancements than competitive solutions for more than five years. MailMarshal SMTP 2006 is the market's first to combine spam URL black list lookups and spam filtering based on country of origin.

A privately-owned software company Marshal has headquarters in Basingstoke, UK with regional offices in UK, France, USA, New Zealand and South Africa.

About MailMarshal

Marshal's MailMarshal is a content security solution for email that works with Microsoft Exchange, Lotus Domino, and many other messaging systems. MailMarshal protects an organization against spam, spyware, phishing, and viruses. It also offers a range of defense mechanisms for denial-of-service attacks and directory harvesting attacks. MailMarshal provides a platform via a single management system that enables the deployment of one to hundreds of nodes to secure mail systems and also implement an organization's messaging policies.

MailMarshal examines all incoming and outgoing messages to protect the company and the network from spam and inappropriate use. Only authorized information is allowed to enter or leave the network, while annoying or potentially harmful messages are blocked at the gateway.

By integrating with an organization's directory, Marshal's MailMarshal can support a range of rule options in order to apply 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 into systems like HP OpenView, IBM Tivoli, and Marshal AppManager.

About WebMarshal

Marshal's WebMarshal is a solution for employee Internet management that enables administrators to enforce corporate Internet "acceptable use" policies as a means of improving productivity and reducing risk. 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. WebMarshal can protect against the risk of legal liability by preventing employees from browsing offensive content or downloading copyrighted material. WebMarshal provides an area of compliance assurance by monitoring Webmail accounts to ensure that email traffic



WHITEPAPER - Using Content Security To Achieve Regulatory Compliance

to and from Web sites is held to the same standard as email entering or leaving the corporate gateway. Marshal's 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.

Authors: Chris Williams, David Via

Editor: Sue Hildreth

Marshal's Sponsorship of This White Paper

Marshal 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 Asia/Pacific.

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 1, San Francisco, Calif. 94133, USA. For more information, visit www.ferris.com or call +1 (415) 986-1414.

The Ferris Research User Panel

The User Panel consists of IT professionals who work with messaging and collaborative technologies, providing services to their organizations' users. People join to share experiences with other people like themselves, learn from each other, and keep current on news and trends.

If you provide technical support for an email system, and you are not a member of the User Panel, you can join and learn more about the User Panel at www.ferris.com/url/userpanel.html. There is no charge to join.

WHITEPAPER - Using Content Security To Achieve Regulatory Compliance



Americas
Marshal, Inc.
5909 Peachtree-Dunwoody Rd
Suite 770
Atlanta
GA 30328
USA

Phone: +1 404-564-5800
Fax: +1 404-564-5801

Email: americas.sales@marshal.com

Marshal's Worldwide and EMEA HQ
Marshal Limited,
Renaissance 2200,
Basing View,
Basingstoke,
Hampshire RG21 4EQ
United Kingdom

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

Email: emea.sales@marshal.com
info@marshal.com | www.marshal.com

Asia-Pacific
Marshal Software (NZ) Ltd
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Greenlane, Auckland
New Zealand

Phone: +64 9 984 5700
Fax: +64 9 984 5720

Email: apac.sales@marshal.com