
EMAIL COMPLIANCE AND REGULATIONS



MESSAGING AND WEB SECURITY ESSENTIALS SERIES

Realtime
publishers
"Leading the Conversation"

» Email Compliance and Regulations

By Dan Sullivan

PRIVACY AND CORPORATE GOVERNANCE REGULATIONS HAVE INTRODUCED SEVERAL ADDITIONAL RESPONSIBILITIES IN IT MANAGEMENT. AS ORGANIZATIONS HAVE ADAPTED TO THE REQUIREMENTS IMPOSED BY REGULATIONS, IT HAS BECOME CLEAR THAT, IN MANY CASES, THERE IS A CONFLUENCE OF INTERESTS IN THOSE CONCERNED WITH COMPLIANCE AND THOSE CONCERNED WITH SOUND IT MANAGEMENT PRACTICES. EMAIL COMPLIANCE AND MANAGEMENT IS ONE OF THOSE CASES.

This article examines some of the more well-known regulations that have an impact on email management practices, then explores the most effective way to comply with these regulations. The best practice is to implement policies and procedures that should already be in place in response to common business drivers. A corollary to this position is that sound email management practices will bring an organization into compliance with multiple regulations at once. There should be little need for silos of compliance procedures crafted for particular regulations.

Major Regulations Affecting Email

Not surprisingly, the major regulations that demand the most attention of organizations, and corporations in particular, are also the ones with the most significant impact on email management. These include:

» **THE SARBANES-OXLEY ACT**—The major U.S. legislation on corporate governance is probably best known in the IT area for section 404. That part of the legislation requires adequate internal controls to protect the integrity of financial reporting.

» **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)**—Addresses the privacy of individuals' healthcare information. The law requires, among other things, that doctors, hospitals, and other covered entities take reasonable steps to ensure that communications with patients are kept confidential.

» **THE GRAMM-LEACH-BLILEY ACT (GLBA)**—Applies to financial services companies and requires that they follow three basic privacy rules. First, personal data of customers must be stored securely. Second, institutions must advise customers of the firm's privacy policies. Finally, customers must have the option to direct the institution to not share their information with third parties.

» SECURITY EXCHANGE COMMISSION (SEC) RULE 17A-4

—Applies to securities brokers and dealers and requires comprehensive recordkeeping. One of the requirements of the rule dictates that records of communications related to securities business must be preserved for not less than 6 years and, for the first 2 years, those records must be in an easily accessible format.

» NATIONAL ASSOCIATION OF SECURITIES DEALERS

(NASD) RULE 3010 AND 3110—Approved by the U.S. SEC, this regulation requires its members to review incoming and outgoing communications to customers.

» **U.S. PATRIOT ACT**—Allows for email surveillance techniques, analogous to older telecommunication monitoring techniques, such as pen register and trap and trace. It also provides authority for government officials to access email records.

» **CYBER SECURITY ENHANCEMENT ACT**—Allows U.S. government officials to receive email records from ISPs without warrants.

As this list demonstrates, the motivations for regulations affecting email management range from corporate governance and consumer protection to law enforcement and counter-terrorism. There is always the chance that focus on a particular public policy will wax and wane, but the broad base of legislation applying to email ensures that regulations of one form or another will be with us for the foreseeable future.

Impact on Email Management Objectives

Looking across the major regulations, you can see that IT has several responsibilities with respect to email; they boil down to keeping email messages confidential, maintaining the integrity of the application, and ensuring that records of communication are available for some period of time. Even without regulations, many organizations would implement most if not all of these practices because these practices make sense from a business perspective. There would, of course, be differences in some details, such as how long to retain communications records and with whom to share certain types of information. The overall management framework, however, would remain the same.

Such a framework includes several procedures:

- › Securing email servers, clients, and related infrastructure
- › Defining email policies, including acceptable use and retention policies
- › Monitoring and auditing email operations
- › Archiving messages

These practices serve to meet the requirements of multiple regulations.

Email Security

The need for email security is nothing new. Viruses, worms, Trojan horses, and blended threats have spread through email for years. It is difficult to imagine connecting a device (or at least a Windows device) to the Internet without anti-malware protection. In addition to client-based anti-malware, detection and filtering applications can be deployed on email servers or at the network perimeter. This setup provides a defense-in-depth strategy widely used in information security.

Access controls should be used to protect both confidentiality and integrity of the email system. Of course, authentication mechanisms should be in place to prevent unauthorized access to a user's account, but strict access controls should be in place on email servers to reduce the chance of a breach. Access events should be monitored and audited.

Deploying security measures is not a one-time activity. Anti-malware applications require updates both to their signature

database for detecting malware and to the application code itself. Like any complex software, these programs can have bugs. Change management and patch management procedures should be used to ensure security measures are up to date. These procedures, like other email management operations, should be governed by well-defined policies.

Email Policies

Email policies should set the scope of acceptable use, privacy and confidentiality, and retention. Acceptable use policies define the types of ways email systems may be used. Typically, organizational email is restricted to company business. These policies can also be used to define the management activities carried out in the process of managing the organization. For example, management may retain the right to monitor all email, keep copies of all emails, and treat email messages as assets of the organization. In effect, users should not expect or assume any degree of privacy with regards to email communications.

Privacy and confidentiality, as it applies to customer, patient, and client information as well as proprietary company information, is a different story. Organizations have a responsibility to protect private information that has been provided for business purposes. Several regulations make this explicit. Email policies should identify categories of information that may be sent through email and under what conditions. For example, private patient information may be sent from a hospital to a doctor only if it is encrypted and digitally signed.

Email archiving policies define what content is archived and how long it is retained. In many cases, archiving all email may seem like the appropriate measure, but such is not necessarily the case. For example, should messages quarantined as spam or phishing messages be archived? The volume of these messages alone could result in significant increases in storage volumes. There are also questions around personal mail folders (.pst files in Microsoft parlance). Should those be archived along with centralized mailboxes? In some cases, such as in securities industries, regulations require records of all communications, regardless of how they are stored internally in the email system; in other cases, the requirements may not be as stringent.

Monitoring & Auditing Email Operations

Auditing email operations can fit both regulatory and business requirements. Regulations may require that you not only perform a specific action but also that you can document that you have carried it out. Understanding trends in email use is essential for capacity planning and maintaining service availability. Monitoring and auditing operations can serve both of these objectives.

SPECIFICALLY, YOU SHOULD MONITOR:

- › Provisioning of email accounts and changes in access controls
- › Rates of malware and spam detection
- › Growth rates in storage volumes
- › Network traffic patterns

Archiving Messages

Another key area of regulatory compliance is archiving. Email storage requirements can grow quickly enough that it is not practical to keep all messages online. Archiving is required to meet compliance and business needs without sacrificing performance or increasing costs unnecessarily.

Archiving should not be conflated with backup and recovery. The purpose of backup and recovery is to ensure operational continuity in the event of a system failure or loss of data. Backups typically operate at the file-system level or lower. They do not necessarily provide ways to easily restore objects within a file, such as a series of emails.

Summary

Email compliance is just one instance of the regulatory impact on IT operations. There are a number of government regulations that apply to email services, and the list of such laws is likely to grow. Fortunately, many regulatory requirements coincide with business requirements for security, business continuity, and operations management. Sound email management driven by business needs can go a long way toward compliance as well.

Dan Sullivan is the resident editor at the Realtime Messaging and Web Security Community. Please contact Dan with your comments at: dan_sullivan@realtimepublishers.net

For more Messaging Security information please visit The Realtime Messaging and Web Security Community, sponsored by McAfee, at: www.realtime-emailsecurity.com.

www.realtime-emailsecurity.com