A Guide to Keeping E-mail Legal: Four Pillars of Compliance

By Daniel J. Langin, Attorney at Law LLC

Introduction

People often yearn for the "good old days," a mythical time when gasoline cost less than three dollars a gallon, people weren't so overwhelmed and life in general was simpler. Unfortunately, in the world of information technology, the "good old days" also refers to a time when wi-fi was still a dream, hackers often held the upper hand and the legal landscape concerning technology represented a frontier more than a settled place to conduct business.

In these "good old days," protecting a company from e-mail based risks was also simpler. Companies could focus on screening incoming messages for malicious code, and worry less about whether their e-mail systems complied with laws, regulations and standards.

Unfortunately, changes to the ways in which sensitive information is gathered, communicated and retained have fostered the creation of laws, regulations and standards that dictate how companies and government entities use and protect e-mail and e-mail systems. Now e-mail must be protected not only from incoming threats, but it must also be monitored, screened and in some cases, retained for compliance with a host of laws and regulations. E-mail policies must be created, administered and monitored and violators must be discovered and sanctioned.

Despite this apparent complexity, the bulk of the compliance responsibilities that apply to e-mail systems can be broken down into four fundamental categories, or "pillars of compliance":

- Prevention of inbound threats
- Management of outbound threats
- Retention and auditability
- Administration (policy creation, enforcement and compliance).

This paper will provide basic guidance on how to meet these responsibilities and thereby keep a company's use of its e-mail systems legal, without interrupting basic business processes. Before exploring these issues, however, it is helpful to examine the compliance requirements that affect e-mail systems.

What Compliance Requirements Affect E-mail Systems?

The laws, regulations and standards that affect e-mail systems include HIPAA, the Gramm-Leach-Bliley Act ("GLBA"), the Sarbanes-Oxley Act ("SOX"), the PCI Data Security Standard ("PCI"), FISMA and FTC Section 5. In addition, international laws and standards such as EU Data Protection Directive 95/46/EC, the Basel II Accord ("Basel II") and the pending changes to EU Directive 2002/58/EC (concerning e-mail retention by service providers) create requirements concerning e-mail systems. Perhaps the most surprising thing about these laws is that most companies are subject to *at least* one of them. They are not limited in scope to traditionally regulated industries (like financial or healthcare institutions) or to "technology companies."

For example, HIPAA applies not only to health care providers, insurers and data processors but also to the employee group health plans operated by most employers. PCI applies to all merchants that accept credit cards, as well as the member banks and credit card data processors. As if these laws were not broad enough, FTC Section 5(a) applies to any business engaged in interstate commerce.

The scope of jurisdiction is also very wide. HIPAA and GLBA apply to U.S. entities, or foreign entities with operations in the U.S. that are subject to the jurisdiction of US regulators. FTC Section 5(a) applies to any company, whether U.S.-based or not, that does business in interstate commerce in the United States. SOX and SEC Rule 17a-4 apply to any U.S. or non-U.S. business whose shares are traded on any United States public exchange, such as the NYSE or NASDAQ. PCI applies to any merchant, member bank or processor for MasterCard, VISA, Discover, Amex or Diner's Club, whether in the US or overseas (because it is a contractual standard enforced by the credit card companies, it is not subject to any jurisdictional limits). The EU Data Protection Directive and EU Directive 2002/58/EC apply to any company located in an EU member nation. Basel II applies to banks worldwide, subject to enacting regulations by individual nations.

HIPAA, GLBA, FISMA and PCI each contain numerous, detailed information security requirements. Although FTC Section 5(a) and SOX do not contain specific references to information security, they have been interpreted to include it within their scope. FTC Section 5(a) has been applied by the FTC to e-mail use (see the Eli Lilly example cited below), and the SEC in May 2005 confirmed that "internal controls apply to general and application level IT systems and processes that influence financial reporting." The EU Data Protection Directive and EU Directive 2002/58/EC respectively contain requirements specific to data security and e-mail retention, while Basel II contains more general guidelines that apply to operational risk, internal loss event data and policies and internal controls for disclosure of data.

Before exploring the specifics of these four pillars of compliance, it may be helpful to understand why they were created. How did we get from an environment with few compliance requirements to an environment with multiple compliance requirements in less than a decade?

How We Got to Compliance:
The Transformation from Risk to Regulation

Before these laws, regulations and standards existed, most companies and government entities perceived the main threat to e-mail systems to be malicious code contained in incoming messages. Numerous high-profile events involving viruses spread by e-mail caused significant losses, such as the Melissa virus. At first, most of these losses were internal losses, and they did little to change the legal or regulatory landscape.

As time went on, however, the gradual transition from paper to electronic recordkeeping focused the attention of lawmakers on potential risks to crucial data arising from e-mail systems. This transition enabled employees and other insiders to transmit millions of sensitive records to outsiders with the push of a button, and exposed sensitive data to greater risks than ever before. In the eyes of many lawmakers, this risk was more insidious than the risk of receiving malicious code in incoming messages because of the difficulty of detecting malicious (or misguided) insiders, and the significant potential for loss to the individuals whose sensitive information could be exposed. Furthermore, the increasing use of e-mail as a medium of business communication meant that document retention requirements that formerly applied to paper communication now also had to be applied to electronic communications.

The result of these developments was the creation of laws, regulations and standards that govern the collection, storage and transmission of sensitive information. These measures include provisions that apply specifically to e-mail systems and e-mail usage because of the crucial role that e-mail plays in communication for virtually all business and government entities.

The Four Pillars of E-Mail Compliance: How to Keep E-Mail Legal

As noted above, virtually all of the laws, regulations and standards that govern e-mail systems include four common, basic requirements:

- Protect against vulnerabilities from incoming e-mail
- Guard against loss or misuse of private or regulated information in outgoing e-mail
- Archive e-mails that contain certain kinds of content, for future review or auditing
- Adopt and enforce administrative measures designed to protect e-mail systems from compromise or misuse

Adopting these four pillars can help a company reach compliance with the bulk of the laws, regulations and standards that affect e-mail systems. These four pillars are described in more detail below

Pillar #1: Prevention of Inbound Threats

In general, most of the laws, regulations and standards affecting e-mail systems contain some kind of requirement that companies adopt measures to adopt protection measures against malicious code or other threats, including viruses, corporate phishing or spam, in incoming messages. These laws and regulations require companies and government entities to protect themselves from inbound e-mail threats for the purpose of protecting the security and integrity of the sensitive data that is regulated by the specific law or standard.

For example, the HIPAA Security Rule requires covered entities to address "procedures for guarding against, detecting and reporting malicious software[1]" to ensure that private health information is not accessed, altered, destroyed or rendered unavailable. Requirement 5 of the PCI standard, titled "use and regularly update anti-virus software," requires merchants and others to prevent inbound messages containing malicious code[2] from harming or destroying credit card information and the systems on which it is collected, transmitted or stored. Section SI-3 of NIST SP 800-53 (the primary technical standard underlying FISMA) requires that government entities "employ[] virus protection mechanisms … to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) transported: (i) by electronic mail, electronic mail attachments, … ; or (ii) by exploiting information system vulnerabilities[3]." The EU Data Protection Directive more generally requires that companies receiving personal data on EU member citizens adopt appropriate technical and administrative measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

In addition to these specific requirements, the "internal controls" requirements under SOX likely require companies to screen incoming e-mail for viruses or other exploits (such as phishing requests) that could disrupt financial reporting processes or lead to unauthorized acquisition, use or disposition of the registrant's assets. A 2003 survey by the Hackett Group found that 47% of the companies surveyed used individual spreadsheets for planning and budgeting, so a virus that destroys or corrupts these individual files could seriously disrupt the financial reporting process. The main technical governance standard used by most companies in implementing SOX (known as COBIT) contains standard DS 5.19, which states that "[b]usiness and IT management should ensure that procedures are established across the organization to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response and reporting[4]."

Most anti-virus software is capable of screening for malicious code, but corporate phishing and other false requests for information may be more difficult to fight because

---

[1] 162 CFR 164.308.(a)(5).
[2] See Visa USA, Inc. Payment Card Industry Data Security Standard, Version 1.0 (December 15, 2004) (available at www.usa.visa.com).
[3] NIST Special Publication (SP) 800-53 Section SI-3, as adopted by FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information Systems" (FIPS 200) (March 2006).
[4] IT Governance Institute, "The Control Objectives for Information and Related Technology."

they involve a "human element" (i.e., the user has to be prevented from falling for a fraudulent request). A virus screen cannot easily detect carefully worded (but fraudulent) text in an e-mail message from a malicious third party who is seeking sensitive information for purposes such as identity theft. To comply with the laws, regulations and standards concerning inbound e-mail, companies may need to not only screen for viruses, but to also adopt measures to protect themselves from the human element of an exploit by:

- Screening incoming e-mail for keywords that would suggest an employee is receiving an inappropriate or unauthorized request for data
- Tracking whether employees are complying with e-mail policies concerning requests for data
- Alerting administrators to these activities.

Pillar #2: Managing Outbound Threats

Simply preventing inbound threats is not enough to establish compliance. Because many laws, regulations and standards limit the sharing of sensitive information with third parties, companies and government entities must carefully screen whether regulated information is being improperly sent out via e-mail. Managing outbound threats may be potentially more difficult than preventing inbound threats because the persons being monitored are insiders with valid e-mail accounts, authorization to use the system and probably better access to sensitive data than outsiders.

In general, the laws, regulations and standards mention four basic types of activities that need to occur to satisfy this second pillar of compliance. They are: (a) preventing accidental or purposeful release of sensitive data to third parties; (b) ensuring that only authorized employees can access and send out sensitive data; (c) ensuring that the parties to whom data is sent are authorized to receive it, and; (d) ensuring that sensitive data in transit is sent securely, whether by encryption or otherwise.

Stopping employees from complying accidentally (or purposefully) with corporate phishing or other unauthorized requests for data is a very important but elusive compliance requirement. The best protections against outsider access to data and systems are useless if the insiders who have access to the data can send it to the wrong persons. According to a survey cited by CFO Magazine, insiders such as current or former employees are often guilty of providing customer information or mailing lists to phishers[5]. One of the early Internet-privacy cases brought by the FTC under Section 5 of the FTC Act involved an Eli Lilly employee who accidentally sent out a company e-mail that identified over 700 users of the prescription drug Prozac[6]. In the more recent FTC action against ChoicePoint, the company was fined $10 million in civil penalties and paid $5 million in consumer redress because its employees were duped into sending personal

[5] ("Preventing Identity Theft," CFO Magazine May 19, 2004).
[6] See the FTC's complaint at http://www.ftc.gov/os/2002/01/lillycmp.pdf.

financial records of over 160,000 consumers to phony "subscribers" who requested them[7].

Companies must also take steps to ensure that only employees who have been authorized to access and send sensitive data can send it outside of the company. Requirement 10 of PCI requires companies to track all individual accesses to cardholder data. The HIPAA Security Rule[8] similarly requires entities covered by HIPAA to maintain technical protections to ensure that only persons who should have access to electronic health information can gain that access. Logically, these requirements include preventing parties who are not been authorized to access such information from sending e-mail messages containing such information.

Equally important is the requirement that companies ensure that sensitive data is only sent to parties who are authorized to receive it. The HIPAA Security Rule, GLBA Interagency Guidelines, PCI and FISMA all require regulated entities to put procedures and technologies into place to ensure that sensitive data is sent only to parties who have been authenticated as being parties eligible to receive it (such as insurers under HIPAA, credit reporting agencies under GLBA, and so forth). The GLBA Interagency Guidelines, for example, require that institutions adopt controls "to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means[9]."

Finally, most of these laws and regulations also require that data in transit be sent securely, whether by encryption or otherwise. This is often not the case as illustrated by a survey in 2003 by ZIX Corporation, which indicated that millions of sensitive health records (known as PHI) are sent *insecurely* in violation of the HIPAA Security Rule. This survey sampled 4.4 million e-mails sent and received by 7,500 healthcare organizations over a one-week period and found that, on average, 4% of these messages included *unprotected* PHI. Companies and government entities need to be able to screen for regulated content, track whether it is being encrypted or protected as required by law, and stop transmission if not.

The internal controls requirements under Section 302 of SOX may also include screening e-mails for issues regarding financial reporting, misuse or disposition of assets without management approval or fraud. A July 2004 study by PricewaterhouseCoopers identified a lack of embedded controls and excess human intervention as a significant compliance difficulty[10]. The ability to screen e-mail for key words or attachments related to financial reporting issues could help break down this barrier, given that most financial reporting is still done on individual spreadsheets exchanged via e-mail systems. This ability could also help detect fraud that involves management or other employees who have a significant role in company's internal controls, as required by SOX.[11]

---

[7] See http://www.ftc.gov/opa/2006/01/choicepoint.htm
[8] 162 CFR 164.312(a)(1).
[9] 12 CFR 364, Appendix B, Section III.C.1(a).
[10] Price-Waterhouse-Coopers, "New Reporting and Compliance Rules Challenge Systems at Most Large U.S. Companies" (July 2004).
[11] Sarbanes—Oxley Act section 302 (a)(5)(B).

Last, compliance with these requirements and the requirements of Pillar 1 are consistent with banks' duties to mitigate operational risk under Basel II.

Pillar #3: Retention and Auditability

An old saying goes "if it's not written down, it doesn't exist." The writers who developed the laws, regulations and standards concerning information security took this saying to heart. Most contain provisions that require companies to retain records concerning sensitive information, and to be able to audit and produce these records on request from regulators or consumers. This would include records of e-mail messages sent or received that contain the kind of information that is subject to the law, standard, or regulation and records of compliance efforts.

Section 5.2 of PCI, for example, requires that anti-virus software be capable of generating audit logs and that these logs be retained in accordance with the company's retention policy. Under SOX, the ability to retain e-mails concerning financial reporting activities can be crucial to ensuring that evidence of internal controls exists sufficient to support the law's disclosure and reporting requirements under Sections 302 and 404. Tracking internal loss event data[12] and adopting specific criteria for assigning loss data into a centralized function such as an IT department[13] are requirements of Basel II that involve e-mail system functions.

Perhaps the most high-profile examples of e-mail related retention requirements however are SEC Rule 17a-4 and EU Directive 2002/58/EC. SEC Rule 17a-4 requires regulated entities such as securities exchange members, brokers and dealers to retain electronic communications such as e-mails. In December 2002, five brokerages were fined $8.25 million for failure to retain e-mails under this rule, and in March of 2004, Bank of America was fined $10 million for failure to produce e-mail on a timely basis under 17a. The proposed amendments to Directive 2002/58/EC would require EU member nations to adopt data retention laws compelling electronic communications service providers to store and retain information on their customers' communications for law enforcement purposes for six months.

Pillar 4: Administration (Policy Creation, Enforcement and Compliance)

Nearly all of the laws, regulations and standards mentioned in this article include a set of administrative requirements for compliance. Most of them require companies to adopt security policies (including policies regarding e-mail usage and access to/transmission of sensitive data), to enforce these policies and to sanction employees who fail to comply with the policies.

Section 12 of PCI, for example, requires the adoption of a security policy that covers all of the requirements of the PCI standard. The NIST SP 800-53 standard that underlies

[12] Basel II, paragraphs 670 and 671.
[13] Basel II, paragraph 673.

FISMA contains several specific policy requirements (including one for a general security policy) and the HIPAA Security Rule requires adoption of a specific sanctions policy for employees who fail to comply with the covered entity's security policies and procedures. Basel II requires adoption of a formal disclosure policy for proprietary and confidential information (both on its own products and systems and on customer data), approved by the Board of Directors, which addresses what disclosures the bank will make and internal controls over disclosure, as well as a process for assessing the appropriateness of disclosures by examining validation, frequency or other factors[14].

Policies are useless, however, if they cannot be enforced. Policy enforcement is generally not practical without automated, technical means to monitor compliance, and sanctions cannot be administered to offending employees unless companies can track down which employees have violated them. Real-time screening of e-mail messages to determine whether they contain sensitive data and the ability of systems to report potential violations involving the e-mail system may enable supervisors or IT security staff to know when violations are occurring, to stop them and to prevent future violations. The ability to detect misuse of e-mail can also support sanctioned policy requirements.

Reasons to Comply with E-mail Laws, Regulations and Standards: Fines and Penalties

The four pillars described above offer a good road map to optimize protection of a company from e-mail based risks. Additionally, they can help companies avoid monetary sanctions in the form of fines, penalties or a loss of funding. Sanctions for several of these laws, regulations and standards are described below:

- HIPAA: up to 10 years prison/$250,000 (for the most serious violations)
- GLBA: FDIC may impose penalties ranging from $5,000 per day up to $1,000,000
- SOX: Up to $1 million fine/10 years in prison for knowingly violating Section 302 (penalties increase to up to $5 million in fines/ 20 years in prison for willful violations)
- FISMA: Loss of or decrease in agency funding
- PCI Data Security Standard: $500,000 per incident under VISA PCI program (if non PCI--compliant member is compromised)
- FTC Section 5 and State Unfair Trade Practices Laws: A typical penalty is a 20-year period of monitored security, and fines can run as high as $10 million plus additional payments in the millions for consumer redress.

Perhaps more than any other factor in the emergence of e-mail laws, regulations and standards, the weight of these sanctions suggests that e-mail compliance has become more than simply running anti-virus software. So long as e-mail remains one of most pervasive means of communication, e-mail systems will continue to be regulated for the

[14] Basel II, Paragraph 819.

purpose of preventing sensitive data from being wrongfully accessed, altered, sent or destroyed.

Conclusion

Following the four pillars of compliance outlined in this paper can help companies avoid serious sanctions under existing laws, regulations and standards. Technical measures that allow companies to track and screen e-mail messages can make compliance much simpler, as they remove the primary monitoring responsibility from the burden of human interaction, can create automated retention or audit trails, and can allow a company to connect misuse of the e-mail system to a specific individual.

Appendix: Overview of Laws, Regulations and Standards Affecting e-Mail Systems

Pillar	**#1 Inbound**			**#2 (Outbound)**				**#3 Retention**			**#4 Policy**	
Action Req'd	*Anti-Virus*	*Anti-Spam*	*Anti-Phishing*	*Only auth'd indiv's can send*	*Prevent response to malicious inbound*	*Send only to auth'd parties*	*Send securely*	*Retain*	*No changes*	*Respond to regulatory or audit requests*	*Enforce*	*Track User*
PCI	√		√*	√	√	√	√	√		√	√*	√*
SOX & SEC Rule 17a-4	√*		√*	√*	√*	√*		√	√	√	√*	√*
HIPAA	√		√*	√	√	√	√	√*	√*	√*	√	√*
GLBA	√*		√*	√	√	√	√				√*	√*
FTC 5	√*		√*	√*	√*	√*	√*				√*	
FISMA	√	√	√*	√	√	√	√				√	√*
EC Dir. 95/46/ EC	√*		√*	√*	√*	√	√*	√		√		
Basel II	√*		√*	√*	√*	√*	√*	√*	√*	√*	√*	√*
EC Dir. 2002/58 /EC								√	√	√		

*Although not specifically mentioned, this term is implied from other terms of the law, regulation or standard.

About the Sponsor

Founded in 1991, SonicWALL, Inc. designs, develops and manufactures comprehensive network security, e-mail security, secure remote access, content security, continuous data protection, and policy and management solutions. Offering both appliance-based products as well as value-added subscription services, SonicWALL's comprehensive solutions enable organizations to secure deep protection without compromising network performance. SonicWALL is a recognized global leader in the small and medium business markets and its solutions are deployed in distributed enterprise environments, government, retail point-of-sale and healthcare segments as well as through service providers.

SonicWALL Email Security coupled with SonicWALL Compliance Subscription provides organizations of all sizes with a powerful framework for stopping e-mail threats and managing compliance requirements. Available as a hardened appliance or Windows software, SonicWALL Email Security combines an award-winning anti-spam engine with anti-phishing, anti-virus, content filtering, policy management and compliance capabilities.

SonicWALL Email Security enables organizations to meet both regulatory and corporate requirements by intelligently identifying e-mails that violate compliance policies, monitoring and reporting and applying multiple enforcement actions. SonicWALL Email Security effectively and securely automates management of outbound e-mail communications.

About the Author

Daniel J. Langin is the principal of Daniel J. Langin, Attorney at Law, LLC. He has over 17 years of experience in private and corporate practice, including thirteen years of experience in technology, insurance coverage and intellectual property litigation and counseling. For more information, see www.langinlaw.com or contact Daniel at (913) 661-2430 or dlangin@langinlaw.com. This article is provided for general educational and informational purposes. It is not intended to provide legal advice.