



LivePrism On-Demand Services

White Paper

**E-mail Compliance
Security Solutions for
Regulatory Requirements**

By Kevin Beaver

Introduction

Email is the most widely used Internet application in the world. Email and other emerging methods for electronic communication help to fulfill the need for the quick response times and immediate gratification required in today's business environment. Given email's pervasiveness throughout the industrialized world today, most organizations cannot function without it. The critical business processes that email supports such as sales orders, customer service, and employee collaboration have created a requirement that email be available at all times.

As if the business needs surrounding email aren't enough for organizations to manage, there has been a recent surge of government regulations that affect this form of communication. These laws, which affect large and small companies alike in practically every industry, were written to ensure that email is being used and managed properly from an employee perspective. Toward that goal, the laws protect confidential customer information, uphold corporate governance and protect law enforcement investigations. However, there are dozens of issues surrounding the security of email in business today – many of which are often overlooked.

Email security issues may include:

- Policy development and management
- Email retention
- Employee monitoring
- Data storage
- Patch management
- Malware
- Spam
- Legal liabilities
- Confidentiality of intellectual property
- Data integrity
- Network and data availability

In order to effectively use email as a business tool, these security issues must be addressed from a technical, managerial, and regulatory perspective. Unfortunately, there is no magic formula, product, or service that will handle all of these aspects of email. At least in the foreseeable future, email security will require some form of human and/or manual intervention.

There are, however, some highly effective solutions that can help with these issues from the executive level all the way to end users. A smart decision for the practical businessperson is to automate as much of the technical, managerial, and regulatory requirements as possible. This is especially important for small and medium businesses that are dealing with fewer IT and security resources.

This paper provides an overview of some of the highly visible U.S. laws affecting email security; a look at St. Bernard's email security service; and information on how St. Bernard Managed Protection Services can help organizations comply with current and future legislation to minimize the impact on their bottom lines.

The Regulatory Landscape

It should be noted that this information is not legal advice, but is rather an introduction, from an IT perspective, to some well-known U.S. laws that have emerged recently and how they might affect the way email is currently managed and secured. This material is only the tip of the iceberg. The laws discussed in this paper, and virtually any other law affecting information technology in today's organizations, can be far-reaching and very complex.

The specifics of these and other laws need to be addressed with legal counsel or other outside advisors to ensure a complete understanding of how they affect each individual organization and industry.

Health Insurance Portability and Accountability Act

The most widespread and well-known piece of legislation is the U.S. Department of Health and Human Services' Health Insurance Portability and Accountability Act, also known as HIPAA. HIPAA, which originated in 1996 under President Clinton, affects the entire healthcare industry, one that happens to encompass approximately 15 percent of the U.S. economy. The section of HIPAA that we're concerned with here is called Administrative Simplification. This section contains three major rules written to help ensure the privacy and security of protected health information (PHI), as it relates to individuals, as well as to standardize various electronic healthcare transactions and code sets. Organizations that must comply with HIPAA are called covered entities. This group includes hospitals, insurance providers, employer health plans, physicians, and more. In addition, any business associate of these covered entities that has access to or handles PHI on behalf of the covered entity such as lawyers, accountants, auditors, and billing companies must have a contract in place with the covered entities stating that they will protect PHI as well.

HIPAA is obviously very far-reaching and will end up affecting a good majority of U.S. companies in one way or another.

The two HIPAA rules that affect email security are the Privacy Rule and the Security Rule. For our purposes, we will focus on the HIPAA Security Rule because it contains specific requirements that mirror the Privacy Rule, but goes into much more detail. The Security Rule was made effective on April 21, 2003 and was enforced for most covered entities by April 21, 2005. This rule primarily focuses on information security best practices and revolves around the security cornerstones of confidentiality, integrity, and availability.

The Security Rule is broken down into three main sections as listed in Exhibit 1.

Exhibit 1 – HIPAA Security Rule Standards

Administrative Safeguards – 9 standards (approximately 55% of the total rule)

1. Security Management Process
2. Assigned Security Responsibility
3. Workforce Security
4. Information Access Management
5. Security Awareness and Training
6. Security Incident Procedures
7. Contingency Plan
8. Evaluation
9. Business Associate Contracts and Other Arrangement

Physical Safeguards – 4 standards (approximately 24% of the total rule)

1. Facility Access Controls
2. Workstation Use
3. Workstation Security
4. Device and Media Controls

Technical Safeguards – 5 standards (approximately 21% of the total rule)

1. Access Control
2. Audit Controls
3. Integrity
4. Person or Entity Authentication
5. Transmission Security

Based upon the results of an initial risk analysis, HIPAA covered entities may have to comply with most or all of these HIPAA Security Rule standards. For all practical purposes, every standard listed in Exhibit 1 somehow affects email security. For all the details on HIPAA including the actual rules, frequently asked questions, and covered entity decision tools, you may access this link:

<http://www.cms.hhs.gov/hipaa/hipaa2/default.asp>.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act, also referred to as GLBA, is to the financial industry what HIPAA is to the healthcare industry. In brief, it is designed to ensure the privacy and security of non-public personal information (NPI) as it relates to individual financial information. Although not quite as far reaching as HIPAA, GLBA, which was enacted in 1999, is still making quite an impact on business in the U.S. GLBA has two rules that affect the privacy and security of personal financial information – the Financial Privacy Rule and the Safeguards Rule. These rules apply to financial institutions (similar to HIPAA covered entities) such as mortgage lenders and banks and possibly even their service providers and affiliates (similar to HIPAA business associates). Eight Federal agencies, led by the Federal Trade Commission, and various state agencies have authority to enforce the GLBA rules. Like HIPAA, the main rule that affects email security is the Safeguards Rule, which is very similar to, but more high-level than, the HIPAA Security Rule. This rule was published on May 23, 2002 and was made effective on May 23, 2003. Organizations that must comply with GLBA, many of which are already known for having above average information security, are given less detail on what needs to be implemented and maintained for compliance. It is, however, a good framework to build on for email and other security requirements.

The main standards for safeguarding customer information in GLBA also revolve around confidentiality, integrity, and availability of information and include provisions for administrative, physical, and technical safeguards just like the HIPAA Security Rule requires. The specific (paraphrased) elements required by the GLBA Safeguards Rule are listed in Exhibit 2.

Exhibit 2 – GLBA Safeguards Rule Requirements

- 1.** Designate an employee(s) to coordinate your information security program
- 2.** Identify reasonably foreseeable risks to NPI in the areas of:
 - o Employee training and management
 - o Information systems
 - o Incident response and contingency plans
- 3.** Design and implement safeguards to control the risks
- 4.** Oversee service providers
 - o Select and retain service providers who are capable of maintaining appropriate safeguards
 - o Require service providers by contract to implement and maintain these safeguards
- 5.** Evaluate and adjust the information security program on an ongoing basis

Obviously, the GLBA Safeguards Rule is more loosely structured than the HIPAA Security Rule, but it basically covers the same areas. As with HIPAA, some areas of the Safeguards rule may apply more than others depending upon the organization, but all of the requirements will affect

email security in one way or another. The full GLBA rules and more can be found at <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>.

Other Laws Affecting Email Security

Although HIPAA and GLBA carry the most weight when it comes to industry-specific information security legislation, there are other new laws that may apply as well. The first of these, the Sarbanes-Oxley Act of 2002 (referred to as SarbOx or SOX), is overseen by the U.S. Securities and Exchange Commission (SEC). This law, which regulates corporate governance over financial reporting of public companies, was enacted largely due to the many highly visible misdeeds of some US corporations in the early 2000's. Certain specific sections of SOX, such as 404 and 802, which address management assessment of internal controls (such as what leaves the organization's network) and records management and retention (such as what electronic information needs to be retained and for how long) respectively, could very well have an impact on an organization's email security practices and overall risk management programs. In addition, the internal financial reporting controls that are required by SOA could parallel, or even overlap, the various information security controls within an affected organization. Public companies and other private organizations that work closely with these companies need to become intimately familiar with SOX to ensure that email practices and information security management in general are in line with its specific requirements.

In addition to SOX, there are other laws on the books, such as the SEC Rule 17a-4 and the NASD Rules 3010 and 3110, that affect email communications for the financial industry. These rules, which are similar to the retention rules of SOX, require organizations to retain emails for at least six years as well as provide for the auditing of email content. Also, organizations that do business in Europe and other foreign countries could be required to comply with foreign legislation as well.

Finally, the USA PATRIOT Act of 2001 and the Cyber Security Enhancement Act of 2002, including future expansion of these government surveillance powers, could also affect email security and management for many organizations. To reiterate, it's critical for all organizations – large and small, public and private – to obtain legal counsel in these and other areas of corporate regulation to determine whether compliance is necessary, and if so, to ensure that compliance is being properly addressed and met.

A Look at St. Bernard Managed Protection Services

St. Bernard On-Demand Email filter offers an "in the cloud" hosted service that protects your organization and helps it comply with the many industry regulations we have discussed. In fact, it's one of the pioneers in this type of email security offering. St. Bernard On-Demand Email Filter offers several features and layers of protection to enhance email management and security. These features include:

- Distributed network architecture that has been up 100 percent of the time since its launch – a statistic very few ASPs can claim – and a 99.999% uptime guarantee
- Global gateway service – acting in an application service provider (ASP) mode –serves as a front-end for the customer's email service accessible from anywhere over the Internet which can help reduce email administration and bandwidth usage
- Local messaging router that can be used instead of the global gateway service for customers that require local control of email management and security yet still want to benefit from all of the other St. Bernard email protection services
- Email attachment filtering and quarantining to help eliminate potentially damaging Malware

- Spam filtering to eliminate 98% of junk email without the customer having to maintain the filtering lists in order to keep up with the latest spam filter evasion techniques
 - Blacklist filtering to block messages from specific senders
 - Whitelist filtering to allow messages from specific senders
 - Content filtering to help minimize intellectual property losses and prevent unwanted messages from entering and leaving the network
 - Virus filter running two different virus scanning engines, which are updated with the latest signatures every 10 minutes, to help prevent malware from ever entering the network
- Outbound email gateway that can scan outgoing emails with the virus filter to help eliminate malware attachments before they reach their destination as well as to offer a layer of privacy and security protection for the originating email server
- Permission-based email that blocks all inbound messages until approved by the recipient
- Policy filter that enables the blocking of emails based on message size and the number of recipients
- Store and forward service acting as a backup email server to temporarily house emails when the customer's email server is unavailable
- Reporting features that allow for granular monitoring and management of email usage

The true value in these features is that they require little to no administrative overhead on the customer's part. Of course users and email administrators are still going to have to address quarantined messages, etc., but the management of the email infrastructure and security are handled entirely by St. Bernard. Internal support staff and automated systems at St. Bernard manage your email security while you're free to focus on other IT and security infrastructure and management issues.

How St. Bernard Can Help With Regulatory Compliance

Having discussed the regulatory requirements that organizations are being faced with in today's marketplace along with an overview of what the St. Bernard Managed Email Filtering has to offer, it's now time to point out how the St. Bernard solution can help with these issues. Email is not the only information system component that needs to be secured in order for organizations to maintain compliance with the various regulations – it's only a piece of the overall information security infrastructure puzzle. Having said that, and knowing how valuable email is to businesses even with the myriad of information threats and vulnerabilities associated with it, email security is still a critical piece of the puzzle. St. Bernard Managed Protection Services offer an email solution that can address your security and regulatory issues while conserving your internal IT resources. A benefit of developing an overall information security plan and infrastructure for regulatory compliance, and general best practices, is that virtually every component is scalable down to the email function and vice versa.

One of the advantages of the U.S. regulations covered in this paper is that they are all written and at a high level yet they do not specify how information is to be protected. This means that services such as St. Bernard's can be used in a hands-off, managed fashion to help organizations meet the regulatory requirements they face without having to add additional staff or technology systems. The email protection services offered by St. Bernard can assist with an overall information risk management framework consisting of the following best practices steps:

1. *Assess* information risks
2. *Plan* out security strategies
3. *Implement* countermeasures
4. *Monitor* for new risks and overall security effectiveness
5. *Control* with corrective actions
6. *Repeat*

As it relates to specific regulatory compliance issues that we've discussed in this paper, the St. Bernard solution can be implemented as part of an overall information security and compliance strategy to assist with the confidentiality, integrity, and availability requirements that are prevalent in current laws affecting business information systems. The specific benefits that the St. Bernard solution can provide to help meet these requirements are:

- Security policy and standards enforcement
- Access controls to prevent unauthorized disclosure of private customer or corporate Information
- Protection from Denial of Service (DoS) attacks against internal email servers
- Email availability in the event of an email server malfunction or other unexpected downtime
- Contingency plan support through distributed offsite systems that are shielded from local disasters
- Content filtering to protect against non-business related computer usage and unauthorized dissemination of confidential information
- Spam filtering to ensure system uptime and availability, minimize network bandwidth storage space requirements, and to help prevent social engineering and other email attacks
- Malware protection that can prevent security incidents from occurring in the first place and reduce their overall impact
- Electronic document retention and records management
- Ongoing email auditing

Email is often the primary means of communication with customers, business partners, and fellow employees. Failure to address risks to email systems, or any information system for that matter, can jeopardize an organization's reputation and long-term viability. This is equally true for compliance requirements. In order to ensure the security of email systems and to effectively manage regulatory compliance programs, certain best practices must be implemented. These best practices, when properly implemented and managed, can be key long-term success factors.

Information security is not easy and regulatory compliance tends to complicate it even further. Solutions such as St. Bernard's on-demand email security offering can help your organization comply with regulatory requirements plus give you the added benefits of reduced IT administrative burdens and less technical expertise required which both lead to lowered costs.

The government has enacted a slew of regulatory legislation during this decade and it doesn't look like we have seen the end of new laws. Organizations that are prepared to address the world's increasing information risks, government regulation complexities, and the demand for better electronic privacy and security will have a leg up on their competition. This competitive differentiation is one of the best information technology returns on investment any organization can have.

About St. Bernard Managed Protection Services

St. Bernard acquired its on-demand security solutions, a company known as Singlefin, in 2006. Founded in 2001, Singlefin, now St. Bernard, is a leading provider of on-demand security and productivity solutions. St. Bernard Managed Protection Services offers state of the art solutions that block spam and viruses as well as protect an organization's entire e-mail infrastructure. Citing several competitive advantages, St. Bernard on-demand security solutions, which include email, Internet and IM filtering, are commonly used by small to mid-sized companies where e-mail and Web access is mission critical. St. Bernard's global network offers a 99.999% uptime guarantee with 100% historical uptime. Utilizing their fully redundant and geographically dispersed data-centers, they are able to quickly process electronic information as well as provide

secure backup for their clients' infrastructures. Viruses are blocked at the gateway and junk mail is held offsite so it never affects their client's critical networks.

For more information, visit www.singlefin.net

About the Author

Kevin Beaver is founder and principal consultant of Atlanta, GA based Principle Logic, LLC. He is an information security consultant, author, and trainer with over 15 years of experience in IT and information security. He is co-author of the new book "The Practical Guide to HIPAA Privacy and Security Compliance" by Auerbach Publications, and author of the new books "Ethical Hacking for Dummies" by John Wiley and Sons and "The Definitive Guide to Email Management and Security" by Realtimerepublishers.com. Kevin is also technical editor of the book "Network Security for Dummies" by John Wiley and Sons, and a contributing author and editor of the book "Healthcare Information Systems, 2nd ed." By Auerbach Publications. In addition, he is a regular columnist and information security expert advisor for SearchSecurity.com and SearchMobileComputing.com. Kevin also serves as a contributing editor for HCPro's Briefings on HIPAA newsletter and is a Security Clinic Expert for ITsecurity.com.

DISCLAIMER: The author has used his best effort in the preparation of this white paper. The information and opinions provided in this white paper do not constitute or substitute for legal or other professional advice. Readers should consult their own legal or other professional advisors for individualized guidance the application of federal, state, and local regulations to their particular situations and in connection with other compliance related concerns.