



Beyond Compliance: Protecting Business Communication Across The Organization

Voltage Security, Inc.

February 2005

Table of Contents

I. Introduction – Being Compliant is a Never Ending Challenge.....	2
II. Privacy Regulations	2
III. The Consequences Of Insecure Communications	5
IV. The Voltage Privacy Management Platform.....	8
V. Conclusion	9

Copyright © 2005 Voltage Security, Inc.

All rights reserved.

All information in this document is subject to change without notice. This document is provided for informational purposes only and Voltage Security, Inc. makes no warranties, either express or implied, in this document.

Voltage SecureMail, SecureFile, SecureIM and SecurePolicy Suite are trademarks of Voltage Security, Inc. All other company and product names may be trademarks of their respective owners.

Rev. 020105

I. Introduction – Being Compliant is a Never Ending Challenge

Protecting the privacy of email communication across all departments and business units can be challenging. Whether it's financial data in spreadsheets, confidential business plans, or emails from HR to your health insurance provider—the data needs to be kept private. On top of this, regulations like Sarbanes-Oxley, GLBA, HIPAA, and PIPEDA place an emphasis on ensuring that confidential and personal information is protected - wherever it resides.

In the United States certain privacy regulations have caught the media's attention and continue to gain momentum. It started with the regulatory revolution of the healthcare industry with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The Privacy Rule, which became enacted in 2003, mandates the protection of "Protected Health Information" (PHI). The Security Rule, which includes the protection of Electronic PHI will be ratified in April 2005.

Following HIPAA, the privacy and security of financial information came to the forefront. In 1999 Congress enacted and President Clinton signed the Gramm-Leach-Bliley Financial Modernization Act (GLBA). GLBA reflects Congress's opinion that "each financial institution has an affirmative continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."¹

Lastly, motivated by corporate scandals, the Sarbanes-Oxley Act (SoX) has profoundly changed the way corporate America does business. SoX demands that executives of publicly traded companies confirm their confidence in the quality and integrity of their financials by signing for their legitimacy. Under SoX, the Securities and Exchange Commission (SEC) holds executives accountable for reliable internal controls, record retention, and fraud detection.

HIPAA, GLBA, and SoX have drawn attention to the challenges of utilizing best practices to securely exchange, transmit and store sensitive information inside and outside an organization. Due to the fact that email is the most popular form of business interaction and is legally binding in many situations, this communication channel (regulated or not) must be protected with the same fervor that most important paper contracts are guarded. By failing to protect corporate information, enterprises are subjecting themselves to capture the media's attention in the most unfavorable way.

This whitepaper will provide a high-level overview of these three regulations that have grabbed the media's attention and have forced specific industries to react. It will also provide an insightful look into the information that is being transmitted from and within an organization that could be putting a company in legal and/or moral jeopardy even though specific compliance regulations may not be directly applicable. Finally it will provide insight into the Voltage Privacy Platform, a solution that can play a critical role in overall corporate compliance and best practices programs by securing not only email but also additional kinds of digital communication.

II. Privacy Regulations

The Health Insurance Portability and Accountability Act (HIPAA)

In the early 1990s, the Bush Administration called a group of health care industry leaders together to discuss how health care administrative costs could be reduced. This group concluded that this could best be done by increasing the use of electronic data interchange (EDI) within the industry.²

¹ Title 15 United States Code ("U.S.C.") Section 6801(a).

² Richard Zon Owen, Hawaii Medical Service Association, 2000

The Workgroup for Electronic Data Interchange (WEDI) was created to address the situation. After conducting a number of studies to determine how this might be accomplished, it finally recommended that Federal legislation be passed to ensure that a consistent set of standards could be used across all states. The Health Insurance Portability and Accountability Act (HIPAA) was signed into law on August 21, 1996.³

Unfortunately, medical records management demonstrated that privacy and security breaches were occurring regularly which led Congress to add privacy and security protections for health information into the Health Insurance Portability and Accountability Act (HIPAA).⁴ HIPAA calls for standards requiring Covered Entities to implement “appropriate administrative, technical, and physical safeguards.” The purpose of these safeguards is to ensure the integrity and confidentiality of health information. The safeguards also are to protect against reasonably anticipated threats and unauthorized uses.⁵

HIPAA covers health plans, healthcare Clearinghouses, and health care providers who transmit information in electronic form for certain kinds of transactions (Covered Entities).

According to Gartner, Health care organizations will spend between 0.1% and 0.5% of their total annual revenue on HIPAA compliance technology.⁶

The Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act, was signed into law in 1999. Congress enacted GLBA to modernize financial services by updating the ways in which banking, securities, and insurance organizations do business. Upon finalizing the bill, which permits information sharing among affiliates or with certain joint marketers, the issue of privacy was accentuated resulting in an entire title (Title V) devoted to this complex issue. There has been a lot of focus on this provision as it concentrates on safeguarding and securing the confidentiality of customer’s non-public information—it’s an issue that everyone (from your neighbor to your grandma) cares about. It’s an issue that highlights the strategic business and technical actions that must be implemented to secure customer data, both internally and externally, from unauthorized access.

GLBA covers “financial institutions.” That category is a broad one. In addition to banks, savings associations, credit unions and the like – financial institutions also covers businesses that are “financial in nature,” - such as insurance carriers, tax and financial advisors, money transmitters, and pay day lenders.⁷ Many businesses may be surprised to discover that they fall under GLBA, even though they consider themselves very different from the typical example of financial institutions, banks.

According to Dan DiFilippo, head of Pricewaterhouse Coopers’ governance, risk and compliance practice, “Technology is a ‘critical enabler’ in achieving accountability. Most organizations lack real-time event, process, and reporting capabilities. They rely on manual processes for compliance, although they expect to implement technology-based solutions.”

³ Richard Zon Owen, Hawaii Medical Service Association, 2000

⁴ Health Insurance Portability and Accountability Act of 1996, Pub. Law No. 104-191, Statutes at Large (“Stat.”), vol. 110, p. 1936 (1996).

⁵ 42 U.S.C. § 1320d-2(d)(2).

⁶ “Health Mandates will give tech a boost”, USA Today, June 3, 2004

⁷ The definition of “financial institution” in GLBA, 15 U.S.C. § 6809(3)(A) refers to a description in another law, 12 U.S.C. § 1843(k), which speaks of activities that are “financial in nature or incidental to a financial activity.”

The Sarbanes-Oxley Act (SoX)

Motivated by corporate scandals such as Enron and WorldCom, SoX has profoundly changed the way corporate America does business. SoX redefines the law of securities more than any statutory change since the original 1933 and 1934 securities laws. It addresses perceived shortcomings in the ability for the law to deal with abuses such as false financial reporting, auditors failing to blow the whistle on shady accounting practices, and the destruction of evidence.

SoX addresses the threat of fraud in the finance departments of public companies by placing great emphasis on companies establishing reliable “internal controls” for gathering, processing, and reporting financial information with the ultimate goal of ensuring accurate reporting of public companies’ finances for the benefit of investors. Taken to its logical conclusion, however, implementing reliable internal controls means more than just avoiding human manipulation of revenue and cost figures. Internal controls relate to the entire system of running a finance department. Moreover, given the critical role played by information technology in finance operations, a focus on internal controls inevitably will involve some scrutiny over assurances of the integrity, reliability, effectiveness, and performance of information systems used by finance or, in other words, information security.

Email communication policy is an integral part of controls to safeguard information from unauthorized use, disclosure, modification, damage, or loss. Email communications is an important means of moving revenue and cost information to those analyzing it, a means of circulating financial reports internally, and communicating information to those who will report it to the public. At the same time, email security vulnerabilities create the risk of the unauthorized disclosure, loss, destruction, or corruption of financial information, thereby thwarting the SOX goal of accurate financial reporting. The interception and unauthorized access to email can lead to leaks of financial information. Malicious code, including viruses, worms, Trojan horses, certain kinds of spyware, may infect workstations with code allowing for later unauthorized access or tampering with financial records. A deluge of spam may overwhelm corporate email servers, reducing the effectiveness and availability of this vital resource.

The bottom line is that internal controls rest on a foundation of system-wide mechanisms, policies, and procedures that include IT security and particularly email security, and given the critical role played by email, as well as the considerable security vulnerabilities plaguing email, securing email within public companies must be a high priority.

While neither Sarbanes-Oxley (SOX) nor the SEC’s implementing regulations imposes specific requirements for email security or IT security in general, the frameworks commonly used for assessing internal controls set control objectives applicable to email security and IT security generally. Companies that fail to implement email or other components of IT security, run the risk that auditors will be unable to attest to the internal controls or to the accuracy of their financial statements. (*A more in depth review is available in the Voltage White Paper “A Guide to the Sarbanes-Oxley Act and Email Security”*)

Gartner Inc. observes companies taking a tactical-ultimately costly-approach to SOX compliance. "Enterprises that choose one-off solutions for each regulatory challenge they face will spend 10 times more on compliance projects than their counterparts that take a proactive approach," says French Caldwell, research vice president at the Stamford, Conn.-based research and consulting firm.⁸

⁸ “Sarbanes-Oxley Compliance Looms”, Insurance Networking News, June 1, 2004

III. The Consequences Of Insecure Communications

Although government regulations to secure sensitive information have caught the media’s attention, there are various forms of unregulated sensitive data being transmitted from and within an organization that could be putting a company in legal and/or moral jeopardy.

The following table highlights a variety of scenarios in which sensitive information is being transmitted from various groups/departments within an organization—it further outlines the consequences that may come from these insecure communications if best practices are not applied.

Group or Department	Scenario and Consequences
Entire Organization	<ul style="list-style-type: none"> • Unauthorized disclosure of information to be kept confidential under a nondisclosure agreement leads to legal action against the company. • Communications that may cast other parties in an unfavorable light falling into the wrong hands may also lead to lawsuits against the company. • Communications that may be misinterpreted may fall into the wrong hands and lead to lawsuits against the company by employees or whistleblowers. • Unauthorized disclosure of trade secret information can lead to the loss of the value of the trade secret, loss of business competitive advantage, and inability to obtain legal relief under trade secret law.
Accounting /Finance	<ul style="list-style-type: none"> • Compromised confidentiality and integrity of financial records that will be used for the basis of reporting to the SEC directly (public companies – SoX liability) or indirectly (private company subsidiaries of public companies or possible acquisition targets). • Exposure of sales and other financial projections classified as trade secrets
Business Development/ Strategic Planning	<ul style="list-style-type: none"> • An organization must prevent advance knowledge of mergers and acquisition, in order to prevent insider trading and premature disclosure of M&A activity. • Business plans for acquisitions and strategic planning can be trade secrets of the company. Companies must protect against unauthorized disclosure.
Communications (producing marketing materials)	<ul style="list-style-type: none"> • Communication of native images for marketing materials may lead to unauthorized disclosure and copying. If copying takes place, the company may need to take expensive legal action to stop it.
Communications/	<ul style="list-style-type: none"> • In the event of a corporate disaster, it is essential that the

Group or Department	Scenario and Consequences
<p>Governmental Relations</p> <p>Communications/</p> <p>Governmental Relations (cont.)</p>	<p>disaster response team be able to communicate confidentially to ensure a single voice speaks for the company and prevent unauthorized disclosure of internal non-public communications.</p> <ul style="list-style-type: none"> • Communications from company officials may be used against the company in legal proceedings. Thus, companies should strive to keep communications confidential to limit disclosure to authorized recipients.
<p>Consulting Services</p>	<ul style="list-style-type: none"> • Unauthorized disclosure of confidential information of client. See “Entire Organization” above.
<p>Customer Service</p>	<ul style="list-style-type: none"> • Unauthorized disclosure of customer records following a security breach may lead to lawsuits or enforcement actions against the company. Governmental enforcement actions can come from the Department of Health and Human Services (health records), a banking or insurance regulator (financial services customer records), the Federal Trade Commission (violation of privacy policies, non-banking financial services providers), and state attorneys general (unfair and deceptive trade practices). Private plaintiff lawsuits can stem from customers whose records were compromised under California AB 1950, state unfair competition laws, and state consumer protection laws.
<p>Engineering/Research and Development</p>	<ul style="list-style-type: none"> • Research, technology, know-how, and code developed by engineering and R&D are trade secrets of the company. They must prevent unauthorized disclosure to preserve the value of these trade secrets.
<p>Executive Management</p>	<ul style="list-style-type: none"> • Management must prevent unauthorized disclosure of strategic plans or important favorable or unfavorable news that is “material nonpublic information” in order to prevent insider trading and premature disclosure of M&A activity.
<p>Financial Services Operations</p>	<ul style="list-style-type: none"> • Customer records must be protected from unauthorized disclosure. • Operations will want to tie online activity of customers to particular financial transactions and user agreements, through controls on integrity and strong authentication, such as through digital signatures. E.g., Secure email or IM transactions in the future.
<p>Health Care Operations</p>	<ul style="list-style-type: none"> • Patient records must be protected from unauthorized disclosure to comply with HIPAA.

Group or Department	Scenario and Consequences
Human Resources	<ul style="list-style-type: none"> • Employers have an obligation to keep certain kinds of information about employees and job candidates confidential. • Employers may have an obligation to keep info confidential, including background check results, HIV test results, images (fingerprints and photos), and polygraph test results. • Unauthorized disclosure of private information may lead to lawsuits. • Employers will want to protect employment review and performance information from unauthorized disclosure.
Information Technology /Security	<ul style="list-style-type: none"> • Communications concerning security assessments, network topography and configuration, and vulnerabilities is sensitive information, and a compromise of the information may lead to attacks exploiting security vulnerabilities. • Security breaches exploiting vulnerabilities and using the company’s systems as a platform to attack “downstream” systems of others may open the company to liability from downstream victims.
Insurance/risk management	<ul style="list-style-type: none"> • If the company provides insurance, customer records must be protected from unauthorized disclosure. See Financial Services Operations above. • Actuarial information gathered at considerable expense to the company can be company trade secrets. The company will want to prevent unauthorized disclosure of such information. • A compromise of risk management information concerning security vulnerabilities may lead to security breaches. See Information Technology/Security above. • Risk management information concerning the company’s failings and wrongful conduct, placed into the wrong hands, can be used against the company in legal proceedings.
Legal Department	<ul style="list-style-type: none"> • Attorneys have an ethical obligation to preserve the confidences of their client (here, the company). They must take reasonable care to avoid the unauthorized disclosure of confidential data. • Information concerning the company’s failings and wrongful conduct, placed in the wrong hands, can be used against the company in legal proceedings. (Note that when lawfully requested, the company may have an obligation to disclose adverse information to opposing parties.)

Group or Department	Scenario and Consequences
Sales and Marketing	<ul style="list-style-type: none"> • Sales forecasts, sales and marketing plans, marketing requirements documents, and other planning documents may be trade secrets of the company. The company will want to prevent unauthorized disclosure of these documents as they are communicated.

IV. The Voltage Privacy Management Platform

Email is now the medium of communication for businesses around the world and has become the trusted communication channel for a wide variety of commercial transactions and private communications. However, email security vulnerabilities do exist and create the risk of the unauthorized disclosure, loss, destruction, and/or corruption of business critical data. Malicious code, including viruses, worms, Trojan horses, and various formats of spyware, may infect workstations leaving code allowing for unauthorized access or tampering of confidential records at a later date. In addition a deluge of spam may overwhelm corporate email servers, reducing the effectiveness and availability of this vital resource. As email security vulnerabilities prevail, corporations are looking for appropriate measures to protect this sensitive information.

The traditional infrastructure used to protect data and communication based on digital certificates, commonly called Public Key Infrastructure (PKI), was not designed to deal with inter-enterprise communications, let alone the massive volume of communication from an ever-growing variety of connected devices that has become commonplace in the Internet-enabled era. Implementations in Fortune 1000 organizations have shown that not only do PKI systems have a high barrier to use, leading users to eschew them, but also they are difficult for administrators to manage. Plus, the high cost is often too difficult for a CIO to justify deployment of a PKI solution.

Other approaches to email security have had little impact, either due to the complexity of using them or because of their scalability characteristics – having to manage keys for millions of messages a day or maintain parallel messaging infrastructures. What is needed is a platform that provides high security, management of security policies and usability that is orders of magnitude better than what is available from secure messaging vendors today. *(A more in depth review is available in the Voltage White Paper “Email Security - The Identity-Based Encryption Advantage: Overcoming the hurdles of PKI, symmetric and web-based messaging”)*

Voltage Security, Inc. provides a privacy platform that secures all trusted business communication. Based on a breakthrough encryption technology called Identity-Based Encryption (IBE), Voltage Security enables today’s enterprises to conduct secure, scalable communication to not only meet regulatory requirements, but to control costs and reap significant business benefits. *(A more in depth review is available in the Voltage White Paper “Voltage Security Platform Architecture”)*

V. Conclusion

While regulatory compliance continues to add pressure to already strained budgets and mounting end-user requirements, many organizations view them as an opportunity to improve systems and upgrade infrastructure to stay ahead of the competition. Moreover, as highlighted, the cost of not adopting new technologies to help secure business communication may have wide reaching consequences far beyond those of regulatory compliance.

About Voltage Security

Voltage Security is a new information security company focused on developing innovative solutions to address the challenges of securing business critical communication. Voltage is the first to use identity to bring confidence to business communication. Voltage solutions make anytime, anywhere business communication easy to use and painless to deploy. Voltage Security is based in Palo Alto, California.

For more information, please visit www.voltage.com, email info@voltage.com or call +1 650 543 1280