

When Pressing the “Send” Button Leads to Legal Liability

Email Security and Regulatory Compliance

Table of Contents

- 1** Importance of Compliance
- 2** Overview of Key Regulations
 - 2** Sarbanes-Oxley Act (SOX)
 - 3** Health Insurance Portability and Accountability Act (HIPAA)
 - 4** Gramm-Leach-Bliley Act (GLBA)
- 5** How Email Security Addresses Compliance
 - 6** Step 1. Examine
 - 7** Step 2. Determine
 - 8** Step 3. Deliver
 - 9** Step 4. Reporting/Documentation
- 10** Summary



Introduction: The Importance of Compliance

Compliance is an issue that can no longer be ignored. Regardless of whether a company is large or small, in a regulated industry or not, the impact of regulations in both the US and abroad is being felt by IT professionals in every corner of the world. Since the announcement of HIPAA in 1996, increasingly onerous regulations and the requisite process, technology and reporting improvements have forced organizations to take a hard look at how private information is managed and stored, ensuring that only the proper individuals or systems have access to private information.

There are many entry and exit points for sensitive information in a typical organization. But none is more pervasive than email, which has emerged as a prevalent method of communication with customers and trading partners alike, increasing efficiency and improving operations. Unfortunately, now sending confidential and/or private information (and the resultant compliance violation) is now as easy as hitting "send."

The good news is that many companies have already embraced an email firewall to help eliminate security issues (spam, viruses, infrastructure attacks) surrounding incoming e-mail. Fortunately the email firewall can also act as the last line of defense for a company, inspecting and applying complicated compliance-oriented policies to outgoing email. This can make the difference between what is and what is not a violation. Once sensitive content travels outside of the boundaries of an organization, it becomes a violation. The email security gateway can stop violations before they occur and help to control an organization's liability.

Despite all the efforts to come up with a simple and complete answer to solving the compliance "problem", it is important to note:

1. There is no panacea – Compliance is both broad and complicated, so no one product provides a total solution. A combination of process, policy, and technology is required to get there.
2. No one really knows what is "good enough" – There have been very few enforcement acts for any of the high profile regulations (SOX, HIPAA, GLBA), so we are largely dealing with speculation as to what is good enough to meet the spirit of the regulation. While it may seem obvious that things like access control and encryption are key parts of any compliance solution, without the legal precedent to truly prove this fact, at this point true lasting requirements are not clear.

The BorderWare MXtreme™ is an email security, privacy and compliance solution that addresses key aspects of compliance requirements as they relate to email. This whitepaper provides an overview of the key regulations and how BorderWare enables organizations to enforce and demonstrate compliance.

Overview of Key Regulations

Sarbanes-Oxley Act of 2002 (SOX)

SOX was initiated as a result of the significant and severe corporate malfeasance of organizations like Enron, Adelphia and WorldCom, as a way to ensure there are significant penalties for corporate officers that commit fraud. The spirit of the regulation is to ensure the validity of financial statements by insuring that proper financial controls are in place.

Every public company that trades in the US is subject to SOX compliance. Large companies were required to be compliant for their fiscal year ending after November 2004, and smaller companies (with market caps < \$75 million) had until April 2005 to become compliant. To date, over 5000 companies have filed their SOX statements with the SEC.

As with all the other regulations, the legislation does not dictate specific technologies or practices, rather stating the required outcome. Yet the SEC (the main enforcement entity for SOX) has stated that a standard list of internal controls assembled in 1992 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) "satisfies their criteria." Yet COSO has very little to say on IT issues, so organizations have been relying on the set of "Control Objectives for Information and Related Technology" published by ISACA otherwise known as COBIT.

SOX AT A GLANCE

WHAT	Ensure financial statements are valid through tight internal controls
WHO	All US publicly traded companies
HOW	Authentication, anti-virus, encryption
WHEN	SOX went into effect in Nov 2004 or April 2005 (companies < \$75 million market cap)
PENALTIES	Jail time for executives, significant fines

From an information security standpoint, COBIT requires organizations to:

- Safeguard information from unauthorized use, disclosure, modification, damage or loss
- Assure that electronic transactions are authorized and authentic
- Have strong processes to issue and manage user credentials
- Prevent an exposure of data due to malicious software
- Ensure systems meet performance and availability requirements

The ramifications of not complying with SOX are severe, ranging from heavy fines to jail time for corporate executives. As a result, every public company (and those contemplating going public) take SOX very seriously and it is important to understand how email security can assist their compliance efforts.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA mandates the privacy and security of protected health information (PHI). The HIPAA security rule was published in May 2003 and subject to enforcement for all covered entities starting in April 2005. Given the productivity gains for healthcare professionals to communicate with patients and other doctors via email, healthcare organizations need to leverage real-time communications but do so securely.

Covered entities consist of healthcare providers, health plans (insurance, etc.) and healthcare clearinghouses (claims and transaction processors). Service personnel (accountants, lawyers, etc.) working on behalf of the covered entities are also subject to HIPAA requirements.

NIST (National Institute of Science and Technology) has published an information security guide that many believe will meet the requirements of HIPAA. This guide (An Introduction to Computer Security: The NIST Handbook) provides all the detail an organization needs to understand the scope of their compliance efforts.

To better understand the outcomes that HIPAA requires, at a high level covered entities must:

- Have a documented process to protect PHI and detect/correct security violations
- Only authorized personnel have access to PHI
- A process to respond in the event of a security breach
- Organizations periodically evaluate their ability to protect PHI

HIPAA AT A GLANCE

WHAT	Protect confidential healthcare information
WHO	Healthcare providers, health plans, healthcare clearinghouses
HOW	Access control, authentication, message encryption
PENALTIES	Fines up to \$100,000 (per violation) and 10 years jail time
WHEN	April 2005, except small health plans (April 2006)

From a technology standpoint, strong cases can be made for organizations to implement:

- Access controls – to ensure the wrong people do not get access to information
- Detailed auditing of mail traffic – to track who is accessing data (and more importantly, prove it to the examiners)
- Encryption - to authenticate sender and recipient, provide protection of the message contents and ensure a message hasn't been tampered with

Gramm-Leach-Bliley Act of 1999 (GLBA)

GLBA is basically the sister legislation of HIPAA, but targeted at the financial industry, as opposed to healthcare. The essence of the regulation is to protect consumer's financial information (credit card numbers, social security numbers, account numbers, etc.) and ensure that unauthorized use or access does not happen. Every financial institution that handles consumer non-public information (NPI) is subject to the GLBA legislation. This includes banks, brokerage firms, mortgage lenders, financial planners and insurance companies (which are also subject to HIPAA).

GLBA AT A GLANCE

WHAT	Protect consumer's non-public information (NPI)
WHO	Financial institutions of all sizes
HOW	Strong authentication, server defenses, encryption
PENALTIES	Imprisonment of company officers for up to 5 years and steep monetary fines.
WHEN	In effect since 2001

GLBA breaks down protection into 3 larger contexts:

1. Financial Privacy – covers the collection and distribution of information, including how NPI is used in operations
2. Safeguards – requires that certain processes and technologies be implemented to protect collected NPI
3. Pretexting – lays out the ramifications of impersonating someone to fraudulently obtain private information

Similarly to HIPAA and SOX, GLBA does not specify technologies to implement the safeguards. Many of the techniques laid out in the NIST guide are applicable to provide GLBA compliance as well.

How Email Security Addresses Compliance

An email firewall implemented in front of an email server protects the message store from direct attack and enforces proper access control and authentication requirements inherent to the regulations. MXtreme has the ability to block infrastructure attacks (directory harvest, denial of service, etc.) and provide both strongly authenticated management access and secure web mail access makes it the foundation that drives privacy and compliance.

Once securing the email infrastructure, the 4 key steps in meeting the spirit of the regulation are:

1. **Examine** - each message passing through the gateway must be checked for private/sensitive data
2. **Determine** – based on the policies and the content discovered, determine the appropriate action to take on the message
3. **Deliver** – take the appropriate action on the message, whether it be handling the identified message in accordance with the defined policy – allow, block, encrypt, copy to compliance officer, message stamping, return to sender, audit/log
4. **Report/Document** – it is important to be able to document both the policies that have been implemented to enforce the regulations, as well as tracking actual message traffic to ensure compliance

EXAMINE	DETERMINE	DELIVER	REPORT
Examine entire message including attachments	Determine appropriate action based on policies and content	Deliver Message in accordance with defined policies – send, copy, encrypt, block	Monitor and provide reports to demonstrate compliance and identify gaps

As Illustrated in **Figure 2**, the MXtreme Compliance Engine with its pre-defined dictionaries offers out of the box capability to stop inappropriate content from being sent via email immediately. MXtreme also looks deeply into all attachment types to make sure private information is not hidden.

Dictionaries			
Select: All None		Selected Items	Remove
Select	ID	Name	Type
<input type="checkbox"/>	14765	Sarbanes-Oxley	compliance
<input type="checkbox"/>	14763	HIPAA	compliance
<input type="checkbox"/>	90	Strong OCF	ocf
<input type="checkbox"/>	89	Moderate OCF	ocf
<input type="checkbox"/>	88	Weak OCF	ocf
<input type="checkbox"/>	87	Default Spam Words	spam

Add Finished Help

Figure 2 - Predefined and customizable dictionaries

Step 1. Examine

To provide the required flexibility for compliance, the email firewall must provide pre-defined dictionaries for each of the applicable regulations. For example, having a dictionary to catch ID-9 codes (healthcare diagnosis codes) is a key component of HIPAA compliance. It is also critical to be able to customize the dictionaries for organization-specific data and formats. Finally the ability to catch universal data formats (also known as regular expressions) like social security numbers is also a requirement.

More than knowing what to look for, it is equally important to know where to look. Common places include:

- Message Headers – Who is sending the message? Who is receiving it? Supporting sender authentication and looking for header inconsistencies is important.
- Body content – What is in the message? Are there key words that violate the regulation? What about account numbers or social security information? All of this must be discovered.
- Attachments – Being able to deeply analyze attachments to look for sensitive data, regardless of the type of file or its size.

Step 2. Determine

Once the content of a message is examined, the email firewall must utilize a sophisticated policy engine to determine the appropriate action to take on the message. Policies need to be easy to set up and applicable to large groups as well as individual users, depending on their job functions and requirements. It can not be onerous to set up and manage these policies across an enterprise of thousands of users.

The policies must allow for both single and compound actions to be taken on a message. For example, a company may want to just block a message that violates the SOX policy. Alternatively it may want to both block, copy the message to the compliance officer and also return the message to the sender indicating why it was blocked. Or there may be the need to allow the message to go through, but encrypt it using a third party encryption server. Those are just a few simplistic examples of potential policies, but the policy engine must be able to support multiple options and actions.

As demonstrated in **Figure 3**, MXtreme provides a series of templates to create policies. The flexible templates also allow users and groups to be attached to the policy by either listing the user's email address, an applicable domain, or using native LDAP lookups. MXtreme policies also define the processing rules, which can be inherited from system default policies.

Select	Policy	State	Email
<input type="checkbox"/>	HIPAA	enabled	acmehealth@borderware.com

Policy: Default | Add

Upload File | Download File | Finished | Help

Figure 3 - Step-by-step guide to policy creation

Step 3. Deliver

Once the content is examined and the appropriate actions are determined, the email gateway must be able to execute the policy in an efficient and scalable fashion. MXtreme provides a number of different message actions which can be associated with any policy and can also be different depending on whether the mail is inbound or outbound. As depicted in Figure 4, these include:

1. Allow
2. Block
3. Quarantine
4. Encrypt – MXtreme supports a variety of encryption techniques, including TLS/SSL, S/MIME, PGP, and PostX
5. Copy – Message can be copied to any recipient
6. Message Stamping – A disclaimer can be added to every message to govern the use of the information in that message
7. Audit/Log – Regardless of the action taken, all message activity can be logged to prove compliance and provide documentation during a regulatory examination.

The screenshot displays the 'Attachment Scanning' configuration page. At the top, there is an 'Enable' checkbox which is checked, and a 'Define' link. Below this, the page is divided into two sections: 'Inbound Attachment Scanning' and 'Outbound Attachment Scanning'. Each section contains several configuration options, each with a 'Define' link. In the 'Inbound Attachment Scanning' section, the 'Compliancy file' is set to 'HIPAA', the 'Action' is 'Quarantine mail', 'Notify Recipients' is checked, 'Notify Sender' is unchecked, 'Notify Administrator' is checked, and the 'BCC Address' is 'compliance_officer@borderware.com'. In the 'Outbound Attachment Scanning' section, the 'Compliancy file' is 'HIPAA', the 'Action' is 'Encrypt', 'Notify Recipients' is unchecked, 'Notify Sender' is unchecked, 'Notify Administrator' is checked, and the 'BCC Address' is 'compliance_officer@borderware.com'.

Section	Field	Value	Define
Attachment Scanning	Enable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Define
	Inbound Attachment Scanning		
Inbound Attachment Scanning	Compliancy file	HIPAA	<input checked="" type="checkbox"/> Define
	Action	Quarantine mail	<input checked="" type="checkbox"/> Define
	Notification	<input checked="" type="checkbox"/> Notify Recipients	<input checked="" type="checkbox"/> Define
		<input type="checkbox"/> Notify Sender	<input type="checkbox"/> Define
		<input checked="" type="checkbox"/> Notify Administrator	<input checked="" type="checkbox"/> Define
	BCC Address	compliance_officer@borderware.com	<input checked="" type="checkbox"/> Define
Outbound Attachment Scanning	Outbound Attachment Scanning		
	Compliancy file	HIPAA	<input checked="" type="checkbox"/> Define
	Action	Encrypt	<input checked="" type="checkbox"/> Define
	Notification	<input type="checkbox"/> Notify Recipients	<input type="checkbox"/> Define
		<input type="checkbox"/> Notify Sender	<input type="checkbox"/> Define
		<input checked="" type="checkbox"/> Notify Administrator	<input checked="" type="checkbox"/> Define
BCC Address	compliance_officer@borderware.com	<input checked="" type="checkbox"/> Define	

Figure 2 - Message actions driven by policies

Step 4. Reporting/Documentation

Perhaps the most critical aspect of compliance is the ability to document and report on the processes used and the results of the safeguards are put in place to meet the regulations. Reports showing policy configuration and which messages were violations, as well as having a forensic ability to determine what happened in the event of an offense. All of the above are critical components of a market leading reporting capability.

The MXtreme compliance reports can be customized to include as little or as much detail as required. MXtreme also provides significant customization capabilities to present the appropriate data in the most applicable format.

The available reports include:

- Traffic summary (total number of messages processed, number of compliance violations) as depicted in **Figure 5**
- Most active senders and receivers of all messages processed by the policy and/or violating the policy
- A ranking of the most common words and phrases triggering compliance violations (used to fine tune appliance dictionaries)

Any compliance violation flagged by the report can be investigated using the interactive tools and event database included in MXtreme.

MAIL FILTER (acted upon)	HOUR	DAY	WEEK	MONTH
Compliance Violation	430	430	430	430
Clean or not Scanned	115	127	127	127
Total Messages	545	557	557	557
Percent Blocked	79	77	77	77

Summary

In summary, compliance is a very broad and complicated topic for organizations of all sizes in all geographies. Though no one technology or product is a panacea to comply with any of the regulations, having a strong email boundary security posture and the ability to deeply inspect all inbound and outbound mail provides a head start on the road to compliance. MXtreme 6.0 adds the capabilities that customers need to secure, examine, determine, deliver, and report on their email infrastructure, and take a major step towards compliance.

Don't wait; deploy MXtreme today to ensure your email traffic is not a regulatory liability. To contact us, you can visit us on the web at www.borderware.com/compliance, reach us at 877-814-7900 or contact your local Borderware reseller.

About BorderWare

BorderWare Technologies makes Internet communications safe. The company's content and application security solutions enable customers to mitigate the risks and threats associated with Internet communications. Founded in 1994, BorderWare has developed partnerships and affiliations with some of the industry's most prominent companies including Cisco Systems, F5 Networks, Kaspersky Labs, PGP, PostX, Research In Motion (RIM), RSA Security, Sun Microsystems and Symantec. More than 8,000 customers in 65 countries have selected BorderWare's solutions for their superior security, scalability, business continuity and lower total cost-of-ownership.



Headquarters. +1.905.804.1855 | Toll Free. +1.877.814.7900 | US Federal Office. +1.866.211.6789 | Europe. +44.20.8759.1999

www.borderware.com

About this document

This document provides general information about personal privacy and compliance initiatives in North America. It is intended to be used for resource and reference purposes only and does not constitute legal advice. Readers of this paper are encouraged to speak with their legal counsel to understand how the general issues discussed above apply to their particular circumstances. Borderware Technologies Inc. disclaims any and all liability for damages, costs, lost profits, fines, fees or financial penalties of any kind suffered by any party acting or relying on the general information contained herein.

©2006 BorderWare Technologies Inc. Any product photos shown are for reference only and are subject to change without notice. Internet Communications Made Safe, BorderWare Intercept, MXtreme, SIPassure, S-Core and related marks are trademarks of BorderWare Technologies Inc. Other product and/or company names mentioned are trademarks and/or registered trademarks of their respective holders. May 2006