

Best Practices in Messaging Security

Managing email security policy and regulatory compliance requirements in financial services, health care and public sector.

Recent activities of the U.S. Congress clearly illustrate the electronic threats to and the increased regulatory demands on businesses today. Over the last few years, the Sarbanes-Oxley Act of 2002, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act of 1999 (GLBA) and the threats highlighted by the CAN-SPAM Act of 2003 and Internet Spyware (I-SPY) Prevention Act of 2004 have driven major changes in the systems, processes and security inside organizations.

Some of these regulations are designed to stop the sources of spam, viruses and spyware. Others intend to make companies more responsible for the protection of customers' privacy and more accountable for the substance of their financial reports.

All have a pronounced affect on corporate email.

While financial services, health care and public-sector groups may be under more scrutiny than others, all organizations must protect themselves and address increasing internal and external concerns and regulations around privacy, confidentiality and financial reporting. In fact, while specific industries and larger enterprises are required by law to act on some of these regulations, companies across all industries and government agencies at the federal, state and local levels are under pressure to respond. In this paper, we address both general and industry-specific business regulations and how they impact an organization's email system.

EMAIL TOUCHES THE HEART OF YOUR ORGANIZATION

Email is about more than just sending messages. In addition to being the most important electronic communication medium inside and between organizations, it is often the primary groupware, personal information manager, and file-sharing system for workers. While some emails contain simple messages much like those that could be given quickly in

person or over the phone, many emails contain valuable company content. Also, unlike a telephone or in-person discussion, email lives on over time.

In fact, a company's email taken in aggregate probably contains fundamental parts or traces of just about everything important to the company. Specifically, these messages almost certainly include non-public information which may be subject to governmental regulations like HIPAA, confidential company information such as internal memos or revenue projections, and for larger companies, content pertaining to financial reporting that is subject to Sarbanes-Oxley or GLBA requirements.

While the primary home of most of this important content is not email (although some employees do use their mailboxes as filing systems), the information finds its way into the email system as employees communicate with each other or others outside the company. Organizations must take notice when this information is found in outgoing email. Of course, incoming messages that contain threats to security and productivity—including viruses, spam and phishing emails—must also be addressed.

Unfortunately, unlike other applications and systems in your company that have well-defined authentication and access-control restrictions, email has been mostly unrestricted, with users able to send any message they want with any content they want to any person they want. For many companies email is an uncontrolled communication medium where unmanaged business activity—and in some cases, dangerous messages—can go on, unchecked. Companies are coming to recognize how important it is to manage, protect, audit, and control incoming and outgoing email.

The email situation somewhat resembles the state of legacy applications prior to the year 2000. Y2K forced companies to address their legacy applications and fix problems related to using short year notations. While fixing that problem, companies found they



needed to fix many other application issues as well. The result, by most accounts, was an increased understanding and better use of the existing applications.

In the same way, the monumental increase in spam volume in recent years has focused attention on email. Companies are now finding email security to have broader implications. In addition to spam, viruses and Trojan horses, a host of industry, state, federal and international regulations are forcing corporations to upgrade their email security to meet acceptable standards.

EMAIL SECURITY MANDATES

In addition to spam, organizations should focus on the key business concerns around email that can be addressed by email security, outlined below.

Protection of Non-Public Information

Non-public information (NPI), specifically that related to customers' personal, financial or health information has come under the scrutiny of international, federal, state and industry agencies. The European Union's (EU) Privacy Directive, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), the U.S. government's Gramm-Leach-Bliley Act and California Assembly Bill 1950 (AB 1950) all address customer privacy protection.

Each approach differs in breadth and specificity, and the regulations are often a bit nebulous, although clarification has come over time as findings, case law and interpretations emerge. However, in all cases, to meet the requirements, companies must address the danger of passing along private information knowingly or unknowingly within emails.

What is considered non-public information depends

on the regulation and the industry. For example, the Graham-Leach-Bliley Act of 1999 protects consumers' financial information and is directed at financial institutions. It puts processes in place to control the use of consumers' private information and includes requirements to secure and protect the data from unauthorized use or access.

California's AB 1950 specifically protects an individual's last and first names in combination with their social security number, driver's license number, account or credit card numbers, or medical information. HIPAA protects patients' personal health information from being shared without their consent.

Email protection requirements for NPI come in two forms:

1. Outgoing email content can be checked for NPI and appropriate action taken. Some of these checks can be performed with standard dictionaries and simple pattern matching such as customer names or privacy key words. Other checks require more sophisticated algorithms that understand the specific data formats of financial constructs such as social security numbers, ABA routing numbers, or credit card numbers; and industry-specific data like treatment codes from the American Medical Association or disease codes from the Centers for Medicare and Medicaid Services.

It is important to choose an email security solution that has sophisticated filters that can rapidly analyze outgoing email for all of these specific industry data types.

2. Second, the transmission of NPI to partners must occur over an encrypted link. This can be done through email transmission security or through specialized products designed to encrypt the contents of an email message.

In all cases, centralized management, reporting and auditing are desirable and typically required by one or more industry regulations.

CONFIDENTIAL INFORMATION

While companies are required by law to protect customer information, they are also very interested in protecting their own confidential information. Employees may inadvertently and sometimes purposefully leak internal memos, proprietary secrets, or new product information to the public, competitors, or the press through email.

Understand that many trespasses with respect to confidential information are not done with malicious intent. It's easy to make a mistake and send an email to the wrong person. For example, many email clients, including Microsoft Outlook, have an auto-complete feature when entering a recipient's email address.

NON-PUBLIC INFORMATION CHECKLIST

1. Define the NPI that must be managed in your company, industry and countries where you do business.
2. Identify all data stores, documents and applications containing non-public information on customers.
3. Identify all data stores, documents and applications containing confidential information.
4. Identify where combinations of identification (e.g., last name, first name) and personal information (e.g., social security number, credit card numbers) are kept.
5. Identify partner companies with which you share NPI.
6. Identify policies and procedures you will enforce around NPI.
7. Define your reporting and auditing approach around NPI.
8. Define your periodic review process designed to keep your policies and procedures up-to-date with current conditions.

Employees might accidentally send along confidential information to a third party without even knowing it if auto-complete is enabled, or if they select “reply to all” rather than simply “reply.”

While a phone call or outside discussion cannot be stopped, a content-rich email with supporting company documents can often be more dangerous in the wrong hands. In addition, companies want to protect against the transmission of inappropriate language through their email systems. These kinds of emails—sent by disgruntled or ignorant employees—can increase a company’s liability and expose it to potentially damaging lawsuits.

Confidentiality breaches and inappropriate content can be caught at the perimeter through filters set on the email recipients, email body content and email attachments. A flexible email security solution will allow an organization to create policies based on recipients and content. For example, the policy might block all internal memos to the outside, but allow employees to send new product information to a partner marketing firm. In the end, confidentiality starts with putting policies in place and educating employees. It won’t prevent breaches altogether, but it will help to raise awareness about the potential severity of even an accidental breach.

FINANCIAL REPORTING

The Sarbanes-Oxley Act of 2002 has arguably garnered the most attention of all regulations. This is primarily due to the publicity surrounding various public accounting scandals, as well as the very personal requirements on and potential penalties against CEO and CFOs. U.S. public companies with a market capitalization of \$75 million or more are required to comply for fiscal years ending on or after November 15, 2004. All others are required to comply for fiscal years ending on or after April 15, 2005.

Sarbanes-Oxley requires that companies identify and document the processes employed to collect information used to build their financial reports. It says that the company’s financial leadership—the CEO and CFO—must review annual and quarterly financial reports to ensure the information is complete and correct. These reports must have effective disclosure controls and procedures and must define and explain how financial information is stored, managed and communicated. Sarbanes-Oxley also requires that external public auditors review these procedures.

Since email is such a common communication tool, any sane Sarbanes-Oxley plan must include the management of the corporate email system along with the incoming and outgoing emails themselves. An email

security solution along with well-defined processes can go a long way toward meeting Sarbanes-Oxley communication requirements. Email sent around end-of-quarter or end-of-year financial preparation should be monitored and audited. Companies should also archive email relevant to financial report generation.

SECURITY AND PRODUCTIVITY THREATS

While regulations have forced companies into action around customer privacy, other regulations addressing the sources of spam, viruses and spyware problems have not been as successful. Companies must take their own actions to combat the increasing threats posed by messages containing this rogue content and to stop directed denial of service and directory harvest attacks on their email systems.

Security and productivity threats attack the foundation of an email system by increasing the negative impact of email. Email-borne viruses can bypass corporate firewalls and attack desktop machines that may not have the latest virus definition update. Once the intruder gains a foothold, a Trojan horse contained within many viruses can launch further attacks from inside the company. These attacks can compromise or destroy an organization’s data. And spam, if left unchecked, can paralyze email users with mailbox noise that decreases productivity and sometimes leads users to turn away from email.

While companies are on their own to determine the right approach to this problem, some guidance exists. The ISO Security Standard (ISO 17799), an international standard addressing general security with sections affecting email, and the Federal Information Security Management Act of 2002 (FISMA), targeted at government projects, have compliance recommendations and requirements. In some cases, such as when doing international business, a company may be asked to meet ISO recommendations, and government agencies will need to address FISMA compliance when implementing email security.

Email administrators must address these threats at the perimeter before they affect end users or internal mail servers. A perimeter email security solution can stop directed attacks, remove viruses and stop spam while letting legitimate messages through.

LESSONS LEARNED IN VERTICAL INDUSTRIES

All organizations must address the issues above, but certain highly regulated industries like financial services and health care put additional restrictions on member companies. In addition, the public sector has added pressure that comes from its own regulations and its position in the public eye. Even if you aren’t

in government or one of these industries, read on, because similar regulations to those found here will likely trickle down to your industry sometime soon.

Financial Services

With financial service companies increasing their offerings and their audience, email has become an important sales (offering notice, new investment vehicles) and customer service (confirm trades, account changes, service updates) tool to reduce costs and increase the effectiveness of client interactions. Email also plays a vital role for communications within financial services companies—to send around stock reports, investment performance and news updates, for example.

When it comes to the regulation of money, everyone takes notice. In the financial services industry, international and federal regulations like the Basel II Accord governing business continuity, risk management and bank supervision and the Gramm-Leach-Bliley Act addressing customer privacy stand alongside more focused regulations from the New York Stock Exchange (NYSE), National Association of Securities Dealers (NASD) and requirements from the U.S. Securities and Exchange Commission (SEC) to create an overabundance of electronic dictates.

With the deregulation that has occurred over the last several years in the financial services industry, companies must still pay close attention to existing and new regulations. NASD has numerous regulations that restrict how financial services firms can sell and market investment offerings. The SEC publishes guidance on the use of electronic media by operating companies, investment companies and municipal securities issuers, as well as market intermediaries. The SEC restricts forward-looking statements during certain time periods and enforces quiet periods that restrict what a company can say publicly after it files a registration statement.

In order to meet the mesh of requirements, companies must deploy a centralized email security solution that can monitor inbound and outbound communications. In addition to protecting customer information, financial services companies must monitor and stop zealous sales people from sending email that might be interpreted as breaking NASD rules. In addition, companies must create discrete policies to control email communications during quiet periods and around SEC filing periods.

Health Care

Any discussion of email security in the health care industry starts with the Health Insurance Portability and Accountability Act (HIPAA). Health care has tra-

ditionally been a paper-based industry, with patient records and health insurance forms completed manually. However, with tightening regulations brought about by HIPAA around patient privacy, and increasing competitive pressures, health care providers have implemented new electronic systems rather than incurring the enormous costs of patching antiquated records systems. With the move to electronic information, email has become a more important communication medium inside companies and among health care providers, insurance companies and patients.

There are many potential applications. Email can be an excellent means for the electronic exchange of health-related information such as patient records, medical images and referral assessments. Electronic medical information systems with access to comprehensive medical records can alert care givers via email when critical health factors are uncovered. Email and other electronic applications can significantly decrease the costs associated with patient management issues such as appointment scheduling, referrals, invoicing and billing workflows.

Email security must honor the protection of patient health information. The typical requirement is that communications with business partners (that contain protected health information, or PHI) be handled via encryption. Email destined for other recipients should not contain patient health information. The email security solution should search the body of the message for occurrences of patient names along with related health terms. To keep up with the ever-changing health codes, email solutions should have dynamically updated dictionaries that define common protected health information code sets—such as AMA treatment codes and CMS disease codes. This will simplify HIPAA compliance and protect against patient or class-action lawsuits.

Public Sector

E-government initiatives abound as government agencies attempt to leverage new breakthroughs in data and communications technology. While many of these projects involve portals for better customer service to constituents, some efforts have also leveraged email as a way to contact individual citizens or large groups. The government must constantly talk to its citizens for many reasons. For example, the Freedom of Information Act compels federal agencies to disclose records requested in writing by any person. This can be done effectively in many cases using email. Interagency communication is also more important than ever, as evidenced at the highest levels in our homeland security efforts as the CIA, FBI and other security teams come together electronically. Email

was born in the academic, scientific, and military communities because collaboration leads to better results. Now, even the more traditional government agencies are using email.

The Federal Information Security Management Act of 2002 (FISMA), created by the National Institute of Standards and Technology (NIST) requires federal agencies and their partners to establish consistent, risk-based security programs. While FISMA does not call out email directly, its parts address the oversight and management of information security risks, which certainly includes those risks posed by email. FISMA leaves the selection of specific solutions in the hands of individual agencies.

The public sector has perhaps even greater email security needs than public companies. Government is a high-profile target and local, state and federal agencies remain quite visible as an indicator of stability. Attacks on government Web sites have been front-page news whenever they occur. Even academic institutions have been hit recently. For example, a research group at U.C. Berkeley fell prey to an attack that might have compromised a large number of social security numbers. Trust and confidence are key issues for police, fire and those in the public eye—especially in the face of emergencies. Public communication can be compromised by breaches emanating from security lapses, viruses or excessive spam.

Email security solutions must protect the email systems used by government agencies and universities and the email sent through them. All solutions must be assessed based on FISMA compliance. Government agencies should monitor the content of all outgoing email, especially messages being sent to large groups of constituents, since inappropriate or disturbing email from a government sender will have a pronounced impact.

THE PROOFPOINT SOLUTION

Proofpoint provides messaging security solutions for large enterprises, universities and government agencies. The company offers comprehensive solutions for both inbound and outbound email so organizations can stop spam, protect against viruses and shield mail servers from denial of service and directory harvest attacks. Simultaneously, outbound email is monitored to protect digital assets and comply with external regulations and internal corporate policies regarding private information. Proofpoint's solutions—the Proofpoint Protection Server® software and Proofpoint Messaging Security Gateway™ appliance—employ Proofpoint MLX™ machine learning technology to accurately identify and classify all types of email content. Proofpoint MLX employs advanced

statistical techniques to deliver adaptive protection to defend against emerging threats.

Proofpoint offers modular defenses to address all types of inbound and outbound messaging threats—including spam, viruses, content compliance, digital asset protection and regulatory compliance—for both general business and highly regulated vertical industries. All Proofpoint modules include powerful monitoring, auditing and reporting capabilities so managers and auditors can monitor and reveal performance and trends over time concerning spam, viruses, confidential information and regulatory compliance.

All modules are available as components of the Proofpoint Messaging Security Gateway and Proofpoint Protection Server.

PROOFPOINT SPAM DETECTION™ MODULE

The Proofpoint Spam Detection Module is the only enterprise messaging protection solution based on advanced machine-learning techniques. The techniques—developed by researchers and scientists at Proofpoint's anti-spam laboratory—block the most spam, including phishing attacks, with the least number of false positives by examining more than 100,000 email attributes. The solution identifies new types of spam and other malicious messages immediately, unlike traditional anti-spam tools that rely on humans to detect spam manually and encode new rules.

PROOFPOINT VIRUS PROTECTION™ MODULE

The Proofpoint Virus Protection Module allows enterprises to combat the virus threat effectively and efficiently using enterprise-grade virus protection. Leveraging the efficient message handling and robust management services of the Proofpoint processing platform, this solution offers integrated administration, automatic updates, high-performance message analysis and flexible anti-virus policy management.

PROOFPOINT REGULATORY COMPLIANCE™ MODULE

The Proofpoint Regulatory Compliance module makes it easy to ensure that outbound messages comply with many different types of email-related regulations, including HIPAA and GLBA. Pre-defined dictionaries and “smart identifiers” automatically scan for a wide variety of non-public information including PHI (protected health information, as defined by HIPAA) and PFI (personal financial information as defined by GLBA) and let you take appropriate actions on non-compliant communications.

A variety of pre-defined dictionaries are included with Proofpoint Regulatory Compliance. These dictionaries define common protected health information code sets—such as AMA Treatment Codes, CMS Disease Codes, NDC Drug Codes and others—to simplify HIPAA compliance. New dictionaries can be also be defined. These dictionaries can support both exact matches as well as regular expressions, which provides the ability to capture important content that might evade exact matching techniques. The Proofpoint Dynamic Update Service™ ensures that installed dictionaries are always up-to-date with the latest codes.

Messages that are identified as containing NPI can be handled using any of Proofpoint's standard message dispositions including redirect to an encryption device (see below), quarantine, reject, annotate or discard, among many other options.

Many privacy regulations specify that non-public data must be transmitted in a secure or encrypted format. Proofpoint Regulatory Compliance supports TLS (Transport Layer Security) and third-party secure messaging solutions.

PROOFPOINT DIGITAL ASSET SECURITY™ MODULE

The Proofpoint Digital Asset Security module keeps valuable corporate assets and confidential information contained in the body of an email or in its attachments from leaking outside your organization via email. It uses patent-pending Proofpoint MLX machine-learning technology to analyze confidential documents and keep them from leaving your organization via email. It uses some of the same advanced statistical techniques applied in Proofpoint's industry-leading anti-spam engine—widely acknowledged as one of the most accurate systems available.

Companies can flexibly handle different content categories. A graphical user interface lets you define document categories such as internal memos, draft press releases, organizational charts, price lists, and so forth. Each category can have its own level of protection (stop internal memos and monitor organizational charts, for example). Proofpoint Digital Asset Security can be used to secure nearly 300 types of documents including text, Microsoft Word, Microsoft Excel, Adobe PDF, Microsoft PowerPoint and compressed formats include zip, gzip, and TAR files.

The Digital Asset Security module is trained to recognize document patterns by the loading or emailing of representative documents by authorized personnel. Putting documents into the system “trains” the module to recognize that document and portions of its contents.

Messages that are identified as containing confidential information can be handled using any of Proofpoint's standard message dispositions including quarantine, reject, annotate, redirect, reply to sender or discard, among other options. For example, an outbound message containing portions of a confidential memo can be quarantined and flagged for review by the appropriate manager.

PROOFPOINT CONTENT COMPLIANCE

The Proofpoint Content Compliance™ Module allows enterprises to define and enforce acceptable use policies for message content and attachments. Proofpoint Content Compliance can be used to identify and prevent a wide variety of inbound and outbound policy violations including offensive language, harassment, file sharing and violations of external regulations. With the Content Compliance Module, companies can define policies such as monitoring offensive language, enforcing maximum message size or limiting attachment types. For example, an outbound message containing offensive language can be returned to the sender for review and modification.

CONCLUSION

Today's regulatory environment—combined with increasing competitive and economic pressures—demands that corporations address internal and external concerns around privacy, confidentiality and financial reporting. A comprehensive plan must include enterprise messaging system security.

The Proofpoint Messaging Security Gateway and Proofpoint Protection Server software offer a complete email security solution for large enterprises, universities, and government agencies. Proofpoint's MLX technology and targeted modules help organizations in vertical industries such as financial services, health care and the public sector address the specific regulations and confidentiality concerns affecting them. Given the pervasiveness of email throughout business today, it is imperative for all organizations to ensure that their email security solution can combat the threats as well as help them to comply with government and industry regulations.

MORE INFORMATION

For more information about Proofpoint's messaging security solutions, please visit www.proofpoint.com or call +1 408-517-4710.

Proofpoint, Inc.
10201 Torre Ave, Suite 100
Cupertino, CA 95014