

Regulations Shift Focus on Outbound Email Security

The Impact of HIPAA, PCI, PIIG, and Other New Government and Industry Guidelines on Email Security Policies

Introduction

Email is the lingua franca of business today. It is the conduit that allows employees to share information, companies to work with partners, and increasingly, provides a way for companies and their customers to interact. Enterprises today deal with an ever-increasing number of email-related threats. Most are familiar with the problems of virus-infected email attachments and productivity-draining spam, but now companies must also address the threats posted by outbound email.

Outbound email and other electronic communications (such as web-based email, blog postings, FTP and other messaging streams) pose a significant risk for data loss or data leakage. Mitigating such risks is becoming increasingly important and complex with the introduction of new information privacy and data protection regulations that cover information exchanged internally, as well as with partners and customers. For example, the relatively new Payment Card Industry (PCI) Data Security Standard (DSS) and the Office of Management and Budget (OMB) Personally Identifiable Information Guidelines (PIIG) place additional constraints on how data is stored, processed, and transmitted.

Compliance with these types of regulations—or simply adopting best practices for protecting the sensitive or private information valued by your company, customers, employees and partners—adds a relatively new twist to email security. Sure, one must still be vigilant against inbound threats, but now outbound mail needs to be examined to be certain there is no data leakage. This often involves setting up corporate data protection and privacy policies, encrypting confidential corporate and private personal data, adopting best practices to ensure the policies are used, monitoring for compliance, and demonstrating (to regulators and security auditors) that procedures are in place and working.

Whatever solutions are selected, they must be easy to deploy and manage. Otherwise, they will not be used. For example, a hard-to-use encryption solution will encourage users to send information in plain text. Similarly, solutions must not prevent or obstruct busi-

ness from taking place. In particular, a solution must be accurate so that it does not block mission-critical and authorized email from getting through.

To meet these criteria, companies often employ a combination of security solutions, practices, and procedures. This white paper will examine the new email security and compliance challenges and ways to address them.

Outbound Email Becomes a Concern

Traditionally, most email security and protection solutions have focused on inbound threats. But increasingly, organizations find that they must also address outgoing mail, too. In fact, nearly one in five outgoing emails (18.9%) contains content that poses a legal, financial or regulatory risk, according to a 2007 survey of email decision-makers at 308 large U.S. enterprises (conducted by Forrester Consulting on behalf of Proofpoint).

Respondents to the survey say that the most common form of non-compliant content is email that contains confidential or proprietary business information. Unfortunately, there are several ways such information can be leaked.

Executive Summary

- New state, federal, and industry regulations are placing additional burdens on IT staffs when it comes to ensuring the protection of private and confidential information
- Companies face increased exposure to fines, penalties, and litigation due to employees unintentionally or maliciously sending information out of the company via email
- Outbound mail must now be checked; however the task is increasingly difficult as employees use personal Web-based email and their own freely downloaded encryption
- IT departments need a way to automate the detection and protect of confidential and private outgoing information
- Solutions must include easy to use, policy-based encryption to make it simple to securely communicate with customers and partners

First, there is the malicious user intent on stealing intellectual property, confidential company information, or customer records. Such behavior is a growing concern. A 2006 *eWeek* article cited a study by the Ponemon Institute that found the “loss or theft of intellectual property came in first in terms of risk, reputations and cost to the organization.”

Disgruntled employees intent on stealing information have many options. They could send a spreadsheet as an email attachment or copy information from a database and paste it into the text of a message. Such employees could use a free Web-based email account or an instant messaging service to try to circumvent scans of corporate email. They could also encrypt information using a third-party solution downloaded from the Internet to hide its content.

Second, data leakage might simply occur by accident. For example, one common problem is for a user to send an email message with confidential or customer information to the wrong person. Imagine a harried employee trying to get a number of things done at once. He or she composes a message intended for a particular person or group of people and in the rush to type in the recipient’s names in the address line, Outlook automatically completes the name. To speed things along, the user simply presses “Enter” to accept the full name, but it turns out the first listing in Outlook is “Mark Smith,” when the message was really intended for “Marks, Joe,” who appears farther down the list of choices.

Along similar lines, a group email address might contain members who no longer should have access to certain information. A 2006 issue of the New Zealand magazine *NZBusiness* noted an example of an employee who had left for a competitor yet was still getting confidential information from his previous employer. The company was “unknowingly still copying email to the ex-employee’s private email address,” according to the article.

The most common source of data loss, however, is caused simply by employees trying to do their jobs—but doing so in a way that ignores company IT policies or bypasses normal IT controls. For example, this is the case when users forward their email to a Web-based. The problem with this approach is that the users are sending their email unencrypted, complete with attachments, to a Web mail service, such as those provided by AOL, Google, MSN or Yahoo!, where it sits on public servers and could potentially be accessed by unauthorized parties.

Some users forward their email in this manner simply to have access to it while they are working at home. For example, doctors have been known to email patient record information to their home email addresses to be

Is Your Company Contributing to the Spam Problem?

Another important concern about outbound email traffic has to do with spam. Most companies are used to dealing with incoming spam, but increasingly, hackers are compromising systems and using them to send spam. This is accomplished by infecting a system through an undiscovered or unpatched vulnerability and installing software such as a remote access Trojan, which listens for instructions over an Internet Relay Chat (IRC) or other channels. Such a compromised system is called a bot.

What is particularly troublesome to many security experts is the trend of harvesting bots into massive botnets, which are then rented out by the hour or day. For example, last year, Jeanson James Ancheta became the first hacker successfully prosecuted for creating and using a botnet for malicious purposes. Ancheta wrote a worm that infected unpatched computers and turned them into bots. Ancheta rented this botnet out to others to use as they pleased.

At one point, Ancheta’s network of bots included more than 400,000 systems, all of which could be used, on command, to launch denial of service attacks or send spam. If a company is not monitoring or scanning outbound email, it may never know it is the source of spam.

able to work on them at night or from another hospital. The American Psychiatric Association recently noted the danger in this trend with a statement on its Web site that said: “Issues of security arise. In addition, the location of the email on another computer system also increases the risk of inappropriate disclosure.”

Others forward email to another account for a more practical reason: They have exceeded the capacity of their corporate mailbox. This is a troublesome trend that is occurring more frequently.

This was borne out at a recent Boston, Mass., roundtable conducted by Ziff Davis Enterprise for Proofpoint. There, several participants said that because of mailbox size limitations in their corporate mail systems, many users were forwarding all of their mail to an online Web-based email service that offered much larger or even unlimited capacity for free. The participants noted that mailbox size limitations (typically 100 to 150 megabytes, according to some attendees) is becoming an important issue as companies rely on more media-rich presentations, as well as audio and video content.

Privacy Regulations Add to Email Security Burden

Regulation	What it entails	Organization actions
PCI DSS	Credit card security standards for companies storing, processing, or transmitting credit cards	Companies must follow strict rules for encrypting emails that contain customer information
PIIG	Office of Management & Budget guidelines for protecting the personal information held by agencies	Agencies must develop their own policies and procedures to handle breaches and notify the people impacted
HIPAA	A set of standards for the confidential exchange of patient health care records	Health care organizations and others who use health information must secure all protected health information
GLBA	Requires financial institutions to respect the privacy of their customers and protect the security and confidentiality of those customers' nonpublic personal information	Institutions must use encryption and other technology to secure the exchange of nonpublic personal information
State privacy laws	Individual states now require organizations that handle personal information to disclose breaches	Organization must take steps to secure personal information while at rest and when shared electronically
International privacy laws	Many new and existing privacy laws apply to U.S. companies doing business in other countries	Companies must abide by countries' specific data protection, retention/purging, and notification regulations

Consequently, file attachments are growing in size, causing users to exceed their mailbox size on a more frequent basis.

Regulatory Landscape Evolves

Any of these scenarios might expose data or put a company at risk of noncompliance with an increasing number of government or industry regulations (see table above).

Many organizations are familiar with Sarbanes-Oxley (SOX) and routinely undergo SOX audits to ensure their systems and procedures are compliant. But today, companies and much of their data are subject to other regulations as well.

Ensuring the Privacy of Healthcare Information—HIPAA

For instance, a company that collects any type of health information about its employees or shares that information with insurance companies would have to take Health Insurance Portability and Accountability Act (HIPAA) privacy regulations into account.

In March 2007, Atlanta's Piedmont Hospital became the first institution in the country to be audited for HIPAA compliance. Among the items checked were the hospital's policies and procedures for handling physical and logical access to systems and data, Internet usage, violations of security rules by employees, and logging and recording of system activities.

According to industry experts, Piedmont was presented with a list of 42 items, on which officials at the U.S. Department of Health and Human Services (HHS) wanted a report within 10 days. With regard to email, Piedmont was asked to show its policies and procedures for transmitting electronic Protected Health Information (ePHI), particularly regarding its list of encryption mechanisms for ePHI and its transmission methods for sending ePHI over an electronic communications network.

A September 2007 article in the *Central Penn Business Journal* noted the impact this audit was having on health care providers around the country. Specifically, the article stated: "The move lets hospitals know that government is serious about enforcing the rules." It went on to say that patients' knowledge about the importance of keeping their information safe is growing and that several hospital CIOs believed that this meant "the bar is going to rise in terms of the robustness of [their] security."

Others seconded those opinions. In a 2007 IT industry magazine publication, Gartner analyst Barry Runyon noted that the mere fact that an audit of HIPAA security compliance was conducted for the first time has many in the health care industry preparing for more enforcement actions. "I don't think Piedmont was an anomaly," he said. "My sense is that there is going to be more feet on the street from HHS going on unannounced audits."

Ensuring the Privacy of Financial Information—GLBA and PCI

Similarly, financial institutions must take the privacy of its customers into account and protect the security and confidentiality of those customers' nonpublic personal information, thanks to the Gramm-Leach-Bliley Act. GLBA requires financial institutions — such as banks, brokerage firms, insurance companies and tax preparation firms, as well as all of their business partners and contractors — to protect the private financial information that passes through their enterprises.

To accomplish this, firms and their partners are required to make a number of information security best practices part of their everyday operations. For example, companies need to ensure that email messages containing confidential information are kept secure when transmitted over an unprotected link, and that email systems and users are properly authenticated, which prevents unauthorized access to confidential information.

In an effort to combat identity theft, there is also a new Payment Card Industry Data Security Standard (DSS), which proposes security standards for companies that store, process, or transmit credit card information. PCI DSS requires that companies build and maintain a secure network, protect cardholder data, maintain a vulnerability-management program, implement strong access control mechanisms, monitor and test networks regularly, and maintain an information security policy.

When it comes to email and transmission of credit card data, companies must encrypt sensitive information that is sent over open, public networks. Specifically, PCI DSS requires that companies use “strong cryptography and security protocols such as secure sockets layer (SSL)/transport layer security (TLS) and Internet Protocol security (IPsec) to safeguard sensitive cardholder data during transmission over open, public networks.” It also requires that companies never send a customer's primary account number (PAN) unencrypted by email.

Federal Government Efforts to Ensure Better Protection of Personal Information—PIIG

In May 2007, the Office of Management and Budget (OMB) issued guidelines on the protection of personally identifiable information (PII) held by government agencies. Essentially, each agency would have to develop its own policies to respond to a breach and to notify potential victims of data theft.

The OMB memo announcing the guidelines recommended that agencies reduce the amount of PII data they collected, limit access to that data, and use encryption, strong authentication, and other security controls to protect the data.

The Department of Homeland Security had begun the development of its Personally Identifiable Information Guidelines (PIIG) even before the OMB memo was issued. The reason: In April 2007, the department's Transportation Security Administration (TSA) lost a hard drive with the social security numbers, dates of birth, payroll, and bank account information of 100,000 employees.

The American Federation of Government Employees (AFGE), the union representing the workers, sued the TSA. A May 2007 *eWeek* article noted that AFGE claimed “by failing to establish safeguards to ensure the security and confidentiality of personnel records, the TSA violated both the Aviation and Transportation Security Act and the Privacy Act of 1974. “The TSA's reckless behavior is clearly in violation of the law,” AFGE National President John Gage said in the union's statement. “TSA must be held liable for this wanton disregard for employee privacy.”

The AFGE asked that the TSA create new security procedures that would include electronically monitoring any mobile equipment that stores personal data on employees and by encrypting personal data.

In many breaches of this type, the organization might offer a year's worth of a credit monitoring service. According to the *eWeek* article, AFGE asked for a very interesting and different form of help. It asked the TSA to grant leave to employees who request time in order to “protect against or correct identity theft or financial disruption caused by identity theft.”

Companies should take notice. This is a new source of employee productivity loss.

State Governments Join the Privacy and Data Protection Bandwagon

At the state level, 35 states and the District of Columbia have instituted privacy laws. In particular, many states require agencies that own or license computerized data that involves personal information to disclose any breach of data security.

The main impact of all these new laws is that they impose privacy and data protection requirements on companies that up until now have not been regulated. For example, many private companies have not had to deal with SOX. But these new laws apply to any company that holds or collects personal information (e.g., Social Security numbers, dates of birth, etc.) from its employees. In other words, everyone is impacted now.

Consequences of a Breach or Data Leak

As the number of data privacy regulations grows, so do the number of breaches and data leakage incidents. A com-

pany unfortunate enough to experience a problem could face a number of severe consequences.

First, there is embarrassment. Data breaches today are front-page news. For example, TJX Companies (including TJ Maxx and Marshalls) have been in the news for several months over what some are calling the largest computer data breach ever, where thieves stole more than 45 million customer credit card and debit card numbers. An August 2007 *Boston Globe* article reports that the cost of the breach to TJX is now pegged at \$256 million.

A 2007 Forrester Research study found that the average security breach can cost a company between \$90 and \$305 per record lost. In a 2007 IT trade magazine article Forrester senior analyst Khalid Kark noted that while “Studies may not be able to determine the exact cost of a security breach in your organization, the loss of sensitive data can have a crippling impact on an organization’s bottom line.”

Additionally, there are liabilities if data is compromised. Fidelity paid for a year’s worth of credit-watch service for 200,000 of its customers whose credit card and loan information appeared on unencrypted tapes that were lost in transit to a credit bureau. LexisNexis paid for credit monitoring services for 32,000 of its customers whose information was stolen by hackers.

The cost of such services varies greatly, but typically they are in the \$75 to \$100 per year range. That means a company that had to offer this service after a data breach would spend between \$2.25 million and \$3 million for a breach involving 30,000 people.

Companies are also subject to fines and legal penalties. The U.S. Federal Trade Commission assessed Choice-Point \$15 million in fines and penalties for a data breach where bogus companies stole the personal information of 163,000 customers.

There are also potential productivity problems. A company whose servers are turned into spamming bots will likely experience lost productivity as infected machines slow down the performance of other applications by flooding the network with unwanted spam and utilizing more bandwidth than usual.

When it comes to PCI DSS, there are multiple penalties a company can incur for noncompliance. According to the PCI Compliance Guide.org, these penalties include:

- Visa may charge your business up to \$500,000 per incident if your network and the information of consumers are compromised.
- If you do not notify the companies of probable or actual violations or thefts of your customers’ informa-

Penalty for PCI DSS Non-Compliance

You may be banned from allowing your customers to use credit cards issued by the company that finds your business noncompliant.

tion, you will also be fined. Again, Visa can charge as much as \$100,000 per incident.

- Other fines may be charged if the credit card company feels that your company’s violations pose a risk to the credit card company and/or its members.

Technical Challenges to Preventing Data Loss

Preventing data loss can be a fairly complex undertaking. Companies must be able to quickly identify emails that contain information that needs to be blocked or encrypted.

Accuracy in identifying these emails is extremely important. A mistakenly blocked message might cause a delay in a business transaction. A client, customer, or partner might become frustrated waiting for that message. And if appropriate notification systems are not employed, the sender might not even know that the message was blocked.

On another level, companies have a challenge in defining their data loss prevention policies. For instance, it is one thing to scan for particular information like a customer record number, Social Security number, birth date, password, or other nonpublic personal information. It is another to prevent a disgruntled employee from sending out key details of a confidential business plan or intellectual property. There must be some way to populate a filter or scanner with such information.

An added complication is encryption to secure a message’s content in transit. Many encryption solutions are hard to use and manage. If a company does business with only one partner, it would be easy to settle on an encryption approach and train people in both organizations in its use.

But it is more likely that a company will need to conduct business and securely share information with many partners and individuals. In most cases, it is hard to impose a particular encryption system on a large number of parties, unless that system supports the easy creation and accurate application of your company’s encryption policies.

If the solution requires desktop client software, some companies might not allow their employees to download any software, and some individuals might simply refuse to

go along. Even if recipients could download encryption software, they might not be able to understand how to use it. So there must be an easy-to-use solution that does not require recipients to alter their system or download special software.

Finally, some data loss prevention solutions can have high management overhead necessitating constant oversight and requiring that many manual tasks be performed.

Employing Best Practices

As with many security-related initiatives, email security and data loss prevention require the development of policies and procedures that are based on best practices.

Specifically, companies need to focus their efforts in a number of areas, including:

- **Measure the current risk:** Procedures must be put in place to monitor and audit traffic in order to understand how much personal information is currently being sent via unencrypted email.
- **Create policies:** IT must confer with business management to understand what regulations apply to particular data and what the consequences of a data breach would be to the company. This information should guide IT in the development of security and data protection policies.
- **Develop procedures:** Companies must specify how personal information is to be handled and what actions to take to address a breach. This should include a plan to correct the situation when a breach occurs and notify customers and appropriate regulatory agencies.
- **Use technology to automate policy enforcement:** IT should select solutions that can automatically check for compliance with policies — and ensure enforcement.
- **Give your compliance team appropriate authority:** Having policies in place is effective only if they are followed. In many organizations, management or some employees feel exempt from the rules. People responsible for data privacy compliance must be in a position to enforce the rules throughout the organization.
- **Produce ongoing reports for management:** Show management the effectiveness of the solutions your team has put in place. Use the reports to demonstrate the level of protection you are offering.

With the wide array of regulations, it is essential that business management and IT work together so that IT will know what data is governed by particular regulations. There should also be a conveyance of the business issues associated with the protection of that data. For example, if a breach or exposure will result in millions of dollars in fines, IT can help cost justify technology solutions based on cost avoidance.

Once it is determined what data must be protected, policies can be created to ensure compliance. Part of any data loss prevention plan must include educating users. But there still must be procedures and solutions in place to monitor for and enforce compliance.

For example, a disgruntled employee might use a third-party encryption product to try to sneak confidential corporate information past an outbound mail content check. To prevent this, a company might adopt a policy where only data encrypted by the corporate-sanctioned encryption solution may be sent outside the company.

Proofpoint as Your Technology Partner

Proofpoint helps protect email and prevent data loss. Its unified email security solutions allow companies to easily manage and combine antivirus, spam filtering, encryption, and outbound data prevention loss technologies. The solutions monitor and protect traditional email, as well as information sent using other protocols and systems, including Web-based email, FTP and instant messaging.

Proofpoint solutions help companies set up and enforce email security policies and procedures. They monitor for problems and for instances where policies are not met, and they alert appropriate managers so that action can be taken.

Many processes, such as the blocking or quarantining of threatening or noncompliant messages, can be automated. Messages that meet company-specified criteria can automatically be routed to appropriate managers. In this way, a manager might inspect a message and deem it okay to be delivered. Or, the manager will be able to identify a malicious employee or a user who simply needs more training on company policies.

From a deployment perspective, Proofpoint offers a physical appliance, installable software, a virtual appliance, and an on-demand service.

All told, the unified, easy-to-manage solutions with the variety of deployment scenarios can help companies address today's emerging email threats and help ensure prevention of data loss through email. ■

Visit proofpoint.com for more information about the latest email security and data loss prevention trends and how you can keep your organization secure and compliant.