Secure and compliant email systems are essential for financial services companies. In this two part series on email security best practices, expert George Wrenn discusses how to capture emails, securely archive the messages and detailed reporting.
Email security and compliance best practices

Table Of Contents

Email security and compliance best practices

Resources from Google Postini
Email security and compliance best practices

By George Wrenn, Contributor

PART I
Managing email regulatory compliance and security in the financial services sector can be a daunting task. To be certain, email speeds up the business and makes servicing customers and partners easier, but there is a dark side.

Consider one high-profile case, which involved a star investment banker at Credit Suisse First Boston (CSFB) who sent an email to more than 400 subordinates telling them to clean up their email accounts -- federal prosecutors used that email as evidence of a cover up of improper trading at CSFB. The banker was convicted of obstruction of justice.

Let's examine the issues around email security and best practices to help manage compliance while still enjoying the benefits of this crucial communications tool.

Have a well-crafted policy
Before you can bring control to email, you must first create a policy. It may seem very basic, but your security policy must define email precisely.

A good working definition would cover all electronically transmitted messages, regardless of format (HTML, XML, RTF, etc.), attachments (documents, spreadsheets, graphics, etc.) and supporting infrastructure -- the servers that transmit and store email. For financial services, this list will include such services as Bloomberg mail and instant messaging, Internet mail providers and your in-house MS Exchange, Lotus Notes or other email system.

Refer to your information security policy or data protection policy (if available) to have a crisp definition of your company's specific data classification framework. This is important if you decide that certain information must not be transmitted insecurely, or at all, via email.

Now that you have defined what email is, it's time to consider the myriad of regulations that apply to it. For most in the financial services industry, a good starting point is the US
Securities and Exchange Commission; for self-regulated organizations, check with your governing body regarding regulations applicable to email.

**Archiving email**
The requirement to archive email for specified period, usually 10 years, should be at the top of your list. Archiving must be done in a manner that prevents users from deleting emails that could be important in an investigation. The best way to accomplish this is to have both incoming and outgoing email archived in real-time. This prevents users from mass deleting emails. It’s best to consider a secure an off-site archive. Ideally, this archive is managed by administrators without a conflict of interest, such as an outsourced provider, lessening the chance of malicious insider email and data destruction.

Your choice of archive technology and/or outsourced provider should include protections against altering or deletion. A forensically compliant system is the best. Here there are cryptographic checksums, hashes, encryption, signatures, timestamps and other data protection mechanisms that can stand up in an investigation or against cross examination in a court of law. When something was emailed may be as important as what was emailed. That’s why nothing less than a rock-solid forensically compliant system is best.

**Supervision review capability**
Supervisory review of email sent through the system is critical to meeting compliance objectives. You must have a program and policy in place that ensures regular review of the email content that is flowing though your company. The review has to be done in such a manner that it constitutes due care and monitoring to catch illicit or prohibited communications. The workflow for this may have to meet other requirements such as keyword matching, randomness, frequency or target specific roles within the organization, such as the trading desk. Your systems must support these policy or regulatory requirements.

**Detailed reporting is a must**
In order to prove the effectiveness of your regulatory compliance program, you need to produce detailed reports on email activity for your auditors.

For starters, your reporting should include the following:
• Measures of the effectiveness of the supervisory process.
• The number noncompliant messages and policy violations in defined time periods.
• Actual messages reviewed and analyzed by supervisors.
• Tracking of outcomes or actions on violations detected.
• Volume of email archived by groups or users.
• System capacity remaining for archive.
• Access violations or archive tampering attempts.
• Audit reports of access to the archive and messages.

Don't underestimate the importance of reporting. If you miss these critical capabilities, you may find yourself with a failed audit despite otherwise solid archiving practices.

PART II

Searching and discovery support
At this stage, you have a good understanding of what it takes to document, capture, review and report on your email compliance program. This is all good until you get hit with your first discovery request, which can turn your world upside down. A simple email discovery request can cost hundreds of thousands of dollars in labor, lost productivity, hardware and software when all is said and done.

It is therefore very important that your implementation supports robust and secure search capabilities. A discovery request can include specific users, keywords, phrases or time periods (sometimes all at once). Sometimes searches can produce damaging information that is not material to the investigation. For example, inappropriate activity recorded in email is often discovered as a byproduct of the search, and the release of this information to outsiders could have consequences.

Your email archiving tool should offer laser-precise search capability and be able to target searches to a limited set of email messages.
Data leakage

All the archiving in the world is not going to stop sensitive data from leaking out of the enterprise. There are two basic concerns with data leakage; the first is the data in the archive. It should be encrypted with a well-known, strong, trusted algorithm, such as advanced encryption standard. The external provider should not be able to access your data in the archive. Also, in the event of a system breach, the email won't be disclosed if it is protected by strong encryption.

The second concern is sensitive data leaking in emails being sent outside the firewall. To control risk, you need to define the types of data that fit this classification. This won't stop corporate espionage, but it will help keep honest users from inadvertently leaking financial data to their entire global address list.

Your data protection policy or data classification framework plays an important role in policy enforcement. Many of the email data leakage products available require a concept of classification.

The first layer of defense in secure email proxy tools is often keyword or expression matching to prevent data leakage. For example, social security numbers may take the form 000-00-0000 through 999-99-9999, a proxy would detect this pattern and block the message, perhaps triggering an event or alarm for the security administrator to review. Similarly keyword systems may catch words like "sell short" and "hot stock" and block these types of messages. These approaches can be hit or miss and can produce false positives, inhibiting the flow of legitimate email.

To help, a second layer of defense is often required. Tagging data, documents or messages with classification levels can prevent sensitive, restricted information from leaving the company mail system. Many appliance-based tools offer a combination of technologies to prevent deliberate or accidental data leakage from emails send beyond the firewall.

If you must send sensitive data outside the firewall, a policy requiring users to protect intellectual property and proprietary information is meaningless without giving them the proper security mechanism. Protecting electronic information exchanges is essential for financial services firms. For email, security usually means encryption.
An email security policy should include the types of accepted encryption, when it should be used and how it will be implemented.

**Use disclaimers for damage control**
A disclaimer statement should be added to the end of each email, informing recipients of the sending organization’s policy, the nature of the email (such as "For Official Use Only") and what material it disavows. For instance, a securities trading firm may include that it accepts no responsibility for falsely or improperly sent messages, and that any violation should be reported to a security manager. A disclaimer puts the onus on recipients to act responsibly when receiving improperly disclosed information.

Disclaimers offer no guarantee of compliance, but they do establish a legal standing for making claims against those who perpetuate a security violation.

**Governance is key**
Email security policies should outline the roles and responsibilities of those managing the email system. Set expectations as to how security managers, email administrators and other department managers respond to email issues and security.

An email security policy is worthless unless users are presented and periodically reminded of it. Best practice is to give new employees a copy of the policy when they are hired. Enterprises should treat email security policies as dynamic documents that evolve to meet changing legal and operating conditions, technologies and threats. Annual reviews and revisions will ensure the policy keeps up with changing needs.

The financial services sector has one of the most difficult email security challenges of any industry. Follow these proven best practices that can help mitigate your regulatory email risks through sound policy, secure archiving, supervisory review practices, audit reporting and data leakage prevention.
About the author:

George Wrenn, CISSP, ISSEP, is frequent contributor to SearchSecurity.com and Information Security magazine, he served as a Director of Security in the financial services industry and is now a consulting security expert. He's also a Six Sigma Black Belt, a Harvard grad and was trained in cryptography at MIT. He can be reached at mitalum@mac.com.
Resources from Google Postini

Google Postini Services

Google Apps for Business

About Google Postini