Global Information Assurance Certification Paper

Julie Benner
GSEC Practical Assignment Version 1.4b, Option 1

Information Security and SEC Rule 17a-4

Abstract

There are several government rulings and regulations that dictate how a company must retain and store information, from customer data to employee memos. SEC Rule 17a-4 is one such regulation. SEC Rule 17a-4 requires that a company selling securities products (mutual funds) has to retain all broker/dealer communications (including e-mail) for a minimum of 3-6 years, depending upon the content of the communication (General 2000). The rule has several impacts to the information security arena, including how to handle encrypted email and how to enable secure third party access to this message archive.

This paper will explore the rule as it pertains to e-mail communications specifically, and the security issues that a company must consider when attempting to comply with the regulation. At a high level, we will also explore the various solutions that meet the requirements, some important questions organizations must ask themselves in order to select the best solution, and the ramifications of non-compliance.

SEC Rule 17a-4

Many things are sent through a company's e-mail system today: company announcements, sales transactions, paycheck and benefit information, as well as viruses and SPAM. What if someone had to sort all of the e-mail by user as well as content, set up different record retention rules for that information, and then store it all in government approved storage media? Look no further, for that time is here and now.

Brokerage firms, insurance companies, as well as everyone who sells or trades securities products are scrambling to comply with SEC rule 17a-4. Upon first glance, you may wonder what the fuss is all about. After all, the aforementioned rule is under the Securities Exchange Act of 1934, right? Well, yes. But, as seemingly all laws and regulations in these great United States, it contains several sections and has been amended many, many times over the years. The original Act mandated that companies keep paper records of specific communications between a broker and a customer (Salkever 2002). This proved quite useful in investigating questionable transactions. In 1997, the SEC made the first update to the regulation to include e-mail communications. They also deemed that these e-mail communications could be kept electronically on WORM (Write Once Read Many) media, and regular audit reports of the

pertinent systems must be performed and maintained. These new amendments also apply to not only to e-mail communications between brokers and customers, but e-mail attachments, policy announcements, instant messages, and any e-mail pertaining to a securities product transaction that is sent through the e-mail system as well.

As one can imagine, there are several ways to come into compliance with this regulation. There are many product vendors that provide some and in certain instances, all of functionality to meet the requirements set forth in the rule. However, very often companies will find that the more complete the vendor solution, the higher the price tag.

The best solution is not determined upon monetary cost alone. Besides this upfront cost, there are many hidden "intangible" costs associated with the solutions. Many of them come with differing amounts of risk and security that must be considered as part of any vendor evaluation. In the following section, we will look at the security concerns that are encountered when trying to comply with the SEC rule.

Security Concerns

Information security is of utmost importance to companies that deal with the financial data of customers. A customer's trust or lack thereof in a company and the way it handles their data plays an immense role in their continuing business with that company. This is clearly evidenced by the downfall of several companies including Egghead.com after they reported that hackers had invaded their network and possibly recovered customer credit card information (King 2001). This volatility related to a customer's trust is evident with all companies that must comply with SEC rule 17a-4.

There are several aspects of the rule that give cause for security concern. First of all, the e-mail may be encrypted. Many companies have security policies in place instructing employees to encrypt e-mail containing sensitive or confidential information. The e-mails that fall under the ruling would by many accounts be deemed as containing sensitive information, including customer names, account numbers, transaction records, etc.

The also rule states that the e-mail must be indexed, searchable, and retrievable within a reasonable time frame (General 2000). Opinions vary on what is considered "reasonable," but a common interpretation is 24 hours from SEC request. This poses a problem for encrypted e-mails. By definition, e-mails that have been encrypted are not readable, not to mention not able to be indexed, searched, or retrieved based upon a user name or keyword search within the body of the message. E-mail is typically encrypted to protect the sensitive information contained within the e-mail from disclosure to others except the intended recipient(s). The notion of decrypting encrypted e-mail for the storage

and retrieval of that information by another person is in direct opposition to the purpose of encrypting the e-mail in the first place.

A company in this situation with the possibility of capturing encrypted e-mails has options in how to address the challenge. One way to deal with these concerns is based upon the encryption technology used. For example, when using PKI (asymmetric encryption), the sender encrypts a message with the recipient's public key (which as the name implies, is made public to those who wish to encrypt their communications). The message is then sent to the recipient. The recipient then decrypts the message with his/her private key (which as the name implies is only known to the recipient and no one else). However, many PKI solutions (including PGP) include a "master key" feature that allows for key recovery as well as centralized administration for all of the key pairs issued. This master key acts in essence, like a backdoor to the e-mail content (Wayner 1997). This is not without it's share of drawbacks, for the master key "…could leave corporate networks in a more vulnerable position because it would give an industrial spy a single point to focus an attack (Wayner 1997)." For more information on PKI, please visit any of the resources listed at http://www.pkiforum.org/resources.html.

Another simpler, yet not always desirable alternative to the encrypted email dilemma is to change the existing security policy governing the encryption of e-mails relating to SEC rule 17a-4. With this option, the only way to ensure 100% compliance is to remove the users' ability to encrypt. Otherwise, they could encrypt the message where it would be stored in the archive as a garbled mass of characters. There would be no capability to discern the content of the e-mail without the recipient's assistance. This would not be feasible in an SEC audit scenario in which all applicable messages to the matter at hand must be turned over within 24 hours. Removing a users e-mail encryption capability is not a very desirable solution either, as it lessens a user's ability to protect their company and it's information. The removal of this capability also invokes a subconscious message that security measures are not required, and even prohibited.

Another requirement from the rule is the presence of "an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to Rule 17a-3 and Rule 17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby (General 2000)." In essence, the SEC would like audit reports of any changes to the records retained and maintained as a result of the regulation. The SEC is very vague as to what exactly it is looking for in the aforementioned reports, so a company must show due diligence in attempting to comply with the rule in good faith. Due diligence in this instance would be adhering to industry best practices with regards to auditing accesses and activities performed on the message archive (as well as backups). The backups must be stored in a separate physical location from the main archive in keeping with standard disaster recovery protocols. Auditing best practices vary

with the platform and message store, but there is some consistent data that should be captured regardless of the archive solution chosen. At a minimum, the reports should include:

- Access control lists (who has been granted to what resource),
- Activity reports on the archive (who accessed the archive, time, and task performed – Read, Write, etc.),
- Verification of any system policies directly referenced in compliance documentation presented to the SEC.

Additional information regarding auditing best practices may be viewed at http://www.sans.org/SCORE/.

SEC rule 17a-4 also requires that "an independent third party have the ability to access stored electronic records and provide them to its examiners upon request (Judy 2002)." This introduces an additional concern, as now the data contained within the message archive is only as secure as the third party that has been granted access. There are several steps a company can follow in order to mitigate this introduced risk. First of all, make sure adequate security policies and acceptable resource usage guidance have been established. If they haven't, the resources at http://www.infosyssec.org/infosyssec/secpol1.htm have several templates and How-To's to assist with those policies that need a little fine-tuning.

As part of the evaluation of the potential third party representatives, conduct on-site visits when feasible in order to evaluate their physical security practices and procedures. Request to see their security policies and awareness programs. Next, include the security requirements that the third party will be expected to follow in the contract. This is essential in order to have legal recourse in the event that the security policies are not followed as intended. Examples of these requirements can include (but are not limited to):

- Connections allowed between company network and third party network (dedicated line, VPN, dial-in solution, etc.),
- Authentication and authorization methods to be employed – if passwords are used, emphasize the usage of strong passwords,
- Allowable ports and protocols for the download of information for the SEC,
- Background checks of the third party employees that have access to the message archive,
- Right to audit their systems, or review their internal audit findings,
- Right to request a third-party penetration test of their systems.

Often, organizations will find that these requirements are incorporated into the enterprise security policy. If not, this is an opportune time to include these in order to strengthen the existing policy.

Once a company has addressed the above concerns, they can begin to address potential compliance solutions. There are several vendor products that fulfill part or all of a fully SEC compliant solution. We will next look at the different categories of products that can bring a company into compliance, and evaluate their security pros and cons.

Selecting a Vendor Product

Vendor products that claim to provide SEC compliance tend to fall into the following categories:

- Hosted off-site, retain all e-mails,
- Hosted off-site, filter or segregate which e-mails to retain,
- On-site, retain all e-mails
- On-site, filter or segregate which e-mails to retain.

There are two main divisions: on-site vs. off-site storage, and retain all vs. retain only selected e-mails. Each of the divisions provides for distinct advantages and disadvantages from a security perspective.

In the first division, on-site vs. off-site storage, there are several pros and cons associated with each solution. On-site storage allows for a company to be in full control of their data. With the exception of the third party requirement discussed previously, all data is maintained and accessed exclusively by the company that owns the information. This is very desirable as it puts the power and control of the data into the hands of the data owners, arguably the ones with the most vested interests in the safety and security of the information in the message archive. This option also allows for the easiest means by which access, authorization, and auditing can be implemented. Because all of the data would reside in-house, existing methods for authentication and auditing could be utilized in order to minimize administrative overhead. However, with all of these benefits comes a set of drawbacks as well. Even though existing authentication, authorization, and auditing could be reused, these is still a large amount of administration that goes along with the data volumes that would need to be retained. In a smaller firm the sheer amount of data and the facilities required to retain and maintain the archive could easily overwhelm a small IT staff. For this reason alone, many small to mid-size companies seek to outsource.

Where on-site storage falters, off-site storage excels. With off-site storage, companies get relief not only from the ever-expanding volumes of data that must be retained, but also from the responsibility of having to control all facets of the data access and authorization. This can be an immense plus for organizations will little security experience. Also, several off-site storage solutions offer SEC representation of their solution, therefore relieving the organization some of the burden of dealing with the regulatory body. But these pluses don't come without a price, often a hefty one.

Off-site storage solutions are frequently much more expensive than their on-site cousin. This is due largely because of the vast amounts of storage that is provided, as well as the administrative costs to maintain the archive for the time period (3-6 years) specified in the regulation. Another item for the con column is that companies would lose control of their data. The off-site storage vendor would have complete and total control over the access, authorization, and auditing of the archive. These risks can be mitigated somewhat by following several of the guidelines regarding third party access to the in-house e-mail archive mentioned previously

In the second division, retain all e-mails vs. filter or segregate which e-mails to retain, there are again some definitive pros and cons associated with the solutions. When all e-mails within an organization are retained, the company is assured that they are 100% in compliance with the requirements of the SEC rule. There is no doubt that all pertinent e-mails were retained, since all e-mails are kept. This may sound like a perfect solution, however it is unacceptable to many organizations. For some companies, especially those that are larger with several different lines of business such as an insurance company that also sells mutual funds, the increased exposure of what is retained (in addition to the securities products e-mail as defined within the SEC rules) is frequently too much risk for the company to accept. These e-mails in the archive would not be required for SEC compliance; however, they would be discoverable items in the event of legal action against the company. This could prove to be devastating to an organization. Also, when all e-mails are retained, the volume of information rises exponentially resulting in increased performance hits when parsing all of that unneeded data during an SEC audit.

Filtering the e-mail can alleviate the legal exposure of a large, diverse company, however it does open the gate for e-mails to be missed resulting in non-compliance with the SEC. Filtering can be done by several methods depending upon the product. Most products can filter and retain e-mails based upon Sender, Recipient, Cc, Bcc, Subject line, keyword/string search within the body of the e-mail, or attachment. These criteria go a long way to be inclusive; however, it is very difficult to prove that beyond a shadow of a doubt, the filter captures all pertinent e-mail communications. For small companies whose only line of business securities products, that risk increase may not be worthwhile. Filtering also assists in the size and availability issues present with the “retain all” solutions. By filtering and retaining only those e-mails with a very high probability of being needed in accordance with the SEC rule, the overall volume of e-mails handled by the system would decrease, thereby making most effective use of system resources.

In selecting a vendor to assist in meeting SEC rule 17a-4, several questions must be answered before a decision can be agreed upon:

- How large is the IT staff? Can they handle the increased administrative work involved with an in-house solution?
- Does the organization have several lines of business that may be compromised in a "retain all" scenario?
- How much of a risk does SEC non-compliance pose to the organization – a slap on the wrist or a devastating blow to their livelihood?
- What budget has been allowed for this solution? Were ongoing costs (additional IT support personnel, server allocation forecasting, etc.) included in the figures?
- How secure is the current organization? If the answer is not very, would it be best in the short term to outsource the solution while spending limited resources on more pressing issues?
- What is the likelihood that security requirements will be included in a contract with a vendor?

There are several solutions in each of the categories listed at the beginning of this section. Answers to the questions above will help drive out some basic requirements that an organization can use to begin initial evaluations, and serve to aid them in narrowing their search for a product.

Ramifications of Non-Compliance

There are so many requirements to meet when attempting to comply with an SEC rule, not to mention the all of the costs of implementing a compliant solution. So, is it worth it? What is the worst that could happen? Well, unfortunately for some folks, quite a lot. Penalties range form simple fines to criminal action, and even the "suspension or expulsion from the securities industry (Morgenson 2002)."

Several major players in the securities industry have fallen victim to the SEC regulatory crackdown. Morgan Stanley has been the recent focus of SEC investigators' microscope as reports have been published questioning the number of e-mails and attachments the company produced in response to an investigation. The investigators believe the documents are too few in number, and are a possible indication of faulty e-mail retention practices (Reuters 2002). A Morgan Stanley spokeswoman was quoted as believing they acted with due diligence, but it looks as though good intentions won't save them from this inquisition.

Morgan Stanley is not alone in the spotlight. "The SEC has moved to levy $1.67 million fines against Salomon Smith Barney, Morgan Stanley, Goldman Sachs, Merrill Lynch, Deutsche Bank, and U.S. Bancorp Piper Jaffray (Morrissey 2002)." Memos known as Wells notices were given out to those firms in which "an investigation has been completed and that it has uncovered evidence that warrants disciplinary action (Morgenson 2002)." The recent strong enforcement

of the e-mail retention rule is believed to be the result of a multi-million dollar conflict of interest lawsuit against Merrill Lynch that used employee e-mails as key pieces of evidence earlier in 2002.

These fines and lawsuits seem large, but in comparison to the net worth of the firms involved, they are really just small potatoes. So where does the real damage come from? Monetary fines are only detrimental once they reach a high enough percentage of a company's value. The real damage comes from the tarnished reputations of the companies that are found to be non-compliant. In this time of collapsing giant corporations (Enron, Arthur Anderson, etc.) the public has become more wary of the big businesses, more suspicious of the slight of hand with which some organizations run their books and their business. In an industry based upon customer trust (as the securities products industry is), you can't afford not to do the right thing. Customers are concerned about the security of their data, and when a company doesn't play by the rules, a seed of doubt is planted with them that often lingers for years to come.

Conclusion

The information security arena is influenced by many factors, including government regulations. SEC rule 17a-4 contains several sections that impact the security of information in an organization, including how to access encrypted e-mail, the need for audit records, third party access, and how to select the best vendor for an organization's compliance needs. Each of these topics must be addressed in order to best protect the enterprise from unauthorized disclosure of information.

Like many laws and regulations, SEC rule 17a-4 does not provide a wealth of guidance or "thou shalls." There are requirements for what a company needs to do, but not *how* a company should to accomplish them. This has advantages and disadvantages for those needing to comply. On one hand, companies are able to interpret the law in a manner in which they see fit. This is an immense plus as it allows organizations the freedom to explore many possibilities in finding a solution that works for them. However, this freedom comes with a price. The vagueness of the law also means that the SEC's interpretation may not correspond with the organization's interpretation and non-compliance can result.

As we have seen some of the largest and well-respected players in the securities industry fall into non-compliance, the stakes are being raised. These initial investigations are paving a very slippery slope that should incite other firms to take heed of the more intense scrutiny and investigations headed their way. As Alex Salkever put it, "the devil is in the e-mail."

List of References

General Rules and Regulations Promulgated under the Securities Exchange Act of 1934. Rule 17a-4 – Records to Be Preserved by Certain Exchange Members, Brokers and Dealers [Effective until May 2, 2003.] 13 March 2000. URL: http://www.law.uc.edu/CCL/34ActRls/rule17a-4.html (31 October 2002).

Judy, Henry L. and Benjamin S. Hayes. "Records Management of E-Mail by Securities Firms: Legal and Compliance Technology Issues." October 2002. URL: http://www.cybersecuritieslaw.com/wslawyer/judy.htm (20 November 2002).

King, Carol. "Egghead.com Sales Soft in Q4." 26 January 2001. URL: http://siliconvalley.internet.com/news/article.php/571601 (31 October 2002).

Morgenson, Gretchen. "Wall St. Firms Said to Break E-Mail Rule." 7 May 2002. URL: http://www.siliconinvestor.com/stocktalk/msg.gsp?msgid=17437733 (29 October 2002).

Morrissey, Brian. "SEC to Wall Street: Don't Delete That E-Mail." 5 August 2002. URL: http://www.isp-planet.com/news/2002/sec_email_020805.html (29 October 2002).

PKI Forum. "PKI Resources." URL: http://www.pkiforum.org/resources.html (1 November 2002).

Reuters. "Morgan Stanley e-mails probed." 22 November 2002. URL: http://money.cnn.com/2002/11/22/news/companies/morgan_emails.reut/ (25 November 2002).

Salkever, Alex. "The Devil Is in the E-Mail." 23 April 2002. URL: http://www.businessweek.com/technology/content/apr2002/tc20020423_1104.htm (31 October 2002).

S.C.O.R.E. Security Consensus Operational Readiness Evaluation. URL: http://www.sans.org/SCORE/ (1 November 2002).

Security Policy Writing Styles and Guides. URL: http://www.infosyssec.org/infosyssec/secpol1.htm (30 October 2002).

Wayner, Peter. "PGP Offers New Encryption Software for Corporations." 3 October 1997. URL: http://www.columbia.edu/~ariel/news/pgp-gak.html (31 October 2002).