SOCJ Feature

< BACK

Top 5 Strategic Email Compliance Mistakes

2005-09-26 12:00:00.0 CDT

By Anthony Sanchez

If you review many of the recent business scandals in the news this last year, it is clear that something has changed regarding email and business risks. I'm not talking about spam, viruses, or even phishing. Those are annoyances, but they don't really have the destructive power that can damage businesses as large as Enron, Arthur Andersen and Morgan Stanley. Companies that do not have a good handle on what is in their email system, what is being sent through their email, or how to retrieve historical emails when necessary, have had major financial losses.

The daily headlines show the major force that email has become. Several factors are driving email compliance: The rise of regulations in the last several years; the growth of email volumes; and the lack of email discipline and enforceable polices.

Many companies are making major strategic errors regarding email compliance because they are operating on an outdated model. Here are the Top 5 mistakes that can BREAK a company's compliance effort:

Mistake # 1: Business Goal
Compliance should not be the business goal of a company. Business goals should be to become a better business; to reduce business risks, to improve business productivity; to improve customer service, and to ensure the company image and reputation is not damaged, etc..

The mistake many companies make is to take the regulations literally and as complete business guidelines. They are not; they are government minimum standards. Do you want to operate your company solely according government minimum standards?

Action: Make sure your business includes goals of achieving high ethical standards, solid operations and processes and an institutionalization of a culture of compliance from the top down. Compliance is an ongoing process that should be the by-product of these goals. If these are your business goals, then meeting compliance mandates will be easy.

Mistake # 2: Retention: Thinking that after the retention period ends, documents must be destroyed
Regulations mandate a minimum period to keep your business documents, not a maximum period. Regulations do not compel a business to destroy their documents. Why should you keep business records longer than the retention period?

Business documents are critical assets of the business, they hold corporate knowledge, customer histories, long term trends, and other information that can be used as a guide to the business long after an email retention period is over.

All the "old" reasons for deleting electronic documents are no longer valid, since storage costs are so low and email retrieval software is so widely

available. There are more reasons than ever to keep all email records. The need for email search and retrieval will continue to increase because the quantity of email is increasing, and more information is created and stored only in email.

Very recently, the judge in the Morgan Stanley v. Ronal Perleman case, created a precedent for requiring a company to produce records regardless of the fact that a company has a document retention policy and has already destroyed the emails in question. The net result of this case was that Morgan Stanley lost a $1.4 Billion judgment in part due to the inability to keep and retrieve their emails assets.

With the increase in business and employee lawsuits, harassment cases, and subpoenas for email records, there are strong reasons to not destroy documents as soon as the retention period is complete. Emails can contain “evidence”, but that does not mean the evidence is always harmful to a company. A recent employee lawsuit for wrongful termination found quite a bit of incriminating and compromising material against him after searching through the archive for emails. The company ended up saving themselves the cost of a major lawsuit and settlement by simply having easy access to emails that would not have been marked for retention under compliance or any other business reason.

If a company does feel that the emails in their system may do more harm than good, I think the larger question they need to be asking themselves is ‘what kind of company do we run here?’ If they are the kind of company that produces so many harmful or compromising emails due to their business practices or company culture that they need to “destroy the evidence” as soon as possible, then they have a much larger problem than email retention and destruction. Their company has an institutional problem that will probably result in trouble in some other way first.

Action: Implement a permanent email archiving solution. I would argue that all emails should be kept forever, and I challenge why any email should ever be destroyed if we have the ability to inexpensively store it and easily access it when needed.

Mistake # 3: Expensive: Thinking that a company needs an expensive, complex content management system to achieve email compliance.
A lot of companies, especially small to medium sized companies, mistakenly complain that they don’t want to get started on compliance because it will take months or years to implement, and hundreds of thousands of dollars in software and services. When it comes to email compliance, this is far from reality.

Many email compliance and content management vendors have needed to justify the expense of their software solution by making it sound complex, technical and only something that an expert in the field should attempt.

The truth is that it is much easier to have email be in compliance with most of the major regulations by simply archiving everything, keeping it in an easily accessible location, and being able to search by keyword, and produce requested documents in a timely fashion. All of this can be accomplished with a fairly priced email archiving solution, which can be installed in a day.

Related to this same mistake is thinking that a backup tape system is sufficient for compliance requirements. It is not. Compliance is not about collecting data for a disaster recovery solution, it is about timely retrieval of specific data. Back up tapes will be more expensive in the long run, and are simply not a valid compliance solution.

Action: Do the research to find reasonable priced email archiving vendors for small to medium sized companies that can implement their system in a few days. Do not rely on your tape back up system for email compliance.

Mistake # 4: Assets: Not including all email as a compliance asset.
Many companies do not consider email documents as part of their record retention and compliance policies. Some companies mistakenly believe that email is simply a communication medium, like a telephone, and that emails are simply verbal conversations that happen to appear in written form temporarily. Following this logic, emails would not have to be

considered a business document any more than a verbal conversation would. And therefore emails can and should be deleted as soon as the conversation ends.

What these companies do not realize is that email is not a fleeting conversation, but it is a business communication record that can have business value, transactional and contractual information, attachments with financial documents, and in many cases the only record of an approval or even a customer agreement. In all of these cases, these are critical compliance assets can show the history of accounting and business decisions.

Action: Emails are business documents, and need to be considered the same way any other hard copy form of communication is for compliance and retention.

Mistake # 5: Kinds of documents: Thinking that categorization of documents is necessary.

Because various regulations require companies to retain certain documents for a specified number of years, many companies take this as the only way to retain documents. For example, in the Sarbanes-Oxley regulation, documents that show how a financial decision was made need to be retained for a certain amount of time.

Some companies interpret this to mean that certain types of documents, spreadsheets, and formal sales projections, need to be identified and marked as needing to be retained for 7 years. Other companies interpret this to mean that all documents and emails from certain people, like the CFO, or during certain time frames should be retained for 7 years. Still others leave the decision up to the individual staff members as to whether a document falls into this retention category and treat it appropriately.

There are several problems with this approach. First, it is not just the formal documents that can contribute to a financial decision. There could be a string of emails between the CEO and his buddy who is on the board of directors at another company discussing their golf tournament next week in Arizona. Yet in that conversation, the CEO asks about a certain financial strategy he is investigating, and the Director cautions him against doing it. In none of the above interpretations would this email be retained for compliance, yet it could have been the most important impact on financial decision for the company. It would not have been considered a formal document, nor did it involve the CFO, nor would the CEO have likely thought to include it himself as a business document meeting compliance regulations.

User error is a major problem with categorization. When users control record categorization, some documents that should be retained as business documents are not, and vice versa. A harmful type of user error is when a user has purposefully not categorized a document for retention because of something that might be self-incriminating, yet would protect the company in a compliance audit, such as some wrong-doing or error in his judgment.

The original reason for categorization was to avoid accumulating too many documents because that would increase physical space requirements and costs of offsite storage. Too many documents would also slow retrieval if the need arose because there would be fewer documents to have to wade through. This is based on an outdated reality. With electronic documents like email, storage space is plentiful and cheap, and with several of the email archiving and retrieval software programs on the market today, it doesn't matter if there are terabytes of records, the search and retrieval are immediate.

The final reason why categorization is a mistake is because there is no way to know for sure, at the time of creation of the email, that it may or may not be required during a future compliance audit or investigation. This is why it would be ideal to keep every record, instead of trying to have your staff inconsistently make guesses as to which documents should be retained and which should not.

Action: Avoid manual and automatic categorization of documents, archive every document.

Conclusion

There is a multitude of federal, state and industry regulations that affect email, and which have elevated the importance of email for nearly every organization. However, since email has been a technology that has been "under the radar" for so many years, most companies have neglected to address the changing nature of email communications as such a critical asset.

Due to this lack of attention and action, most companies may not even realize the extent to which lack of email awareness, polices, retrieval, and workforce education contributes to the increased risk the company is under. Companies will need to more actively manage how their workforce uses email.

Organizations must take action and initiate change in order to avoid breaking compliance regulations. They will need to educate employees how to create emails with care in order to avoid email-borne risks that can devastate a company. Email policy enforcement is a critical component to creating a culture of compliance. Without a system to keep management aware of policy breaches, a policy is worthless.

Gain Significant Other Benefits
Only with the latest email archiving systems can email records be produced in seconds instead of days or weeks. This can mean the difference between meeting compliance audit requests or not.

Additionally, when email is archived for longer periods, there are trend analyses, behavioral patterns and profiles of how email is used within a company that can be very useful in such things as reducing storage, eliminating MP3 files, identifying those who abuse email for personal reasons, and changing policies to improve business.

By implementing an email management archive system, companies will be able to better respond to a subpoena, compliance audit or investigation in a quick and efficient manner. This system can have the long term benefits of helping a company educate users, change their behavior and enforce new policies, making businesses run better. This is after all, the underlying goal of regulatory compliance.

Anthony Sanchez
VP of Marketing
Waterford Technologies

Anthony Sanchez is a technology, Internet and email veteran, having nearly two decades of experience as a technology marketer.

He is currently VP of Marketing for Waterford Technologies, Inc., an Email Management, Archiving and Compliance software developer.

He has also worked at a major ISP, at a leading e-security company, and for over a decade at Oracle Corporation.

For more information on Email Archiving and Compliance, go to www.mailmeter.com.