

# From Policy to Practice: The State of Enterprise Messaging Compliance



an Osterman Research white paper  
sponsored by MessageGate, Inc.



## Executive Summary

---

Osterman Research has found that only 60% of surveyed companies have policies in place to address e-mail and instant messaging risks. Of those, only 14% (1 out of 7) have deployed a tool to enforce them at a system level.

The fact that six in seven enterprises have no tool in place to mitigate against email and IM communications risks means that the vast majority of enterprises face enormous liability in the normal operation of their messaging systems. The 40% of enterprises that have no policies face even more significant exposure to risk and potential for loss due to the absence of proper controls and oversight measures.

*What enterprises need is a mechanism that can help them to enforce corporate policies, help them comply with government regulations, help them archive information and provide a defense against messaging-borne threats.*

The impact of not adequately managing messaging infrastructure with formal policies and system tools means that enterprises:

- Face an increased risk of failing to adequately satisfy government-imposed regulatory requirements.
- Put intellectual property and customer data at risk.
- Face an increased risk of an adverse judgement during a legal action.
- Fail to optimize the storage of their messaging systems and, hence, the performance of these systems.
- Are less productive because users spend time on tasks that otherwise could be handled more efficiently through automation.

When large organizations were asked about the level of liability created by email, 34% responded that the liability was in the "hundreds of thousands of dollars", while 40% felt that the liability was in the millions of dollars.

What many enterprises need, therefore, is a mechanism that can help them enforce corporate policies, comply with the growing maze of government regulations, archive information that must be kept for long periods, and provide an adequate defense against messaging-borne threats.

Despite this need, Osterman Research has found that nearly 50% of large organizations are either not making sufficient

investments in compliance-related messaging products and services, or they are unsure about the adequacy of their investments.

This white paper discusses the results identified above in more detail and presents a solution offered by MessageGate that can address this need.

## Messaging Priorities

---

What messaging concerns are important to large enterprises? In a survey conducted by Osterman Research in November 2004, we found the top ten list to include:

- Protecting intellectual property
- Avoiding legal liability
- Enforcing corporate email policies
- Ensuring compliance with regulations
- Reducing storage requirements
- Enforcing regulatory compliance in messaging

Interestingly, six of the top ten priorities for large organizations are directly connected to policy-related compliance and enforcement for the enterprise. Rounding out the list were the on-going challenge of virus protection, reducing the nuisance of spam, reducing overall email infrastructure costs as well as providing central control and administration of the messaging system.

*This shift from external threats to internal risks and considerations is a major trend for large organizations.*

This shift from external threats to internal risks and considerations is a major trend for large organizations. Over the past ten years, there has been a major shift in how companies generate and process information. Up until the early 1990s, most information was created and accessed via paper. Paper documents were the most common medium for transmitting information in the enterprise and even most electronic documents were printed and stored on paper. However, during the past ten years there has been a shift from the paper world to an online one with e-mail at its core.

According to an analysis from the University of California at Berkeley, 93% of all information today is created in an electronic format. Furthermore, more than 70% of that information is never printed. Today, users feel comfortable receiving, reading and saving information in a purely digital format and most of this information is sent and received via

email. Email has become the de facto communication standard for most organizations and the messaging system and associated archives represent a large portion of most organizations' intellectual property.

Email and other types of electronic messaging grew up somewhat organically. Unlike other applications, such as financial systems, for example, there were few controls or policies established for the use or retention of these messages. For the most part, these systems emerged without policies and controls on what types of information need to be saved, how long it needs to be saved, where it needs to be saved, and so forth. A key reason for this lack of formality with regard to email has been the fact that many organizations viewed email as informal and a sort of 'unofficial' communication medium.

## Policy Enforcement

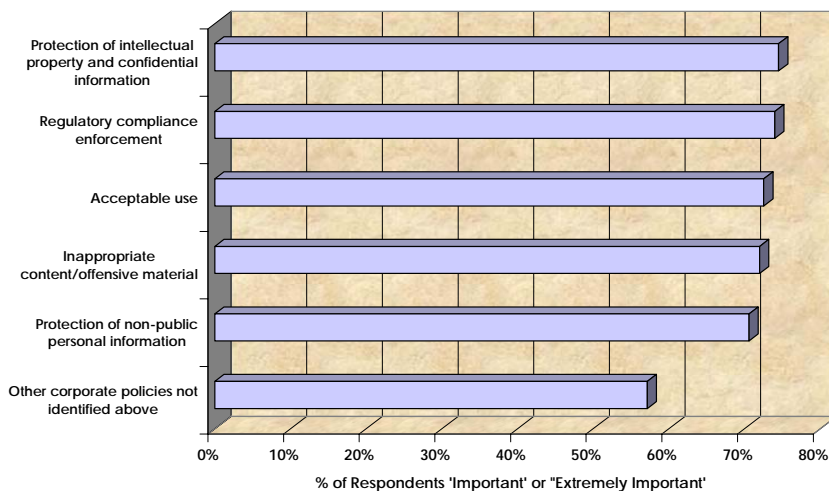
*Among those organizations that monitor messaging systems:*

*- 65% of organizations find emails that violate corporate policies at least weekly or more frequently*

*- 22% of organizations find violations on a daily basis.*

In the Osterman Research survey mentioned above, we found that protection of intellectual property and confidential information was deemed as important or extremely important by 75% of large organizations, as shown in the following figure.

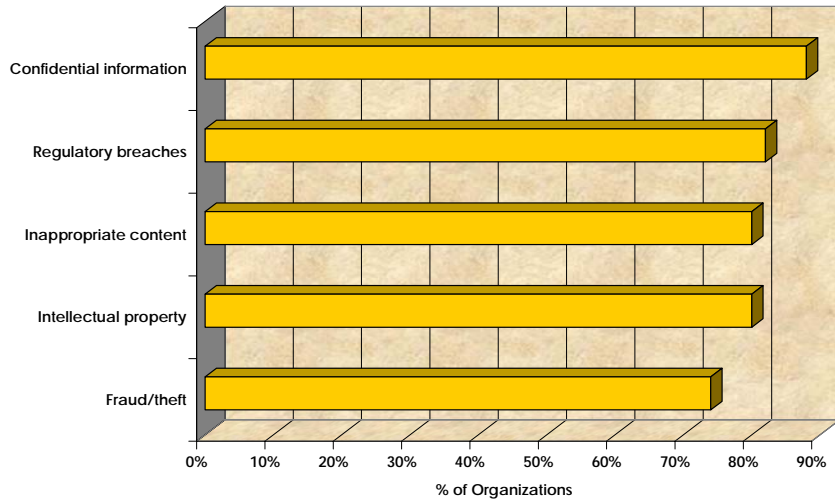
**Importance of Various Corporate Policies**



Further, when large organizations were asked what they would look for in email if they could monitor it, we found that 88% of organizations would look for confidential information, 82% would look for regulatory breaches, 80% would look for

inappropriate content and intellectual property, and 74% would look for fraud or theft, as shown in the following figure. Clearly, large organizations want to look for email-borne content that could be damaging to their reputation or business activities.

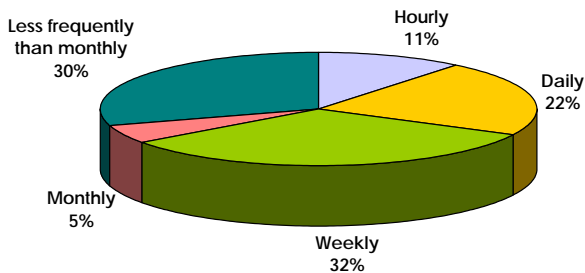
**Content that Organizations Would Search For in Email**



*When emails have been disclosed during the course of a complaint or action or in defense of one, 68% of organizations have removed personnel as a result, while 46% have suffered damage to their reputation.*

The absence of tools in place to bolster corporate policies is a serious problem: the Osterman Research survey found that among those organizations that monitor messaging systems, 65% of organizations find emails that violate corporate policies at least weekly – 22% of organizations find violations on a daily basis, as shown in the following figure.

**Frequency With Which Emails Are Discovered That Violate Corporate Policies and Regulations**

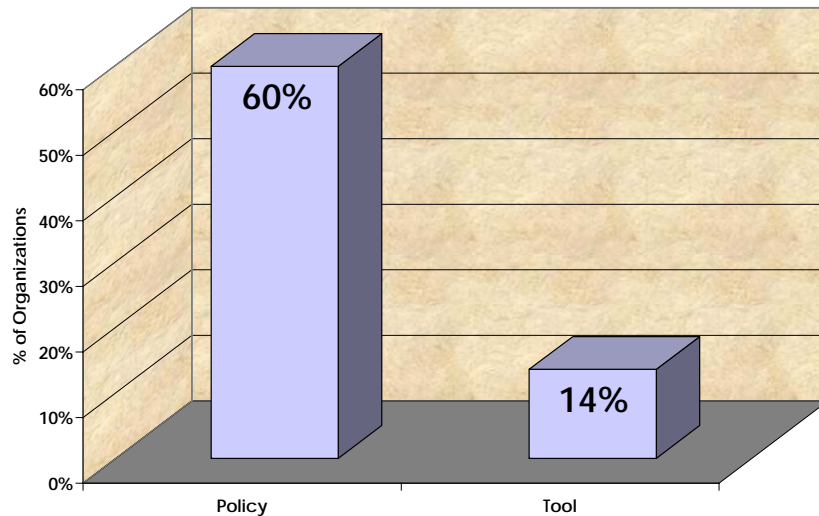


Underscoring the potential severity of policy violations, when emails have been disclosed during the course of a complaint/action or in defense of one, 68% of organizations have removed personnel as a result, while 46% have suffered damage to their reputation.

Many enterprises have established policies for managing email and IM communications risks, such as leaks of intellectual property or trade secrets, hostile environment issues, dissemination of confidential information and the like. However, Osterman Research has found that only about one in seven (14%) enterprises have deployed any sort of tool to prevent these risks, as shown in the following figure.

*Many enterprises have established policies for managing email and IM communications risks...[but] only about one in seven enterprises have deployed any sort of tool to prevent these risks.*

**Organizations That Have Deployed Policies or Tools To Prevent Email/IM Communication Risks**



The fact that six in seven (86%) enterprises has no tool in place to mitigate against email and IM communications risks means that the vast majority of enterprises face enormous liability in the normal operation of their messaging systems. Further, while 60% of enterprises have policies to address email and IM communications risks, 40% do not. This means that 40% of enterprises face even more significant potential for loss of corporate data through their messaging system.

## Regulations: Driving Compliance Initiatives

*...virtually all organizations must satisfy statutory information security and record retention requirements...*

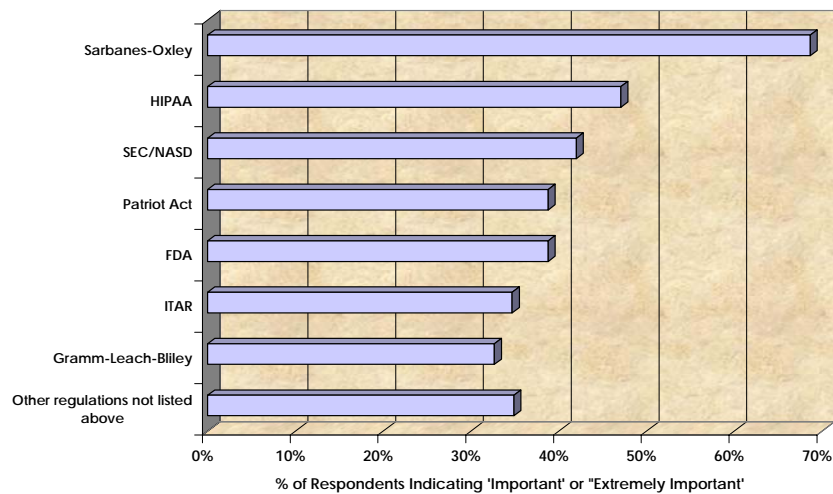
Industries that are heavily regulated, such as financial services, energy, or healthcare, must meet a variety of statutory requirements with regard to information control and records retention. For example, the Securities and Exchange Commission (SEC) imposes a series of requirements on broker-dealers including proper supervision and preservation of email and IM communications.

In addition, virtually all organizations must satisfy statutory information security and record retention requirements, including line of business specific requirements such as the Gramm-Leach-Bliley Act designed to safeguard personal financial information as well as guidelines from entities like the Federal Energy Regulatory Commission (FERC) on proper information sharing and operational partitions among business units. Other statutory drivers include the Americans with Disabilities Act, the Age Discrimination in Employment Act, and the Occupational Safety and Health Act; as well a variety of state, international and other requirements.

Although many information security and records retention requirements do not impose specific requirements on email or instant messages, Osterman Research has found that approximately 80% of enterprises use email for closing orders or performing other types of business transactions. As a result, email is increasingly home to a greater proportion of corporate and other records, and so increasingly is subject to existing information security and records retention requirements.

With regard to the importance of various regulations, in the Osterman Research survey mentioned earlier, we found that 69% of large organizations view Sarbanes-Oxley compliance as either important or extremely important, as shown in the following figure. Nearly one-half of organizations view the Health Insurance Portability and Accountability Act (HIPAA) as this important, while a variety of other regulations, such as the Patriot Act and Gramm-Leach-Bliley are viewed as very important by a large percentage of large organizations.

### Perceived Importance of Various Regulations



*The ease with which data can be sent makes email a natural avenue by which employees can distribute all sorts of confidential and otherwise sensitive data outside of an organization...*

That said, preventing and correcting breaches of corporate policies and government statutes is not a trivial exercise. The ease with which data can be sent makes email a natural avenue by which employees can distribute all sorts of confidential and otherwise sensitive data outside of an organization, often without any intention of violating a corporate policy or regulation.

### Intelligent Archiving: Why Categorize Email?

Osterman Research found that among large organizations, about one-third are not yet archiving, but plan to do so in the relatively near future. Further, while it is important to archive content that must be preserved, it is equally important not to archive content that can be discarded. By properly managing the content of the archive through intelligent classification of the indexed data, storage costs decline because less content is being stored (or stored more cost effectively) and retrieval effort is reduced due to the speed, accuracy and relevance of retrieved content categorized as it is archived.

Consider the following derived from recent Osterman Research surveys:

- Most enterprises that are not heavily regulated, such as organizations outside of the financial services industry, are not satisfying the minimum data

retention periods imposed by the array of statutory requirements for records retention.

- For the most part, enterprises view their preparedness for regulatory compliance to be inadequate.
- Enterprise satisfaction with the current ability to search for and find needed information from the messaging archive or backups tapes is, at best, modest.

Current practices by most non-regulated enterprises make it very difficult to recover old email during legal discovery, during a regulatory agency's audit or other form of investigation or review.

*Even outside of the financial services industry – the most heavily regulated industry with regard to the preservation of email and IM communications – there are a vast array of data retention requirements that affect almost all industries and enterprises within those industries.*

However, during the past three years, the IT departments of nearly three in four enterprises Osterman Research has surveyed has been required to search through backup tapes to retrieve one or more emails in response to a request from their legal department, human resources department or some other entity. About 40% of enterprises have been ordered by a court or regulatory body to produce employee email. Compounding the problem is the fact that message stores are growing rapidly, increasing 32% in volume during the 12 months ending in October 2004. Nearly 40% of enterprises are experiencing message store growth in excess of 25% per year.

In those instances in which enterprises cannot or do not produce old emails, the consequences can be severe; for example:

- In *Zubulake v. UBS Warburg*, in which the judge in the case ruled that a new standard should be established for evaluating whether the plaintiff or the defendant bears the cost of electronic discovery. The judge took a decidedly pro-plaintiff approach, meaning that defendants may be more likely to be charged for the costs of electronic discovery.
- Five Wall Street brokerage houses – Deutsche Bank, Goldman Sachs, Morgan Stanley, Salomon Smith Barney and US Bancorp – were fined a total of more than \$8 million by the SEC in December 2002 because these firms did not retain certain emails for SEC-mandated retention periods and for other infractions of SEC rules.

Much of the data in a messaging system, however, and the records contained in the message store, comprise important corporate assets. Despite this, most enterprises do not have any tools or policies in place to properly categorize or classify e-mail as it is archived. Only about one in five enterprises has deployed systems to prevent important data from being lost, while about three in five enterprises have either no systems or policies in place, or they have not sufficiently considered the issues involved in appropriately managing their information.

*Most enterprises that are not heavily regulated, such as organizations outside of the financial services industry, are not satisfying the minimum data retention periods imposed by the array of statutory requirements for records retention.*

Because most enterprises do not have any mechanism in place – not even a policy – about how messaging system users should preserve critical, long term data from the messaging system, they place their organizations at significant risk of non-compliance during a regulatory audit or legal action, not to mention the significant productivity loss that results from an inability to access old information. Even outside of heavily regulated industries like financial services or healthcare, the lack of records retention practices and policies could have important and damaging long-term consequences for an enterprise faced with a lawsuit, a regulatory action or other requirement to produce older messaging data.

There are a vast array of data retention requirements that affect almost all industries and enterprises within those industries. Here are a few examples:

- The Occupational Safety and Health Act requires that records of monitoring exposure to hazardous materials must be kept for 30 years.
- The Employee Retirement Income Security Act of 1974 requires that any correspondence, inquiries or notes relating to individual eligibility determinations be kept indefinitely.
- The Toxic Substances Control Act requires that employee claims of occupational disease or occupational health problems be kept for 30 years.
- The Age Discrimination in Employment Act requires that records relating to the promotion, demotion, transfer, selection for training, layoff, recall or discharge of an employee be kept for one year from the date of the personnel action.

- Something as simple as an email sent by an employee to her supervisor requesting vacation time constitutes a personnel record according to the Equal Employment Opportunity Commission's interpretation of Title VII of the Civil Rights Act of 1964 – personnel records under this statute must be kept for a period of one year.

Because of the growing proportion of corporate records that are sent through and stored in email, it is critical that virtually all enterprises establish email retention periods that correspond to the minimum requirements set forth by statute. Although statutory requirements and protection from lawsuits are often the primary reasons for archiving messaging system data, there are a variety of benefits that accrue from an intelligent archiving approach utilizing policies to categorize and classify messages. Enterprises should evaluate their internal and external requirements for message categorization and retention and determine how best to deploy an intelligent archiving approach.

*Due to the exploding volume of email that can be retained, it is critical that companies can selectively set retention periods and actions based on content.*

## From Policy to Practice

---

Once an organization realizes that it must monitor its messaging systems in order to prevent the misuse of corporate and personal email, to prevent the loss of confidential and other sensitive information, and to maintain compliance with statutory requirements, there are four primary considerations for any system that can protect the organization from these threats:

- First and foremost, the system should intercept content *before* it is sent and can do damage to an organization. Post-send review is simply not an option for an organization that wants to prevent problems before they occur. Osterman Research found that pre-send interception of messaging content is deemed important or extremely important by 61% of large organizations.
- The solution must be scalable. Osterman Research has found that message volumes are increasing at the rate of 32% annually, meaning that the volume of emails and attachments processed by an organization will increase dramatically over the next

few years. Further, any solution must be able to handle peak traffic loads so that message delivery is not impeded. Osterman Research found that scalability is one of the top three concerns for messaging security and compliance products and services.

*Secure messaging will become a much higher profile requirement in organizations of all sizes during the next several years.*

- The system must be easy to deploy. Given that IT is generally overworked in most organizations, adding another burdensome system to deploy and monitor will not be effective for most organizations. That said, Osterman Research found that the information security and messaging-related IT functions represent two of the top three functions in organizations that are aggressively pushing for messaging compliance measures. These two functions, along with the CIO and IT operations, are typically those that have primary responsibility for enforcing network and information security policies related to email usage.
- The system should have a highly flexible policy server that enables companies to build custom policies that address their specific needs. This flexibility should include a broad set of message actions, detailed messaging analysis, and the ability to easily integrate with existing corporate systems for policy-related information.

## The MessageGate Approach

MessageGate enables large companies to secure their corporate messaging systems against corporate and regulatory policy breaches. MessageGate specializes in high-volume, large-user environments that need to easily configure policies to address their specific areas of concern.

MessageGate's solution provides companies with measurable business improvements in the following areas:

- Risk identification & mitigation
- Cost reduction
- System efficiency

MessageGate strongly advocates an audit-led approach to messaging compliance. This approach enables companies to start the compliance process with a low-cost audit that

provides deep insight into a company's current messaging activity. This insight becomes the basis for a messaging compliance strategy that may or may not require the installation of new software to monitor messaging traffic. In addition to diagnostic messaging audits, MessageGate provides the following offerings:

- On-going audit services for monitoring and reporting purposes
- Real-time email monitoring and control software
- Intelligent archiving software to reduce storage costs and improve information retrieval

MessageGate has substantial experience addressing issues related to e-mail compliance, policy enforcement, and security. Their professionals include both domain experts with deep industry knowledge and email expertise and technical experts with backgrounds in pattern analysis, electronic communications, and behavioral methods.

For more information visit [www.messagegate.com](http://www.messagegate.com) or email [info@messagegate.com](mailto:info@messagegate.com).

MessageGate, Inc.  
10900 NE 8<sup>th</sup> St., Ste. 1300  
Bellevue, WA 98004  
425-460-5060  
877-544-8500

© 2005 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed outside of the client organization that has purchased it, nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.