



The New Compliance Imperative

Electronic Communications as a Source of Risk & Accountability

A MessageGate Whitepaper

May 2004

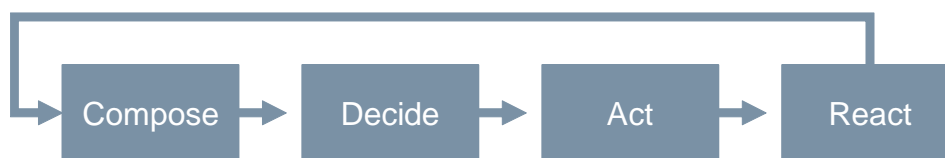
New Realities

E-mail has evolved to being the most mission critical application in the enterprise today. According to the Radicati Group, the typical corporate user receives an average of 81 e-mails per day and sends 29 per day resulting in some 32 billion e-mails a day in 2003. The study also demonstrates the explosive growth in usage citing an 80% increase over the previous year and forecasting over 82 billion e-mails in 2007. This number does not even take into consideration the malicious or unsolicited e-mail that requires organizations to have anti-virus and anti-spam technologies in place. Close on its heels is Instant Messaging (IM) created as a personal communication tool, but rapidly being adopted for enterprise use.

As e-mail has become a workflow tool, its relevance has begun to deteriorate in many ways. Users are copied and blind copied as both a courtesy and requirement. E-mail has replaced memos, voice mails, and face to face meetings as a means of sharing information and getting work done. In fact, according to a META Group study, 80% of company personnel prefer e-mail over telephone conversations citing the ability to communicate easily with multiple parties and the creation of a paper trail as the top reasons. Periodicals, newsletters, order confirmations and personal e-mails among other things make up a substantial portion of "opt-in" email traffic further adding to the volume of message activity in the enterprise. IM traffic is surging through the enterprise being used in both productive and unproductive ways. A June 2003 study by the Radicati Group projects the number of active IM accounts to grow from 590 million today to over 1.4 billion by 2007 with the ratio of consumer to corporate accounts changing from 9 to 1 to 3 to 1.

As these methods of electronic communications have matured in both functionality and usage, organizations are realizing the benefits from a more connected business world while at the same time beginning to understand that this type of free form connectivity and communication comes with inherent risk. This risk is forcing companies to create and enforce email specific privacy policies.

E-mail and IM are unstructured in their nature meaning that there are limited constraints on what can be said, who can be addressed, or what kinds of attachments can be sent. Users take four different and distinct steps as they communicate:



1. Compose:
 - Begin an e-mail or an IM conversation (new or reply) with a recipient or recipients in mind
 - Driven by business requirement or personal need
 - Message is created and edited several times before finalization
2. Decide
 - Final wording in place
 - Confirm recipient or recipients
 - Decide on who to CC or BCC
 - Confirm message content and any attachments

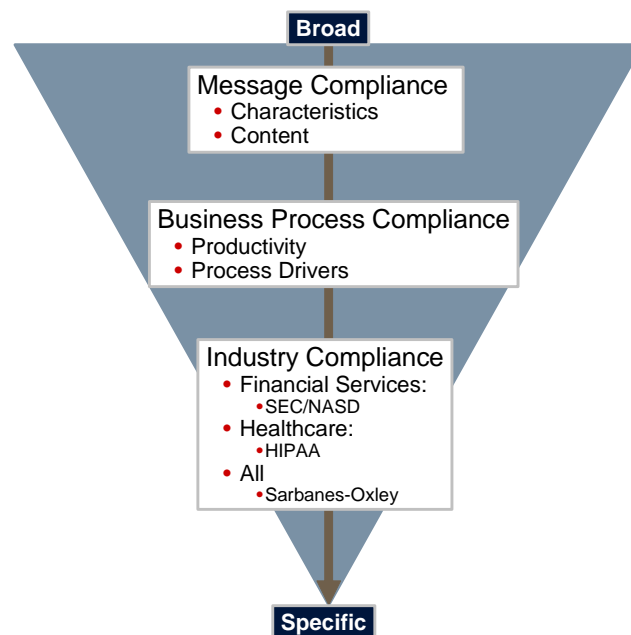
3. Act
 - Hit "Send" OR
 - Save to "Draft" OR
 - Delete and close out
4. React
 - Wait for a response OR
 - Forward response OR
 - Print response OR
 - Reply - start process over

The purpose, intent, and timing of each of these steps varies from user to user and situation to situation making this activity difficult to control and even more difficult to anticipate. Organizations are struggling to mitigate the risk of these unconstrained activities by attempting to control what users do and say as they communicate with these tools. The New Compliance Imperative requires all organizations to carefully examine electronic communications as a source of risk and accountability and to act with technology and processes to regain control over this mission critical enterprise asset.

Compliance Defined

Compliance can be defined in many ways depending on the organization, industry, or regulation in question. The compliance framework defines three distinct types of compliance moving from broad applicability to all industries to very specific industry-based needs:

The Electronic Communications Compliance Framework



Source: MessageGate

1. Message Compliance - broadly applicable to all organizations covering both the content and characteristics of a message and driven by business policies and limiting legal liability

Examples include the number of recipients, the language used, attachment sizes, or confidentiality breaches (intended or unintended)
2. Business Process Compliance - specific to functions and is driven by productivity concerns and a lack of true visibility

Examples include how e-mail is used for selling, managing customers, or certain purchasing activities
3. Industry Compliance - specific and generally driven by external factors such as a regulatory authority

Examples include the SEC & NASD regulating how broker/dealers archive and supervise electronic communications, HIPAA regulations related to the sharing of Protected Health Information (PHI), or ITAR regulations for export control. Coming quickly is Sarbanes Oxley compliance and, specifically, how firms will address electronic communications under Section 404 - Internal Controls.

All organizations need to reduce the risk of non-compliance through documented appropriate use policies or specific individuals or functional groups dedicated to compliance activities. Firms have both inside and outside legal counsel to mitigate risks and address situations as they arise while brokerage firms have compliance and surveillance organizations. In companies dealing with healthcare or health related issues, there is typically a designated Privacy Officer responsible for maintaining reasonable and appropriate controls over patient privacy.

Electronic communications is inherently risky with great difficulty in controlling and anticipating user activity. The New Compliance Imperative requires a control system that mitigates risks where possible and can engage human judgment where required.

High Stakes

Non-compliant activities can impact an organization on many levels from reputation damage, to legal liability, to stock price declines. In the wake of the recent Wall Street scandals, one leading firm saw their market capitalization decline by over 25% when e-mails were released that revealed the inappropriate and unethical treatment of certain stocks. Firms that have public trust built into their share price run the risk of substantial declines if non-compliant activity is allowed to occur and is then made available to the public in the form of e-mails.

Less tangible, but as important is damage to reputation and brand which can haunt an organization as one pharmaceutical firm learned after inadvertently releasing the names and email addresses of a group using an e-mail reminder service. The service sent an e-mail when it was time to take or refill a prescription for an anti-depressant. Almost 700 people had their names and e-mail addresses disclosed when their information appeared in the "TO" field of an e-mail reminder.

The costs extend to fines and sanctions imposed by regulatory authorities. The Brokerage industry's record \$1.4 billion fine to settle charges related to Research and Investment Banking activities was a bellwether in the industry which supplied

the wake up call for Compliance departments and executives alike. Regulatory compliance moved from being necessary to do business to being essential to stay in business.

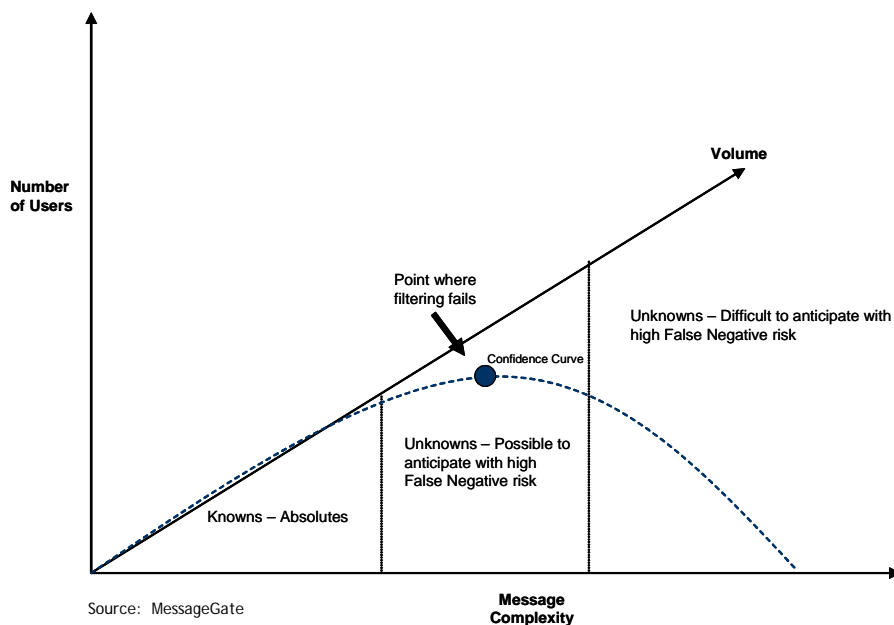
Even more exposure comes from legal liabilities occurring as the result of inappropriate communications or non-sanctioned activities of employees acting on behalf of their firm.

Regulations aimed at protecting consumers and shareholders must be at the top of risk management programs. Every Healthcare organization, payor and provider alike, must have reasonable controls in place to safeguard patient's private health information as well as a designated Privacy Officer to perform the oversight function. Sarbanes Oxley requires management teams to sign off on their books citing knowledge that they are complete and without fraud. The pervasiveness of electronic communications in all organizations requires a system in place that can monitor and control what is communicated and how.

Harsh Realities

The reality of stopping non-compliant activities before they occur via electronic communications is complex. Very quickly, one moves beyond 'Knowns' or 'Absolutes' to circumstantial or exception scenarios. For example, inappropriate/offensive words and phrases are generally known and agreed to as inappropriate and thus they can be accurately filtered out of the message flow. As one moves further away from "Knowns" the risk of "False Positives" (what I don't want to catch) increases as does the risk of "False Negatives" (what I should have caught).

The figure below details this situation as complexity and users grow along with the volume of electronic communications. One quickly leaves "Absolutes" behind and must face the prospects of both False Positives and False Negatives. The Confidence Curve begins a steep decline when one leaves "Absolutes" pointing to the limits of basic filtering and highlighting the need for policy-based monitoring and enforcement. Automation alone cannot effectively manage compliance activities. However, automation combined with the expertise and insight of those responsible for risk management and compliance can.



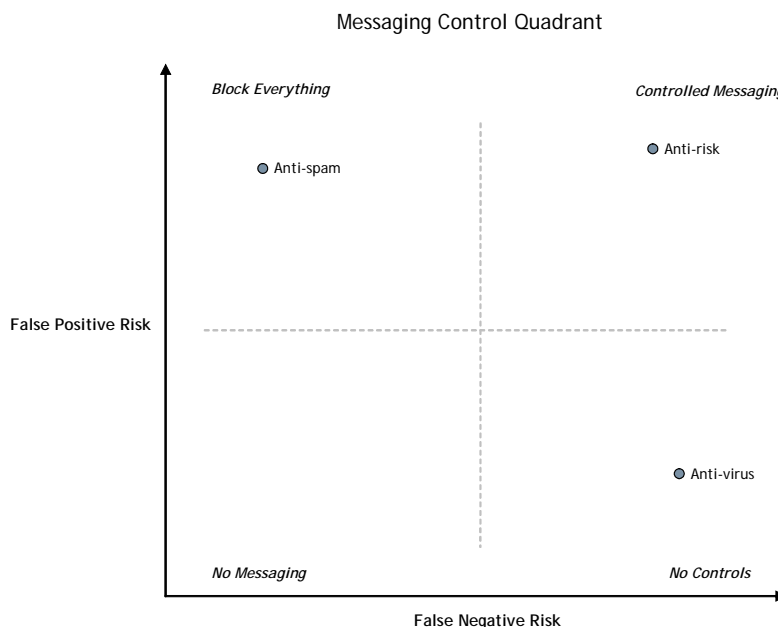
In many cases, judgment is required to make the final decision on what is or is not allowable or acceptable. This judgment can reside in many places from the user who created the email to the supervisor who must review it to the executive who has final say. Critical and crucial is to provide each of these users with relevant information about what is or is not compliant. A system to manage and control electronic communications must provide intuitive, user-focused interfaces that provide the right information at the right time and in the right amount.

Absolutes can be accurately blocked from occurring. Areas of exposure where rules and policies exist can be sampled or filtered to mitigate risk. Arguably the largest source of risk is False Negative exposure and this is managed through policy enforcement and monitoring. All messages are not risky, but those that are must be identified and dealt with efficiently and effectively.

Lessons Learned

Efforts to control spam, viruses, and other types of unwanted e-mail highlight the challenges and complexities faced by compliance initiatives in electronic communications. Both technology vendors and their customers have become very aware of the complexities, realities, and trade offs required to deploy an effective system to control these types of messages. Any vendor not firmly rooted in this experience is not prepared to address the New Compliance Imperative and organizations will demand this level of knowledge as they choose technologies.

The Messaging Control Quadrant below illustrates the interrelationship that exists among anti-spam, anti-virus, and now, anti-risk efforts. Anti-risk describes the compliance solutions designed to help organizations address the New Compliance Imperative across the enterprise.



Source: MessageGate

Enterprise struggle with the trade-offs between doing too much or doing too little with regard to messaging control. The initial challenges were around protecting against the threat of viruses or the nuisance of spam. The New Compliance

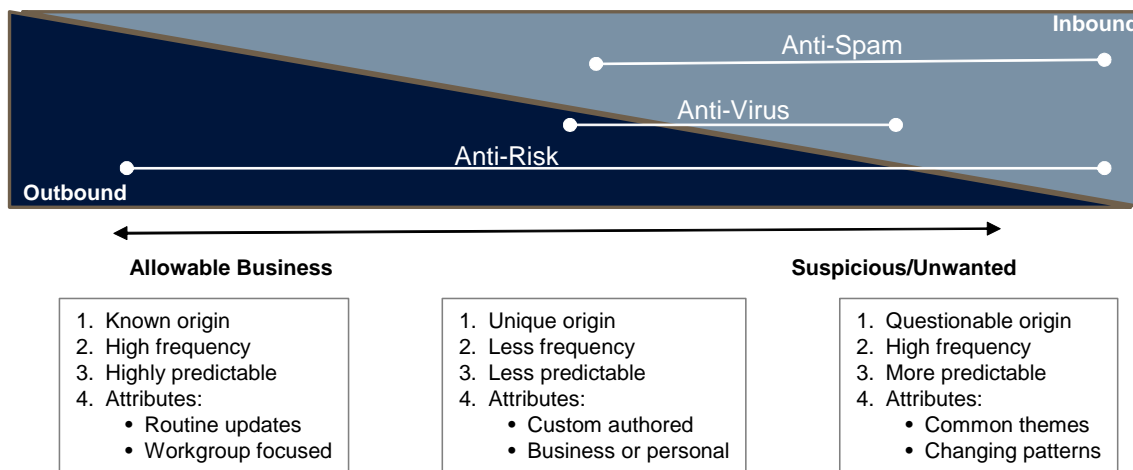
Imperative requires firms to have an integrated approach to controlling messaging through a comprehensive anti-risk solution.

Anti-virus solutions have high false negative risk meaning that a missed virus can cause infection and widespread damage in a corporate e-mail system. However, the false positive risk is low as this merely leads to a quarantine of the message and review/release by the IT organization. At worst a file is stripped from a message before it arrives to its intended recipient.

Anti-spam solutions have a higher false positive risk meaning that misidentifying a message as spam can lead to communication disruptions as a perfectly legitimate message is blocked from delivery. However, the false negative risk is low resulting in annoyance and unwanted messaging traffic.

Anti-risk solutions are quite different in that they have both a high false positive risk and high false negative risk. A false positive can lead to workflow disruption, irrelevant results in a supervisory environment, and overall volume challenges as messages have limited relevance due to the sheer number identified. A false negative can lead to regulatory fines, legal liability, reputation damage, and various other types of direct and indirect costs. Although both false positive and false negative risks are high, firms must embrace anti-risk solutions as part of the New Compliance Imperative.

Anti-virus and anti-spam have historically focused on inbound suspicious and unwanted messages where as an anti-risk solution is focused primarily on outbound messages that are generally allowable business communications. These allowable business communications are the focus of compliance activities and where a policy enforcement solution is so critical. The importance of anti-spam and anti-virus capabilities compared to anti-risk efforts is further detailed in the chart below.



Source: MessageGate

Anti-virus configurations are historically defined based on what has been seen before and faces a continually changing range of messages, characteristics, and attributes to identify and stop. Further complicating this is that the originators of

viruses are increasingly more sophisticated as they attempt to counter solutions put in place to stop them.

Anti-spam, much like anti-virus, utilizes historically defined configurations to block these types of messages. They too face a continually changing array of messages that are designed to circumvent these types of solutions. Best in class anti-spam capabilities move beyond historical definitions and into sender validation, message authentication, and intelligent filtering among other things as they combat spam in the enterprise.

Although both false positive and false negative risks are substantially higher for anti-risk solutions, the ability to solve the problem is more certain. Electronic communications in the enterprise are defined by historical patterns, by senders & recipients, by content related to the business, and by defined risks related to corporate and regulatory policies. Having the scope of messaging defined at this level makes it more addressable and solvable with an anti-risk solution.

Getting Started

The New Compliance Imperative is a strategic priority that requires business driven policies and a flexible technology deployment to enforce them. There are message compliance opportunities that will apply to every individual in an organization as well as specific business or regulatory policies that may apply to very few individuals.

For example, everyone in an organization is prohibited from sending documents marked "Internal Use Only" to external recipients. This is a straightforward policy that can be easily enforced at the perimeter of an organization. However, the policies that govern electronic communications between functional groups (inter-group boundaries) are specific to a limited number of users in certain business units and can be driven by regulatory or corporate policy requirements.

The key is to start with the issues that are most pressing from business perspective and evaluate how they might translate into policies to enforce in electronic communications. With a tool in place, policies can then be expanded iteratively to focus on the most pressing much over time.

Conclusion

The sheer volume and complexity of electronic communications makes the task of compliance daunting. The New Compliance Imperative requires technology and processes that can separate non-compliant messages from those that are compliant while equipping the individuals responsible for oversight with the tools to apply sound business judgment where required.

The technology to accomplish this task must be proven at an enterprise scale and possess the institutional understanding of what it takes to monitor and control electronic communications. Organizations that embrace the New Compliance Imperative will regain control over their corporate messaging systems and benefit from reductions in risk and improvements in overall productivity.