

Internal Email Control

Its Essential Role in Compliance Management

A Whitepaper By:

Nemx Software Corporation

14 Poplarwood Avenue
Ottawa, Ontario K2S 1V3
Canada

Internal Email Control

— Its Essential Role in Compliance Management

TABLE OF CONTENTS

Introduction.....	2
Why Internal Email Control Is Needed	2
Internal Email Control As It Relates To:	3
Regulatory Compliance	3
Internal Corporate Policy Compliance.....	4
Architectural Requirements for Internal Email Control	5
Limitations of “Appliance” Solutions	6
The “If You Can’t See It You Can’t Monitor It” Problem	6
The “Who Are You and What Are You Permitted To Do?” Problem.....	6
Internal Email Control – An Effective Approach	7
Product Considerations	8
Integration with Corporate Mail System	8
Integration with Corporate Authentication Systems.....	8
Encryption & Digital Signatures.....	8
Intelligent Content Analysis – Concept Scanning.....	9
Conclusion.....	9

Internal Email Control

— Its Essential Role in Compliance Management

Introduction

Hardly a day goes by without another example surfacing of how a breakdown in corporate compliance is linked to email. No wonder, with 103 billion corporate emails a day projected for 2008¹. The sheer volume of electronic correspondence guarantees literally every company will experience a serious incident of non-compliance resulting from their use of email — whether they know about it or not!

Any uncontrolled use of email can lead to violations of both government regulations and internal corporate policies, with consequences that can range from employee lawsuits, to substantial government penalties, even to irreparably damaged brand and corporate reputation affecting sales and customer retention. Protecting your organization against all these risks, liabilities and costs is crucial.

The sheer volume of electronic correspondence guarantees literally every company will experience a serious incident of non-compliance

A truly effective compliance strategy is proactive and preventative in scope and would, by necessity, require every email message be managed with consideration for both regulatory and corporate policy. Yet, most organizations have focused their email compliance efforts on only their inbound and outbound traffic—a mere 15% of their total corporate email volume!

Why Internal Email Control Is Needed

If there were only one reason internal email control is needed it would simply be because there's 8 times as much of it (i.e. email between employees) as all other inbound and outbound traffic combined. Put another way, a corporate security or compliance policy violation is 8 times more likely to occur within internal email than outgoing.

Compliance violations are 8 times more likely to occur within internal email than outgoing

Of course, volume isn't the only reason. While outbound email control currently occupies the publicity spotlight, and for valid reasons, many of the driving factors that have pushed it to the forefront of corporate attention substantiate the immediate need for internal email monitoring and control as well.

Consider, for instance, the following:

- According to IDC's 2005 Security Survey, employees following security policies was rated as the second-highest security challenge organizations will face over the next 12 months
- Less than half of email users always comply with corporate email policies²
- Trusted employees deliberately or inadvertently distributing sensitive information are quickly becoming a major concern in many organizations³

¹ Source: Radicati Group Inc., "Active Policy Management – Third Generation Compliance for Today's Corporate Environment" Whitepaper February 2005

² Source: Harris Interactive, market research

Internal Email Control

— Its Essential Role in Compliance Management

- Nearly 50% of corporate email users have sent or received inappropriate content
- A 2004 survey by the American Management Association and the ePolicy Institute revealed that 20% of responding companies have had employee email subpoenaed in the course of a lawsuit or regulatory investigation—and if you think this is just a big company issue – wrong, 51% of respondents have fewer than 500 employees
- Regulations relating to Sarbanes-Oxley, SEC and NASD, impose requirements that reach *inside* the organization and impact *internal* email communications – such as the requirement to restrict information between analysts and brokers, or demonstrate “evidence of control” for financial information distribution, or the protection of personal confidential information

Bottom line, including internal email monitoring and control to the scope of your compliance strategy and efforts is the only way to achieve 100% compliance and peace of mind.

Internal Email Control As It Relates To:

Regulatory Compliance

Various laws and regulations, such as Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLBA), Health Insurance Portability and Accountability (HIPAA) and NASD 2711 have been enacted with the goal of not only enhancing corporate governance but restricting the flow of confidential or private information.

Initial efforts directed at regulatory compliance have focused on preventing external leaks, accidental or otherwise, of sensitive information. However, as organizations gain more experience and understanding concerning the full scope of these imposed regulations they discover their regulatory obligations extend to their internal communications as well.

SOX, for instance, requires demonstrable “evidence of control” over the processing, reporting and distribution of, in particular, financial information. Email is the de facto form of intra-company communication. To guarantee financial data is not revealed to persons (including other employees) that shouldn't have it requires that the content of internal email be monitored and its distribution managed in accordance with regulatory and company policy.

Internal corporate email is also subject to government and industry compliance regulations

The NASD rule 2711 is aimed at ensuring integrity in the public markets by stipulating that investment banking must operate independent from research and trading operations. This means that communications between research analysts and their investment banking counterparts must be highly restricted or even prohibited in some instances. Despite extensive physical, data and network security measures, simple email usually circumvents such security and can become a channel for improper or prohibited communication. The only way to prevent such violations is by monitoring all

³ Source: IDC, “Excerpt – Worldwide Outbound Content Compliance 2005-2009, Forecast and Analysis : IT Security Turns Inside Out”

Internal Email Control

— Its Essential Role in Compliance Management

internal email correspondence and controlling (i.e. preventing or allowing) its delivery based upon criteria such as sender/recipient groups or authorizations as well as actual message content.

Bottom line, with over 70% of business-critical information contained in corporate email, effectively monitoring and controlling internal email flow can help provide the strong evidence of control regulators are demanding and is essential to achieving 100% compliance.

Internal Corporate Policy Compliance

External regulatory requirements aren't the only rules corporations need to enforce.

A holistic approach to compliance will encompass both internal and external policies and regulations.



A myriad of internal corporate rules and policies are established by every company designed to:

- o protect corporate assets from misuse
- o protect employees from unacceptable behaviour
- o mitigate corporate risk and liability
- o streamline business processes and improve productivity, and
- o establish good governance and business best practices

Some combination of these guidelines form what most organizations typically call their "Acceptable Use Policies" (AUP). A specific policy on the acceptable use of email is almost always included.

Yet we know that fewer than half of employees always follow corporate email policies and nearly 50% admit to sending or receiving inappropriate content using corporate email. Reality is that corporate policies are only as effective as your ability to enforce them!

Internal Email Control

— Its Essential Role in Compliance Management

It is just as critical to prevent internal email containing inappropriate content, whether that's offensive language (racially or sexually discriminating, profane, etc.), personal private information or sensitive corporate data, from being delivered as it is to block it in outbound messages.

For instance, it may be acceptable for HR staff to send each other email containing employees' private personal information such as compensation details, banking or credit card info or performance reviews, as it is within the scope of their job function to process such information. However, clearly such information should not be sent outside the HR department, except perhaps to an employee's direct supervisor.

*Fewer than
50% of
employees
always follow
corporate
email policies*

Similarly, sensitive information such as new product plans, merger or acquisition discussions, corporate strategic plans and financial results are all restricted information with very limited internal distribution in both public and private enterprises. While access to file servers, applications and corporate databases that contain and manage such information can be managed through common network, authentication and data security tools, measures to control its dissemination via email are usually lacking. Monitoring the content of internal email and attachments to enforce strict distribution rules, both internal and external, for such restricted or sensitive information is a critical business issue.

In addition to the usual AUP and risk management related rules, many internal corporate policies are established to define preferred business practices and even streamline internal workflow and improve productivity. Real-time internal email monitoring enables policy-based, automatic control and management of employee-to-employee correspondence resulting not only in adherence to these internal guidelines but often also in significant administrative and operational cost savings.

Bottom line, only through accurate content analysis and monitoring of internal email traffic are you able to protect employees, mitigate corporate liability and enforce many of your internal corporate and acceptable use policies.

Architectural Requirements for Internal Email Control

With so many compelling reasons to monitor and control internal email why aren't the majority of enterprises already doing it? There are two main reasons:

- a) in truth, many organizations are only beginning to understand the necessity, and
- b) there are only a handful of solutions available that are capable of internal email monitoring and control functions

One of the goals of this whitepaper is to educate users on the need for internal email control and help them understand how internal email monitoring and control is intricately bound to comprehensive, proactive compliance best practices. Only information, and experience, will ultimately address point a) above.

Internal Email Control

— Its Essential Role in Compliance Management

Limitations of “Appliance” Solutions

With the realization that serious damage can be inflicted upon the enterprise not just by malicious attacks in the traditional sense, but by actions or omissions that result in significant corporate exposure, risk and liability both customers’ and vendors’ focus shifted to outbound content control from traditional inbound control applications like anti-spam and anti-virus protection.

Many incumbent inbound scanning vendors encountered serious delays and technical obstacles in rolling outbound functionality into their legacy products. Meanwhile, many new vendors entered the outbound content control market and adopted an “appliance-based” architecture for their solutions. The appliance approach simplified their development and allowed vendors to get products to market sooner by eliminating the need (and benefits!) of integrating with specific email environments. Seeing the initial success of many outbound email control appliance vendors, the majority of traditional inbound content control vendors adopted the appliance model for their next generation products as well. This then became the platform for their outbound functionality enhancements.

The problem is this, appliance and other perimeter-based solutions, suffer serious limitations in terms of overall email coverage and protection.

The “If You Can’t See It You Can’t Monitor It” Problem

Unfortunately, the single biggest advantage of appliance-based products is also their biggest shortcoming. By completely divorcing content control functions from the corporate email system and placing them on an appliance at the edge of the network these devices can only monitor email that passes through the SMTP connector and crosses the network boundary. That limits their application to just inbound and outbound email, or about 15% of an enterprise’s total email traffic—essentially, not much more than passively checking random samples. It should be noted that this is true of virtually all so called “perimeter” solutions, whether appliance or software based.

The “Who Are You and What Are You Permitted To Do?” Problem

Outbound email control appliances are pitched as fast and easy to install, just “plug it into the network.” Appliance-based email monitoring solutions don’t know and don’t care what corporate email system is used – Microsoft Exchange, Lotus Notes, Novell Groupwise, or whatever. That’s the good news. Then comes the bit where you have to make it understand your company’s policies, security and organizational structure. That’s when the email system neutral, plug and play strategy comes back to bite you.

“It’s important to remember that in order to make sure that all users are in full compliance with policies, not only incoming and outgoing messages should be monitored, but also messages exchanged between users internally”

*The Radicati Group Inc.
Compliance and Policy
Management Market,
2006 – 2010 Report*

Internal Email Control

— Its Essential Role in Compliance Management

Beyond generalized policies that forbid inappropriate content such as pornographic material and offensive, discriminatory or harassing language between anyone, most corporate, and even regulatory-based, AUP and compliance policies include user-specific parameters. For instance, financial results can be sent between finance department employees and to/from senior management but not to the general employee population.

But an email appliance is really an isolated island on the network with no knowledge of the corporate email system or integration to it. Email appliances must be told about individual user, user groups and security profiles to establish a context for and the ability to enforce most content related policies. Even though this information is usually already defined, in Microsoft Active Directory or an LDAP Directory for example, it has to be replicated within the email appliance – a time consuming process despite attempts to automate the task. Then, of course, there's the issues of synchronization, data replication and multiple updates every time there's a change.

Internal Email Control – An Effective Approach

It should be clear that a different approach is required to provide internal email monitoring and control. The most effective architecture for internal email control will have these unique characteristics:

- the ability to actively monitor internal employee-to-employee email
- the awareness of corporate organizational structure – individual and user group profiles
- interoperability with inbound and outbound email monitoring solutions, when those systems are already installed, to preserve any pre-existing product investment and provide a much more comprehensive and layered approach to solving email compliance and security challenges.
- sophisticated content inspection and analysis techniques providing the accuracy to detect complete content or information concepts (internal policies often pertain to company-specific subjects, projects, etc. that are unique and not easily characterized like many external regulatory definitions)
- the flexibility and capability to quickly define the diverse range of internal corporate policies that exist from company to company
- interoperability with corporate security and authentication technologies to leverage existing security and user authorization profiles without replication and duplication

For purposes of this document these architectural and product requirements will be described and discussed further in the context of a Microsoft Exchange email environment as MS Exchange is by far the most prevalent corporate email system.

Internal Email Control

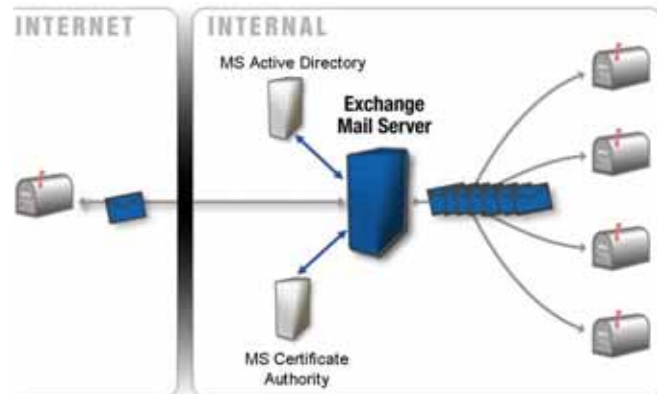
— Its Essential Role in Compliance Management

Product Considerations

In a typical MS Exchange site the architectural and technical requirements for effective internal email control is illustrated by the diagram below.

Integration with Corporate Mail System

For the primary reason that perimeter or network edge products cannot see internal message traffic the first major architecture requirement for internal email control is that the solution is not a typical network appliance product. To monitor internal email traffic requires a direct interface to or integration with the corporate mail server – MS Exchange in this case. Since every message is processed by Exchange this approach allows you to monitor all internal email as well as all inbound and outbound traffic for 100% email coverage.



In terms of deployment strategy, therefore, the most logical location for an internal email control solution is on, or directly attached to, the Microsoft Exchange Server. Of course, this requires a certain degree of integration with MS Exchange Server itself. This deployment strategy also enables the

compliance monitoring product to inherit existing user profiles, security, management functions and authorization definitions already established for use by Exchange.

Integration with Corporate Authentication Systems

The next key requirement is an interface to Microsoft's Active Directory (AD). AD is the primary source for all user and group authorization and security profiles and policy definitions. An interface to AD enables the email control product to utilize existing, predefined user and security profiles for email compliance policy enforcement eliminating the time and cost associated with replicating this information within a product-specific proprietary environment.

Encryption & Digital Signatures

Many regulatory and privacy rules, as well as just good business practices, require that certain content such as non-public personal information (NPI) be protected both externally and within the organization.

Email encryption is an effective way to ensure that such information is totally protected during transit and in the event that it is erroneously received by any recipient for which it was not intended. Thus, there are two more architectural requirements:

- 1) an active, policy-based, on-demand secure mail (i.e. encryption) capability to automatically enforce secure email policies without user intervention, and

Internal Email Control

— Its Essential Role in Compliance Management

- 2) an interface to MS Certificate Authority to provide complete key life cycle management, to leverage existing user certificates and eliminate costly, time-consuming redundant set-up, configuration and administration functions.

Intelligent Content Analysis – Concept Scanning

Intelligent Content Analysis (ICA) is important to all email scanning applications. However, the diversity of content subject to internal corporate policy enforcement challenges many content analysis engines that were designed primarily for inbound or outbound monitoring applications. Highly sophisticated content analysis is absolutely crucial. Typical key word and Bayesian techniques are neither flexible nor comprehensive enough to accurately capture the complexity or *context* associated with many internal corporate policies resulting in unacceptable false positive rates or potentially worse, false negatives.

For instance, how does one properly differentiate correspondence relating to secret internal development projects or business plans from other email that might also reference the common products, technologies or market descriptions? Or email about the company's plans to merge with a competitor or partner from perhaps sales staff's messages about the same competitor or partner? This is a far more complex problem than simply blocking outbound messages addressed to a competitor's email domain.

The answer is through the use of "Concept" definitions rather than just key words and phrases. To accurately define and detect information concepts the ICA engine must be optimized for accurate internal email control and employ a combination of inspection and linguistic techniques such as automatic dictionary lookups, thesaurus term expansion, root word analysis (stemming), term proximity, and term placement (i.e. where is the term found) and term weighting. *Concepts* offer the advantage of more effective and accurate monitoring and detection, fewer false positives, and the ability to recognize context in content policy definitions.

Conclusion

For organizations of all sizes internal email control and monitoring adds crucial capabilities that enhance security, mitigates corporate risk and liability, and safeguards sensitive or confidential business information. Monitoring and control of internal email is fundamental for any comprehensive compliance strategy and for 100% enforcement.

SecurExchange, from Nemx, is the leading active email control solution for Microsoft Exchange Server environments. SecurExchange is fully integrated with Exchange Server, Active Directory and Certificate Authority to provide accurate monitoring and control of internal email as well as inbound and outbound traffic. SecurExchange employs advanced concept scanning, a flexible policy builder, unparalleled flow control (with more than 17 standard Smart Action Triggers and the ability to create unlimited customized actions) and automatic policy-based email encryption and digital signing.

To learn more about SecurExchange and how it can contribute to your organization's email compliance efforts visit Nemx at www.nemx.com