

HOW TO GET IMMEDIATE PAYBACK FROM INTERNAL EMAIL CONTENT CONTROL

Prepared By:

Nemx Software Corporation
#201 - 275 Michael Cowpland Drive
Ottawa, Ontario K2M 2G2
Canada

Best Practices—How to Get Immediate Payback from Internal Email Monitoring & Control

Table of Contents

Introduction	3
The Importance of Internal Email Content Control	3
Where Internal Content Control Adds Value	4
1. Preventative Compliance	4
2. Risk/Liability Management	5
3. Protecting Sensitive Information and Intellectual Property.....	6

Best Practices—How to Get Immediate Payback from Internal Email Monitoring & Control

This document describes why internal email monitoring and control is important to an organizations' overall compliance strategy and four best practices to employ to get immediate payback.

Introduction

Most of the focus for email content control (ECC) initiatives has been directed at traditional inbound and, more recently, outbound email monitoring applications. The requirement for protection from external threats like viruses and spam (inbound content control) is well understood. Increasing regulatory compliance obligations, combined with growing concerns over possible sensitive information leakage, are fueling the demand for outbound email content control solutions.

Currently, the majority of compliance and content control products, and therefore corporate initiatives, are typically focused on solving just one particular issue, such as the archival component of a compliance requirement or enforcing HIPAA content privacy protection on outbound messages.

Internal email content control, a very important piece of the overall content control puzzle, is often overlooked. As enterprises gain more experience with their initial ECC efforts they've realized a more comprehensive view and ECC strategy is required where they have the ability to monitor, manage and control the processing of all email content whether inbound, outbound or internal.

The Importance of Internal Email Content Control

For organizations of all sizes internal email content control and monitoring adds crucial capabilities that enhance security, mitigate corporate risk and liability, and safeguard sensitive or confidential business information. Industry analyst firms, such as IDC, have recently indicated that the need to safeguard confidential or sensitive information within the organization is equally as important as inbound and outbound content control. The Radicati Group echoes this view stating that "compliance and policy management tools are a must, not an option."

Many organizations already use various forms of internal employee monitoring, from network, database and application access control, tracking and auditing to individual keystroke capture, and even, in extreme cases, video surveillance. Such measures are required, and justified, to either protect the security of corporate intellectual property and assets and/or for performance and productivity purposes.

"The issue of internal content control is an emerging and growing concern for corporations.

IDC EMEA Emerging Technologies

Best Practices—How to Get Immediate Payback from Internal Email Monitoring & Control

Ignoring internal email traffic in monitoring and content control efforts exposes the organization to significant risk and liability especially when you consider that:

- ▶ *over 70 per cent of business-critical information is contained in corporate email*
- ▶ *internal email outnumbers all other email by a factor of 8:1*
- ▶ *nearly 50% of corporate email users have sent or received inappropriate content*
- ▶ *fewer than half of email users always comply with corporate email policies, and*
- ▶ *over 75% of all harassment or discrimination cases originate between employees*

Consider the following example. A major bank was surprised when without warning several key employees left and started a competing brokerage services firm. Email archives provided evidence that these employees were plotting their departure, making plans and obtaining client information while still employed by the bank. Consequently, the bank initiated litigation claiming the former employees violated the terms of their employment. It would have been much easier and less costly if through internal email monitoring, these infractions had been discovered at the time they occurred. The bank, in this case, would have been in a strong position to take immediate disciplinary action and pre-empt the damage that was ultimately done. This is a clear illustration of how prevention is the best strategy.

Where Internal Content Control Adds Value

Here are three areas where implementing internal email content control can provide immediate value.

1. Preventative Compliance – Most email compliance initiatives are still focused primarily on the archival component. By archiving every message the assumption is in the event of an investigation they can be reproduced and thus the compliance obligation has been satisfied. While this approach will meet the archival requirement, it may just as readily prove non-compliance with the regulation, as it will compliance. The “archive it all” method in no way improves the organization’s odds of being compliant.

The goal of any compliance strategy should be prevention, not just detection. This is what is meant by preventative compliance. To prevent potential compliance violations requires the ability to monitor, in real-time, the content of email messages including attachment content. Flexibility is also needed to control how those messages are processed in accordance with regulatory, acceptable use or other corporate content control policies.

The distinction between preventative compliance versus merely detection, and the importance of real-time monitoring, is best distinguished through the following example. Detection of compliance, or non-compliance, is the passive form of compliance provided by email archival solutions. By archiving every email and providing the ability to search the archive one can, in an after-the-fact manner, determine if the organization has been compliant or not. By contrast, monitoring of every email message using intelligent content analysis capabilities at the time of delivery enables real-time enforcement of compliance

Best Practices—How to Get Immediate Payback from Internal Email Monitoring & Control

policies and the ability to prevent violations by, for instance, blocking delivery of non-compliant content.

Since email is the dominant form of communication between managers, executives and employees, internal email monitoring and content control is a critical element of any comprehensive, proactive, policy-driven compliance strategy.

Best Practice: Include enforcement and management of internal email content control policies within the overall compliance mandate of the enterprise. This includes the ability, for example, to apply content-driven policies by user group or department. Manageability is key. Evaluate internal email monitoring solutions on their ability to reuse content definition templates and processing rules. If, for example, the concept of confidential or financial information has been defined to prevent outbound information leakage the same policy rules should be reusable for internal monitoring – and vice versa.

2. *Risk/Liability Management* – Mitigating corporate liability and effectively managing risk has become increasingly important to most enterprises in light of recent publicity concerning the size of fines for non-compliance, employee lawsuits for harassment and other events that can seriously harm the reputation of, or result in significant financial consequences for, the corporation.

Distribution of offensive content, whether it be pornographic material, sexual or racial harassment or other inappropriate language remains a major corporate liability issue. Inbound and outbound content control solutions may provide an effective barrier to externally sending or receiving such content, but what's to stop the internal distribution of this offensive material? The fact is, virtually all cases of harassment occur *between* employees. Only by effectively monitoring and controlling internal email content can these kinds of violations be prevented before they can cause damage to the corporation, or an employee.

Best Practice: Implement content control similar to that used to block offensive content from the Internet and inbound email for internal email as well. Solutions should block any internal message containing offensive content from being delivered and should also instantly notify the appropriate HR or compliance officer of any such incident or return the message to the originator outlining the violation.

Risk management is also an important consideration in the regulatory compliance context. For example, among its various principles achieving SOX compliance also means that information relevant to financial reporting is identified, captured, processed, and distributed within the parameters established by the company's control processes to support the achievement of financial reporting objectives. Much of the information that may provide evidence of control, such as the review notes between the CEO and CFO, confirmation of board meeting schedules and attendees, or responses from other departmental executives to questions from the CFO is often contained in internal email. SOX compliance requires

Best Practices—How to Get Immediate Payback from Internal Email Monitoring & Control

that organizations demonstrate these internal controls and procedures; therefore, internal email content control and policy enforcement is a major step toward achieving compliance and reducing corporate risk and exposure.

Best Practice: In terms of risk management identify the “evidence of control” responsibilities embodied in external compliance obligations, such as SOX or GLBA, as well as those that just make good business sense.

From an implementation perspective, flexibility is your friend. Solutions should provide tools to quickly and easily tailor content templates used to identify messages and/or their attachments that should trigger an associated processing or deliver rule. In addition, a variety of actions should be possible such as selectively archiving a message, automatically redirecting it, or adding or deleting recipients as dictated by the appropriate content policy.

3. *Protecting Sensitive Information and Intellectual Property* – Studies show that most organizations use email to distribute confidential information. Often business sensitive information is subject to privacy rules and/or restrictions even as it applies to other employees within the organization—one of the best examples is the need to restrict communications between brokers and analysts within a firm. Information leakage can occur not just in outbound email, but equally as likely in internal email as simply as inadvertently adding an unintended recipient. Unfortunately, popular perimeter-based monitoring solutions and email appliances cannot enforce these restrictions on internal email traffic!

The only way to effectively guarantee that employee “need-to-know” rules are enforced is through internal email monitoring and content control.

Best Practice: Whether to comply with external compliance regulations or not, enterprises should identify critical corporate “need-to-know” requirements. This may be as simple as defining that the CEO and CFO must be copied on all email containing information about financial results and/or projections.

Rules should define both who should get information as well as who should not. For instance, it may be necessary to define a content control policy that specifies that an email containing a client’s credit card number can be delivered to the executive management team and any employee of the finance department but must not be delivered to any other employee. Similarly, look for the ability to implement policy-based encryption rules. For example, a policy that states email containing content deemed “confidential” should automatically be encrypted by the compliance monitoring solution even if the user (sender) forgets to do so.

The bottom line is that internal email content control is crucial to the security, compliance and information protection mandate of any enterprise. To successfully manage corporate risk and liability, organizations must make internal content control part of their ECC strategy to effectively safeguard sensitive information and completely satisfy compliance obligations.

Best Practices—How to Get Immediate Payback from Internal Email Monitoring & Control

Nemx Software is the leader in Active Email Control solutions for Microsoft Exchange environments. SecurExchange is the most comprehensive family of active email control solutions providing "every message monitoring" and delivering Total Email Peace of Mind™.

*Nemx Software Corporation
#201 - 275 Michael Cowpland Drive
Ottawa, Ontario K2M 2G2
Canada*

*Tel: 613-831-2010
www.nemx.com*

