



**Managing Instant Messaging
for Business Advantage:**
Phase One: Assessing IM Usage

Managing Instant Messaging for Business Advantage: Phase One: Assessing IM Usage

Contents

Introduction	4
Instant Messaging Has Invaded the Enterprise	4
Unmanaged Instant Messaging Exposes Your Company to Security and Legal Risks	4
The Real-Time Security Threats of IM Are Unique	4
Electronic Messaging — Including IM — Is Subject to Regulatory Requirements	5
Significant HR and Legal Risk Can Arise from Employee Misuse of IM	5
Unmanaged IM Can Be a Channel for Lost Intellectual Property and Sensitive Information	5
A Four-Phased Approach to Secure Instant Messaging	5
An Introduction to Phase 1: Assessing IM Usage	7
Conducting an IM Usage Audit	8
Step 1: Install an Evaluation Version of Symantec IM Manager	8
Step 2: Operate in “Stealth Mode” to Monitor Corporate IM Traffic without End-User Disruption	9
Step 3 (optional): Apply Optional Content Filters to Detect Inappropriate IM Behavior and Usage	9
Step 4 (optional): Assess Specific User and/or Group Behavior	9
Step 5: Generate and Analyze IM Usage Reports	9
Step 6: Identify Key IM Risk Areas	10
Step 7: Develop a Plan for Ongoing IM Monitoring	10
An Overview of Symantec IM Manager	10
The Management of IM to Drive Business Results	10
Security and Usage Control to Protect the Organization	11
Compliance with Legal and Corporate Accountability Standards	11

Managing Instant Messaging for Business Advantage:
Phase One: Assessing IM Usage

Contents *(Cont'd)*

Conclusion	11
Additional Resources	12
Best Practices for IM Archiving & Compliance	12
Top 5 IM Security Risks 2006	12

Managing Instant Messaging for Business Advantage: Phase One: Assessing IM Usage

Introduction

The ubiquity of consumer-grade, public instant messaging clients and the emergence of enterprise instant messaging servers has challenged IT organizations to develop management policies that deal with the corporate IM landscape as it exists today, while planning for the deployment of emerging presence-based technologies tomorrow. For organizations seeking prescriptive guidance for driving business advantage from instant messaging applications, this white paper provides a best practices overview for effectively managing the risks and costs associated with the corporate use of IM.

Instant Messaging Has Invaded the Enterprise

Instant Messaging (IM) use in the enterprise has exploded and is now seen as a valuable business communications tool. Across companies of all sizes, the benefits of real-time communications and presence awareness are changing the way people communicate with colleagues, customers and partners. The Radicati Group estimates that 85% of all enterprises in North America are reporting IM use, with over 387 million IM users worldwide sending 13.8 billion IM messages per day. The majority of these IM messages are sent over public networks — under the radar of the enterprise IT organization — and without the security and compliance tools required to mitigate the risks of this new communications tool. In fact, studies estimate that while 60% of organizations monitor and secure email, 90% of organizations lack any form of IT sanction or control for IM. With both the Gartner Group and IDC predicting continued increases in business IM usage, including increasing levels of IM growth at the expense of email usage, the risks of unmanaged IM are only increasing.

Unmanaged Instant Messaging Exposes Your Company to Security and Legal Risks

Most organizations today spend a significant amount of time and money managing, securing and archiving email communications. However, few realize that IM not only carries with it much of the same security and legal risks as email, but that the nature of IM creates its own unique management and security challenges.

The Real-Time Security Threats of IM Are Unique

IM worms and viruses are growing exponentially, spreading rapidly due to the real-time nature of IM, and mutating frequently to evade reactive security models. When combined with effective social engineering techniques, the rates of infection and propagation from IM threats are continuing to rise.

“85% of all enterprises in North America are reporting IM use, with over 387 million IM users worldwide sending 13.8 billion IM messages per day.”

*The Radicati Group
Instant Messaging for the Enterprise
July 2005*

“Studies estimate that while 60% of organizations monitor and secure email, 90% of organizations lack any form of IT sanction or control for IM.”

Managing Instant Messaging for Business Advantage: Phase One: Assessing IM Usage

Electronic Messaging — Including IM — Is Subject to Regulatory Requirements

From industry-specific regulatory requirements, such as the strict requirements of the NASD and SEC within the financial services industry, to broad, sweeping legislation such as HIPAA and Sarbanes-Oxley, electronic messaging, including IM, is subject to increasing levels of governance and control. The risks of inaction or non-compliance can be costly, with large financial penalties and often larger indirect costs that include potential damage to the organization's reputation, brand and stakeholder trust.

Significant HR and Legal Risk Can Arise from Employee Misuse of IM

Employee conduct in the workplace is often subject to established HR policies governing accepted behavior and use of company resources. Establishing IM usage policies and a corresponding policy enforcement mechanism is now critical to ensuring that offensive or disruptive messages are not exchanged. In addition to preventing misconduct and monitoring adherence to HR policies, centralized IM archives provide IT administrators with a storage system of record to conduct discovery and provide protection in cases of legal dispute.

Unmanaged IM Can Be a Channel for Lost Intellectual Property and Sensitive Information

With the explosive growth of IM inside organizations and the increasing acceptance of IM as a critical business communications tool, IM contains information that is pertinent to or property of the firm. Without any safeguards or protections, these IM messages can lead to direct or indirect loss of intellectual property and sensitive corporate data.

A Four-Phased Approach to Secure Instant Messaging

Fortunately, the risks of unmanaged, unsecured instant messaging can be addressed quickly and cost effectively so that organizations can leverage IM as a secure business messaging tool.

Symantec has developed a four-phased approach for bringing IM under corporate control.

Designed to serve as a basic framework for understanding how IM is being used across the organization, this process enables businesses to implement the appropriate risk management controls necessary for securing and controlling IM while establishing a longer-term enterprise IM strategy.

Managing Instant Messaging for Business Advantage: Phase One: Assessing IM Usage

- **Phase 1: Assess Current IM Usage** — With a large percentage of corporate IM growth occurring without IT sanction, few companies have a clear picture of how IM is being used inside their organization. A detailed picture of IM usage is required in order to develop a company-risk profile and a deeper understanding of the value that IM is bringing to the end-user community. An IM Usage Audit will uncover who is using IM, what they are using it for and which IM clients are being utilized. The IM Usage Audit and corresponding risk profile can then be mapped to a company's specific key risk areas to drive a comprehensive risk management strategy for instant messaging. Symantec provides a complimentary trial copy of Symantec™ IM Manager to assist companies in the initial IM Audit process.
- **Phase 2: Protect the Organization from IM Threats** — Once the IM risk profile is developed, organizations should move quickly to mitigate the most pressing threats based on the established profile. IM threats generally affect an organization in the form of viruses and worms that attack and compromise user desktops and corporate networks as a whole. Once current threats are neutralized, the company can focus its attention on the medium-term challenge of enforcing use policies that mitigate the broad spectrum of risk, including regulatory compliance, corporate governance and IP loss. Of course, some organizations may see these risks as equal to virus-based threats, and will elect to tackle these problems as part of Phase 2. It is at this stage that a vendor selection will be made. Symantec IM Manager offers a best-of-breed solution for managing the breadth of risk associated with instant messaging.
- **Phase 3: Establish an Effective IM Usage Policy** — An effective usage policy focuses on changing a company's risk profile all together. Through a comprehensive program of policy development, end-user education, enforcement and ongoing monitoring, companies can dramatically reduce the risks associated with IM. This effort will necessarily move beyond IT to include HR, general counsel and at-risk business units or departments.
- **Phase 4: Determine the Longer-Term IM Strategy** — As IM usage is brought under control, secured and managed, organizations should establish a longer-term IM strategy. This longer-term strategy should include a broader direction for reducing the costs to support real-time communications, identifying areas for building economies of collaboration through standardization and consolidation, and integrating Real-time communications into the organization's business processes.

While this document focuses on Phase 1: Assessing IM Usage, more detailed information is available for Phases 2 – 4 at: <http://www.imlogic.com/resources/literature.asp>

Managing Instant Messaging for Business Advantage: Phase One: Assessing IM Usage

An Introduction to Phase 1: Assessing IM Usage

Public IM networks were not designed for enterprise use or centralized control by IT organizations, and their rapid adoption inside organizations has resulted from a free, easy-to-install download process that connects users with little or no end-user configuration. This means that the viral adoption of such clients as AOL Instant Messenger or AIM, MSN Messenger and Yahoo! Messenger has occurred outside the watch of IT. The end result is that corporate use of these networks is unmonitored and unmanaged. Therefore, the first step toward bringing IM under control is to understand who in the organization is using IM and how this communication tool is being leveraged.

While the basic nature of public IM is relatively simple — a specialized client connects to a public networking service for the registration of user presence and the exchange of messages — the nature by which the client software discovers and locates the specific IM network is relatively complex. IM clients can use multiple protocols, including both native TCP streams and HTTP channels, and multiple discovery mechanisms, including well-known DNS names (for example, login.oscar.aol.com for AOL Instant Messenger). From an internal IT organizational perspective, the native public IM networking system does not provide a centralized mechanism for user or service management. This mechanism mirrors that of individual web browsers accessing public Internet sites. IM clients are similar to Internet web browsing in that they connect to external service providers. However, IM clients are very different in that they contain intelligence for network discovery and connectivity, with the real-time, instantaneous exchange of information and presence layered on top once this connectivity is established.

Many organizations have also deployed an internal enterprise IM system with the hopes of delivering centralized, managed IM services to enterprise users. In many instances, these organizations have not effectively addressed the legacy of public IM usage already occurring or have failed to put in place the proper migration incentives and/or safeguards for continued public IM usage.

Regardless of the environment, an accurate public IM usage assessment is the foundation for building an effective management framework for IM. This assessment helps the broader organization understand public IM architecture while answering a number of critical questions in the quest to understand the nature of IM usage across the organization. The following list is a representative sampling of questions that an IM Usage Audit will help answer.

“Regardless of the environment, an accurate public IM usage assessment is the foundation for building an effective management framework for IM.”

Managing Instant Messaging for Business Advantage: Phase One: Assessing IM Usage

- Which IM networks are being used inside my organization?
- Who are my public IM users? Which individuals, groups, business units?
- What types of IM usage trends exist (daily, weekly, monthly, etc)?
- What names are they using for IM? Are these names a risk to my organization?
- What type of content is being exchanged — files, text, other?
- How is IM being used (personal, business, both)?
- Are users sending a large volume of files over IM?
- Are users sending a large volume of URLs over IM?
- Is IM use violating any governmental regulations (SEC, SOX, HIPAA)?
- Is IM use violating any existing IT, HR or legal policies?
- Is intellectual property leaving the organization?
- What types of IM support costs are being incurred by my organization?
- How are my IM users being managed?
- Should I be concerned about blocking sensitive information?

Conducting an IM Usage Audit

In conducting an internal IM Usage Audit, Symantec recommends a seven-step process for creating a unique IM usage and risk profile for your organization. This process helps organizations understand how employees currently use IM within the scope of their daily work so that they can tailor their management strategy and investment to fit their users' unique business needs. What follows is an outline of a Symantec IM Usage Audit that organizations can conduct using a complimentary trial license of Symantec IM Manager for IM detection and analysis.

Step 1: Install an Evaluation Version of Symantec IM Manager

Symantec™ IM Manager deploys easily and without onsite assistance, enabling organizations to begin capturing the IM usage statistics required for organizational analysis. You can request an evaluation copy of IM Manager at www.symantec.com.

Managing Instant Messaging for Business Advantage: Phase One: Assessing IM Usage

Step 2: Operate in “Stealth Mode” to Monitor Corporate IM Traffic without End-User Disruption

During the initial IM usage audit, Symantec recommends organizations run detection in stealth mode as the objective is to obtain a snapshot of current user behavior. Most companies will run in this mode for a full week to get a clear understanding of IM usage patterns.

Step 3 (optional): Apply Content Filters to Detect Inappropriate IM Behavior and Usage

If, as part of the initial audit, organizations would like to assess whether risky behavior is occurring, Symantec IM Manager provides content filters to detect the transmission of inappropriate content. For example, administrators can set-up filters for HR content, regulatory compliance, intellectual property, content security and other IM message content. During the audit, IM Manager will simply report on these events. However, once deployed IM Manager provides the capability to filter and/or block inappropriate content from being transmitted.

Step 4 (optional): Assess Specific User and/or Group Behavior

If, as part of the initial audit, organizations would like to assess specific user and/or group-based behavior, administrators can require the registration of IM users to link IM screen names to known corporate identities. There are several approaches to this, but for the purposes of the IM Usage Audit, self registration is the most cost effective. This provides users with a mechanism to register IM screen names to the Windows username. Once this process is complete, Symantec IM Manager will be able to assign instant messaging events and usage patterns to users and groups.

Step 5: Generate and Analyze IM Usage Reports

Once IM usage data has been collected, organizations can leverage Symantec IM Manager for a variety of in-depth reports that help IT administrators build a company-specific IM usage and risk profile. These reports include:

- Volume of IM traffic, in messages, per unit of time
- Volume of IM traffic, in messages, per IM provider
- Volume of IM traffic, in messages, per LDAP group
- # of file transfers by unit of time, IM provider and LDAP group
- # of content filter violations

Managing Instant Messaging for Business Advantage: Phase One: Assessing IM Usage

Step 6: Identify Key IM Risk Areas

Based on the assessment of IM usage patterns, organizations now have the data to prioritize efforts to reduce risky behavior based on their specific concerns and usage profiles. Ultimately, the audit data provides organizations with the flexibility to deploy the different features of Symantec IM Manager to meet specific organizational requirements.

Step 7: Develop a Plan for Ongoing IM Monitoring

As organizations move from IM usage assessment to the deployment of a secure IM management solution like Symantec IM Manager, maintaining a plan for the ongoing monitoring of IM usage, especially for areas seen as low risk, should remain a top priority. For example, the volume of file transfers may have been low during the initial audit, but over time file transfers may increase to the point that they present a significant enough risk to deploy the Symantec AntiVirus™ Scan Engine through IM Manager.

Even though the audit is focused on identifying risky behavior, most customers are surprised to see how prevalent IM is within the organization, not just in terms of the number of IM users but the volume of traffic. These audits tend to serve the dual purpose of identifying risks while reinforcing an organization's dependence on IM.

An Overview of Symantec IM Manager

Symantec IM Manager seamlessly manages, secures, logs and archives corporate IM traffic with certified support for public and enterprise IM networks, including granular policy enforcement and security controls for files, audio, video, VoIP, application sharing, and other real-time communication capabilities. As a leading provider of security solutions for IM, Symantec provides organizations with advanced capabilities for managing instant messaging, including:

The Management of IM to Drive Business Results

- **Powerful, Flexible Group Policy** — Manage single users or large enterprise groups with redefined, configurable rules within a configurable hierarchy.
- **User Access Control** — Manage employee IM use behind your firewall and control access to external IM networks by user or group.
- **Transparency to End Users** — Deploy IM Manager without touching the desktop and use Symantec IM Manager to detect inappropriate use of IM.

Managing Instant Messaging for Business Advantage: Phase One: Assessing IM Usage

Security and Usage Control to Protect the Organization

- **Zero-Day Protection** — Patent-pending technology for detection and protection against zero-day attacks.
- **Automatic Threat Updates** — Automatically update virus and spam signatures from the industry-leading Symantec™ Response Team.
- **Virus Scanning and File Transfer Control** — Scan file transfers leveraging Symantec AntiVirus™ Scan Engine to prevent infected or confidential files from traversing your network.

Compliance with Legal and Corporate Accountability Standards

- **Rich Message Archive** — Capture all messages and enrich message archive with employee data from the corporate directory for enhanced search capability and reporting.
- **Compliance Auditor Workflow** — Review conversations, append audit comments, and mark messages as reviewed to demonstrate compliance review procedures.
- **Real-time Content Filtering** — Block messages and/or notify administrators when messages containing restricted phrases are sent.

Conclusion

As organizations work to keep up with the rapid rate of change with regard to employee communications, it is imperative that they understand and assess how public IM is being used within the organization. The benefits of real-time communications using IM have become clear to end-users. The explosive growth of IM as a preferred method of communication validates this assessment. However, many organizations do not have a clear picture of the use of instant messaging by their employees. IM Manager allows organizations to understand how IM is being used and to develop a complete risk profile. An instant messaging audit gives companies the information they need to assess this risk and is an important first step toward managing and securing IM.

Managing Instant Messaging for Business Advantage: Phase One: Assessing IM Usage

Additional Resources

The following additional resources are available for more information on IM security, compliance and management:

Best Practices for IM Archiving & Compliance

Spurred by regulatory compliance requirements, corporate governance mandates and internal HR policies, businesses must now consider IM as an electronic record subject to the same retention requirements as email. This prescriptive white paper reviews the best practices for ensuring IM compliance within already established corporate communication policies.

Top 5 IM Security Risks 2006

The continued growth of IM as a preferred tool for business communication has introduced a new class of IT security challenges for businesses today. This white paper explains the top 5 emerging IM security risks in 2006 as identified by Symantec Security Response.

These resources, as well as many other valuable documents, can be found by visiting IMlogic resources on the Symantec website or by navigating to the following hyperlink:

<http://www.imlogic.com/resources/literature.asp>

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
1 408 517 8000
1 800 721 3934
www.symantec.com

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. All other names may be trademarks of their respective owners. Printed in the USA. All product information is subject to change without notice.
03/06 10536262