



**Managing Instant Messaging
for Business Advantage:**
Phase Three: Establishing an
Effective IM Usage Policy

Managing Instant Messaging for Business Advantage: Phase Three: Establishing an Effective IM Usage Policy

Contents

Introduction	4
Instant Messaging Has Invaded the Enterprise	4
Unmanaged Instant Messaging Exposes Your	4
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	5
Instant Messaging	5
An Introduction to Phase 3: Establishing an Effective IM Usage Policy	7
IM Usage Policy Components	8
Implementing an Effective IM Usage Policy Framework	11
Step 1: IM User Registration	11
Step 2: Deploy IM Message Disclaimers	11
Step 3: Track and Monitor IM Usage	11
Step 4 (Optional): Archive File Transfers	11
Step 5 (Optional): IM Message Logging and Archiving	12
Policy Enforcement and Auditing	12
The Management of IM to Drive Business Results	12
Security and Usage Control to Protect the Organization	12
Compliance with Legal and Corporate Accountability Standards	12

Managing Instant Messaging for Business Advantage:
Phase Three: Establishing an Effective IM Usage Policy

Contents *(Cont'd)*

Conclusion	13
Additional Resources	13
Best Practices for IM Archiving & Compliance	13
Top 5 IM Security Risks 2006	13

Managing Instant Messaging for Business Advantage: Phase Three: Establishing an Effective IM Usage Policy

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 Three: Establishing an Effective IM Usage Policy

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 Three: Establishing an Effective IM Usage Policy

- **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 3: Establishing an Effective IM Usage Policy, more detailed information is available for Phases 1, 2 and 4 at: <http://www.imlogic.com/resources/literature.asp>

An Introduction to Phase 3: Establishing an Effective IM Usage Policy

A recent survey conducted by Symantec found that 45% of employees use IM at work because they believe their communication is unmonitored.¹ Statistics like this only underscore the need for effectively managing IM for business through the creation and enforcement of policies around the sanctioned use of IM by employees.

After the completion of the IM Usage Audit in Phase 1, organizations will have a clear understanding of their specific IM usage and risk profile, and a solid basis for proceeding with the secure IM management deployment in Phase 2 designed to protect the organization from the real-time threats posed by unsecured, uncontrolled corporate instant messaging. With immediate IM security risks addressed, companies can begin establishing and communicating an effective policy for corporate IM — a critical component to an organization's overall enterprise IM strategy.

Symantec has identified several points of best practice when developing and implementing policies for corporate instant messaging usage.

- IM has been defined by several regulatory bodies as an electronic record. As such, best practice suggests treating IM the same as email. Organizations should, whenever possible, treat IM and email under a single policy for electronic communications. However if such unification is not appropriate or available, establish a clear, concise IM usage policy.
- An effective policy includes, but is not limited to, provisions for acceptable use, personal use, confidentiality, expectations of privacy, unsolicited messages, inappropriate content and end-user acknowledgement.
- Establish the appropriate process, organizational and technology enforcement mechanisms to ensure consistent and ongoing compliance.
- Consult with the appropriate, internal legal, HR, IT and executive management members and groups to construct a policy appropriate for the specific organization's needs and requirements

The information contained in this document is not intended to replace or substitute professional or legal advice, and is merely provided as a tool to assist in building the appropriate IM usage policy. Individual codes of conduct and usage policies should be developed with the assistance from legal counsel.

1 See IMlogic Research press release titled, "IMlogic Survey Says Majority of IM Users Unknowingly Increase Corporate Exposure to Cyber Threats," September 13, 2005

Managing Instant Messaging for Business Advantage: Phase Three: Establishing an Effective IM Usage Policy

IM Usage Policy Components

The following items are provided as a guide to the possible elements available for inclusion in an IM usage policy.

Subject	Instant Messaging (IM) Usage Policy
Purpose	To establish policies governing the use of electronic instant messaging communications for the organization
Guidelines	This policy applies to all users of instant messaging systems accessed via the organization's network, including regular or temporary employees or non-personnel (e.g., clients, vendors, consultants, visitors, guests, etc).
Definition	<p>IM is a tool for business communications. Instant Messaging (IM) is defined in this document as a form of electronic communication that involves immediate correspondence between two or more users who are all online simultaneously.</p> <p>Instant Messaging systems include AOL Instant Messenger, GoogleTalk, MSN Instant Messenger, Yahoo! Messenger and other Enterprise IM servers deployed and managed by the organization.</p>
Acceptable Use	Users have a responsibility to use this resource in an efficient, effective, ethical, and lawful manner. IM communications should follow the same standards expected in written business communications, electronic mail and public meetings. Violation of this policy may result in disciplinary action, including possible termination or legal action.
Ownership	All content and correspondence which originates or terminates on the computing systems maintained or owned by the organization are the sole property of the organization.
Personal Use	<p>Instant Messaging on the organization's network may be used for incidental personal use provided such use does not interfere with the organization's business operations or the user's employment obligations to the organization.</p> <p>Users are expected to use their best judgment in limiting personal use to acceptable levels. Excessive personal use of IM on the organizational network is prohibited.</p>

Managing Instant Messaging for Business Advantage: Phase Three: Establishing an Effective IM Usage Policy

- Privacy** The organization reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the IM system(s) for any purpose. The contents of IM messages may be disclosed within the organization to and among authorized personnel without permission of the affected IM user. IM messages and content are subject to compliance with this policy, compliance with any applicable laws and industry regulations, and where there is reasonable suspicion of activities that may violate this or any other organizational policy. Users have no reasonable expectation of privacy as all IM systems and/or IM content are the property of the organization.
- Notwithstanding the organization's right to retrieve and read any IM messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. IM users are not authorized to retrieve or read any IM messages that are not sent to them. Any exception to this policy must receive prior approval by a designated representative of the employer.
- Discoverability** Users should be aware that IM messages may be discoverable by opposing parties during litigation, and that even though the sender and recipient(s) have deleted their copies of an electronic record, back-up copies may be retrievable after deletion.
- Conduct** Users of IM networks and communications are expected to do so responsibly and uphold the organization's policies and standards of professional and personal courtesy and conduct.
- Acknowledgement** Users acknowledge the organization's IM policy by formally signing the appropriate policy and/or utilizing IM clients and/or protocols within the organization's network. By reading and agreeing to abide by the IM policy, users understand that a violation of any elements or procedures of the policy may result in disciplinary action, up to and including termination. Formal acknowledgement includes user name, user signature and acknowledgement date.
- Passwords** IM users should not compromise the privacy of individual passwords by providing them to other users or exposing them to public view. Passwords should be changed on a regular basis and should adhere to minimum standards that are not easily spoofed or guessed.

Managing Instant Messaging for Business Advantage: Phase Three: Establishing an Effective IM Usage Policy

- IM Applications** Non-business purpose IM applications are prohibited, including IM-based audio, video, games.
- Consumer IM** Only authorized IM software and IM network access is permitted. Consumer IM software and accessing the public Internet to send IM traffic, whether for internal or external communications, is prohibited, unless otherwise stated or allowed. (Many organizations allow and support the use of AOL, MSN and Yahoo! IM networks for business purposes.)
- Prohibited Use** The following uses of IM systems are strictly prohibited. Users receiving such material should immediately report the incident through their supervisors to the Chief Information Officer, Chief Security Officer, Chief Technology Officer or the Chief Compliance Officer:
- Creation and exchange of messages which are offensive or disruptive. This includes, but is not limited to, any messages which contain sexual implications or harassment, racial slurs, gender-specific comments or any other comment that may offensively address someone's age, sexual orientation, religious or political beliefs, national origin or disability.
 - Exchange of proprietary information; trade secrets; or any other privileged, confidential, or sensitive information outside the enterprise, or outside the defined privileged group.
 - Creation and exchange of advertisements, solicitations, or other unsolicited IM. Users are not permitted to copy, transfer, rename, or edit copyright-protected material without permission of the owner.
 - Creation, storage, or exchange of information in violation of copyright laws.
 - Read or send IM messages from another user's account, except under properly delegated arrangements.
 - Alter or copy a message or attachment belonging to another user without the permission of the originator.
 - Use of IM for personal or individual financial gain, or on behalf of external business ventures.
 - Gambling or any activity that is in violation of local, state or federal law.

Managing Instant Messaging for Business Advantage: Phase Three: Establishing an Effective IM Usage Policy

Entering into any contracts or agreements on behalf of the organization. Any such contracts or agreements must be executed through normal channels and must be expressly authorized by management.

To send (upload) or receive (download) employee, customer or other stakeholder information including, but not limited to, names, addresses, telephone numbers, dates of birth, social security numbers.

Ramifications Disciplinary action for violation of this policy may be an oral or written warning, suspension or termination. Remedial action may also include counseling, changes in work assignments, reimbursement for loss caused, limits or restrictions to IM networks, or other measures designed to prevent future misconduct.

Implementing an Effective IM Usage Policy Framework

Once the components of an IM usage policy have been defined and the appropriate cross-functional team members consulted, the next step is to implement an effective IM usage policy framework. The following high-level steps represent many of the auditing and compliance provisions recommended by Symantec.

Step 1: IM User Registration

As Symantec IM Manager operates out-of-the-box in “stealth mode,” the next step is to register all IM users. IM Manager can be easily configured to support end-user registration to provide the mapping of public IM screen names to LDAP identities.

Step 2: Deploy IM Message Disclaimers

Once users and groups are identified and have been brought under management via user registration, IM message disclaimers should be added. These disclaimers should be customized and tailored to the appropriate requirements for the specific user, group and business unit.

Step 3: Track and Monitor IM Usage

Organizations should create content filtering policies to detect and report on inappropriate content. For example, administrators can set up filters for HR content, regulatory compliance, intellectual property, content security and other IM message content.

Step 4 (Optional): Archive File Transfers

If IM file transfers are allowed, organizations can archive all file transfers to provide a single mechanism for reviewing and auditing this content.

Managing Instant Messaging for Business Advantage: Phase Three: Establishing an Effective IM Usage Policy

Step 5 (Optional): IM Message Logging and Archiving

IM message logging and archiving can be selectively enabled to provide message content review and discovery. Many organizations are subject to regulatory, legal or HR requirements for logging and archiving their electronic records which extends to IM. Symantec IM Manager provides 100% message capture with Web-based reviewer capabilities.

Policy Enforcement and Auditing

In addition to documenting and communicating an IM communications policy, organizations must consider putting in place the appropriate technology and process infrastructure to ensure the consistent and effective implementation of the defined policy. Symantec IM Manager provides a number of methods by which IT administrators can establish IM usage enforcement and conduct ongoing audits for compliance. The following is a list of several important capabilities IM Manager provides:

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.

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.

Managing Instant Messaging for Business Advantage: Phase Three: Establishing an Effective IM Usage Policy

- **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 effective policies are enforced to maintain legal and regulatory requirements. In addition to defining and communicating these communications policies, organizations should implement the right amount of process and technology controls to ensure effective and consistent enforcement of the policy. IMlogic has worked with industry leading companies and vendors to help ensure the security and compliance of instant messaging communications, and provides the necessary tools for effectively enforcing and managing organizational IM policies.

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 10536264