



Managing Instant Messaging for Business Advantage

Phase Two: Protecting Against
IM Threats

Managing Instant Messaging for Business Advantage

Phase Two: Protecting Against IM Threats

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	5
Instant Messaging	5
Introducing Phase 2: Protecting the Organization from IM Threats	7
Understanding the IM Threat	7
IM Is Presence Based	7
IM Has Unique Social Engineering Aspects	7
IM Is Seen as an Easy Target	8
Growth of IM Worms Is Unprecedented	8
Blended Threats Are Becoming the Norm	8
File Transfers over IM Are Increasing in Popularity	8
IM Can Increase the Rates of Identity Theft and “Phishing” Attacks	9
IM Can Serve as a Source of Unwanted Messages or Spam	9
IM Can Serve as a Source for Intellectual Property or Sensitive Information Leakage	9
IM Is Becoming a Target for Attacks on Enterprise Domains	10
Implementing Effective IM Threat Protection	10

Managing Instant Messaging for Business Advantage

Phase Two: Protecting Against IM Threats

Contents (Cont'd)

Step One: Install an Evaluation Version of Symantec IM Manager	10
Step Two: Operate in "Stealth Mode" to Secure Corporate IM Traffic without End-User Disruption	10
Step Three: Establish File Transfer Rules	11
Step Four: Protect Against Malicious IM Messages	11
Step Five: Re-Route Internal IM Messages	11
Step Six: IM Client Version Control	11
Relevant IMlogic IM Manager Product Features for Real-Time Threat Protection	11
The Management of IM to Drive Business Results	12
Compliance with Legal and Corporate Accountability Standards	12
Conclusion	13
Additional Resources	13
Best Practices for IM Archiving & Compliance	13
Top 5 IM Security Risks 2006	13

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.

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

“A recently released *2005 Real-time Communication Security: The Year in Review* report highlights a staggering 1693% increase in IM virus and worm outbreaks over 2004.”

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 Two: Protecting Against IM Threats

- **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 2: Protect the Organization from IM Threats, more detailed information is available for Phases 1, 3 and 4 at: <http://www.imlogic.com/resources/literature.asp>

Introducing Phase 2: Protecting the Organization from IM Threats

Trend analysis from the IMlogic Threat Center (now part of Symantec Security Response) shows a continued increase in the breadth and complexity of IM-borne attacks. A recently released 2005 Real-time Communication Security: The Year in Review report highlights a staggering 1693% increase in IM virus and worm outbreaks over 2004.

After the completion of Phase One's IM Usage Audit, organizations will have a clear understanding of their specific IM usage and risk profile, and a solid basis for proceeding with a secure IM management deployment to protect the organization from the real-time threats posed by unsecured, uncontrolled corporate instant messaging. Once an organization has addressed the immediate and very real IM security risk, the longer-term process of developing and communicating an enterprise IM usage policy can begin. This approach, and the urgency it implies, is driven by several factors specific to the IM security market.

Understanding the IM Threat

Although instant messaging threats are similar to email-based threats, the real-time nature of IM creates unique challenges for IT organizations crafting a comprehensive security strategy.

IM Is Presence Based

The notion of presence — the ability to see if someone is online and willing to engage in conversation — lies at the heart of instant messaging's appeal. In fact, presence is a key element of all real-time collaboration, including VoIP, video conferencing and desktop sharing. It is also the element that makes IM so attractive to virus writers; presence-awareness accelerates the propagation of threats such that the spread of IM viruses is just as instant as IM itself.

IM Has Unique Social Engineering Aspects

Put simply, people trust their buddy list and the messages received from their personally-created community. This provides virus writers with an opportunity to employ social engineering techniques to have malicious payloads activated — and requires organizations to educate their IM users about this type of potential risk.

IM Is Seen as an Easy Target

Growth through grass-roots adoption and outside the control of IT makes IM an attractive vector for corporate network infection by virus writers. The rise in IM-based threats, both blended threats and viruses targeted directly at IM networks, reflects this reality. It is not surprising given the near instantaneous spread of IM viruses and worms, higher infection rates from embedded social engineering tactics and the dearth of corporate risk management strategies for IM.

Growth of IM Worms Is Unprecedented

Just as the adoption of IM has been several times more rapid than the adoption of email, the evolution of the IM virus “market” has occurred more rapidly than the analogous email virus market. In terms of the number of viruses, the sophistication of propagation mechanisms and the severity of virus payload, the threat of IM viruses continues to increase at an unprecedented rate.

Blended Threats Are Becoming the Norm

The increasing levels of sophistication by virus writers, combined with the continued increase in global networking and communications use, has created a system by which virus writers can benefit from multiple infection and propagation vehicles. In many instances, virus writers can attempt to infect unsuspecting end-users through a mixture of Web, email, IM and other networking communications. These hackers attempt to deliver malicious payload or exploit known vulnerabilities over multiple channels to increase their likelihood of penetration resulting in infection. Once infected, a user in turn can become a propagation mechanism for the virus or worm, blending the approach to how the malicious payload or exploit is utilized. In one common example, users are infected through a malicious Website while surfing the Web and once infected, propagate the virus using an internal, enterprise IM system in an environment where public IM is actively blocked at the organization’s network perimeter.

File Transfers over IM Are Increasing in Popularity

With the rapid adoption of IM, file transfer over IM has gained in popularity. One important advantage of leveraging IM rather than email to transfer files is that file exchanges over email are dependent on the recipient’s mailbox storage capacity and can create significant resource drains on the mail server itself. As email volumes increase, the pressure on email administrators to maintain cost controls is also increasing, often translating into strict limits on user mailbox storage quotas. Many users now find file transfers over IM to be a markedly more reliable way to exchange information. Unfortunately, IM file transfers are not scanned or filtered for potential viruses or malicious content, and thus can inadvertently expose an entire network to virus infestations.

IM Can Increase the Rates of Identity Theft and “Phishing” Attacks

Since IM usage within the enterprise has risen predominantly on consumer/public networks, it lacks many safeguards for protecting users and the nature of the content exchanged. Identity theft over IM can be easily accomplished when an organization has not implemented the appropriate controls to its enterprise domain for the IM networks. In such an environment, malicious users can easily pose as other members of an organization by using screen names or identities that imply ownership or association to a known person or entity. For example, many organizations tightly protect their email accounts and domain names but have not considered whether IM users might be using a similar account or domain name for their IM communications. In a similar fashion, phishing attacks can be successful when a user is misled into believing a false request, resource or Website is a representation of an actual trusted entity, organization or user. For example, many financial service firms have been attacked through phishing scams that lead end-users to believe a request for personal account information is being requested by the financial services company, but is in fact an effort by a scammer to obtain sensitive financial information.

IM Can Serve as a Source of Unwanted Messages or Spam

Unlike email Spam, IM Spam (or spIM) can be personalized to the individual IM user based on their presence or screen name, and can embed malicious URLs. These URLs can be used to either propagate malicious payloads, entice the user to visit the spammer’s website or serve as the mechanism for a phishing attack.

IM Can Serve as a Source for Intellectual Property or Sensitive Information Leakage

Many enterprises do not have the necessary IM security solutions to prevent employees from sending confidential or unauthorized content beyond the firewall. Particularly in workgroups which handle proprietary information, the risk of unmonitored content leaving the corporation without the knowledge of the information security department can introduce both competitive and legal risk (e.g., a CFO sending confidential spreadsheets via IM without any audit trail). Unmanaged, unmonitored IM file transfers are a particularly powerful vehicle for sending information underneath the forensic capabilities of the IT department. In addition, the lack of content logging or archiving makes it difficult for administrators to discover potential breaches of information security policies, or to hold individuals accountable for their actions.

IM Is Becoming a Target for Attacks on Enterprise Domains

As enterprises move from grassroots employee-provisioned names on IM networks such as bubbles99@yahoo to corporate-controlled domains more similar to Internet email addressing, employees will be assigned names such as first.last@company.com. Many companies will ensure that employees are given identical IM and email addresses to streamline discovery and facilitate IM communications. When this occurs, companies will be “broadcasting their IM addresses over the public Internet. This will make organizations vulnerable to a new series of attacks such as directory harvest attacks, denial of service attacks, and more advanced phishing and spIM attacks. Few organizations are prepared for these new threats that will emerge with federated, open IM environments.

Implementing Effective IM Threat Protection

With the completion of the IM usage and risk profile, implementing an effective IM threat protection solution is the next step toward safely leveraging IM as a business-critical communications and collaboration tool. This process helps organizations bring their IM security policies in line with already existing security policies for the Web and email. What follows is a high-level overview of how technology such as Symantec IM Manager provides organizations with the necessary IM security capabilities needed to ensure IM is not exposing their business to unnecessary risk.

Step One: Install an Evaluation Version of Symantec IM Manager

Symantec™ IM Manager deploys easily and without onsite assistance, enabling organizations to begin securing public and enterprise IM usage right out of the box. You can request an evaluation copy of IM Manager at <http://www.symantec.com>. Symantec provides detailed installation and configuration instructions to assist IT administrators in deploying Symantec IM Manager.

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

Operating out-of-the-box in “stealth mode” enables organizations to monitor and secure all IM traffic without end-user disruption while the appropriate IM security policies are created. Part of this policy creation might involve optionally configuring Symantec IM Manager to support end-user registration to provide mapping of public IM screen names to LDAP identities. In fact, most IT organizations positively impact end-user behavior and corporate IM security by leveraging different features of Symantec IM Manager such as forced screen name registration and message disclaimers.

Step Three: Establish File Transfer Rules

Organizations should decide whether or not IM can be used as a vehicle for file transfer, and then configure their Symantec IM Manager software to either disable this capability or scan IM file transfers using Symantec AntiVirus™ Scan Engine.

Step Four: Protect Against Malicious IM Messages

Because IM threat propagation occurs in real-time, Symantec recommends connecting to Symantec Security Response for the added benefit of the industry's first behavior-based IM threat protection system along with automatic security updates. Through Symantec Security Response, Symantec IM Manager actively monitors IM traffic, detecting and protecting against zero day attacks before they propagate over corporate networks.

Step Five: Re-Route Internal IM Messages

Employee use of public IM networks means IM communication crosses the corporate firewall into the Internet cloud before crossing back inside the organization. In addition to protecting against external IM security threats, Symantec suggests configuring Symantec IM Manager for internal message routing. Once enabled, all internal IM messages using public IM networks are routed internally, within the company's network.

Step Six: IM Client Version Control

The final step for initially implementing an effective IM security solution is to proactively manage IM client versions. Symantec IM Manager provides for flexible IM client version control so that organizations can block older, out-of-date clients that contain known security vulnerabilities from being used.

Relevant IMlogic IM Manager Product Features for Real-Time Threat Protection

To help organizations protect themselves against the next generation of threats associated with real-time communications, Symantec helps many of the most complex organizations secure their IM and communication systems. As a leading provider of security solutions for IM, Symantec provides organizations with advanced capabilities for IM security, including:

Managing Instant Messaging for Business Advantage

Phase Two: Protecting Against IM Threats

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.
- **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

The real-time nature of IM, combined with its pervasiveness in corporations, requires that organizations deploy and leverage effective safeguards and protections for corporate IM use. As the breadth and complexity of IM threats grows, a proactive approach to securing this real-time communications channel is required in order to properly prevent rogue IM usage, block external security threats and control the exchange of sensitive information within the organization. With Symantec and Symantec IM Manager, companies can leverage IM as a secure business messaging tool that helps connect the right people to the right information in real time while enhancing the flow of ideas, information and knowledge across the organization.

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 10536295