



**Managing Instant Messaging
for Business Advantage:**
Phase Four: A Strategic Plan
for Broad Adoption of Real-Time
Collaboration

Managing Instant Messaging

for Business Advantage:

Phase Four: A Strategic Plan for Broad Adoption of Real-Time Collaboration

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 4: A Strategic Plan for Broad Adoption of Real-Time Collaboration ..	7
Broadening the Deployment of Real-Time Technologies	7
Managing and Securing Real-Time Communications	9
Management and Security Technologies Shouldn't Dictate IT Strategy	9
Access Control for Real-Time Services Is Critical	9
Detailed Systems and User Monitoring Should Be Part of Every Technology Deployment	9
Each Real-Time Service Has Its Own Set of Security Issues	9
The Real-Time Network Will Be Heterogeneous	10

Managing Instant Messaging for Business Advantage:
Phase Four: A Strategic Plan for Broad Adoption of Real-Time Collaboration

Contents *(Cont'd)*

Conclusion10

Additional Resources10

Best Practices for IM Archiving & Compliance10

Top 5 IM Security Risks 200610

Managing Instant Messaging for Business Advantage: Phase Four: A Strategic Plan for Broad Adoption of Real-Time Collaboration

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.

“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

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.

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

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.

Managing Instant Messaging for Business Advantage: Phase Four: A Strategic Plan for Broad Adoption of Real-Time Collaboration

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 Four: A Strategic Plan for Broad Adoption of Real-Time Collaboration

- **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 4: A Strategic Plan for Broad Adoption of Real-time Collaboration, more detailed information is available for Phases 1, 2 and 3 at:

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

An Introduction to Phase 4: A Strategic Plan for Broad Adoption of Real-Time Collaboration

For most organizations, instant messaging is the first foray into the realm of presence-enabled, real-time communication and collaboration services delivered over an IP network. But, it will not be the last to be deployed and managed by IT. Tuning the notion of convergence — or the delivery of all real-time collaboration services, including phone services, through a single technology platform — will be the single biggest task facing IT organizations over the coming decade.

Both enterprise IM servers and public IM networks are delivering unified clients that give users access to services such as IM, VoIP, group video and application sharing — all integrated with contact and calendaring management applications. The promise of convergence is the promise of ubiquitous, easy-to-use, real-time collaboration at dramatically reduced costs. These cost savings are driven by the reliance on a unified platform that obviates traditional telephony networks and generates economies of scale for platform services like management and security.

Organizations will look for a consistent set of management and security policies as they move from secure IM deployments to the management of a broader set of real-time technologies. IT groups will likely invest in projects that deliver a combination of time to value and overall return on investment. As these investments are made, it is important to make sure that the management foundation is in place prior to broad deployment of new services.

Broadening the Deployment of Real-Time Technologies

Based in part on the rapid adoption of IM and in part on the possibility of real cost savings associated with converged communications, IT organizations are seeking to broaden their investment in real-time technologies. Most organizations will face similar basic questions as this process unfolds.

- What new services do users want? Are they valuable? As end users push for new and better collaboration services, IT organizations will have to respond with technology and with sound business analysis. Collaboration improvements are typically measured in terms of difficult-to-monetize productivity gains. Platform companies recognize this difficulty, and are pricing their platforms to encourage the deployment of the breadth of services they offer. There is a tremendous amount of value to be had in deploying these technologies, but each request for additional services will compete for resources and with efforts at cost reduction. Additionally, each new service will have incremental network costs, and IT will be tasked with managing internal access to each new service to keep costs in line with value. For example, many IT organizations were caught off guard by the huge fees generated by hosted Web meeting services. These costs may be obscured by an internal Web meeting server, but the variable costs of Web meetings will not disappear.

Managing Instant Messaging for Business Advantage: Phase Four: A Strategic Plan for Broad Adoption of Real-Time Collaboration

- What cost savings are available? At what investment? Even though end-user demonstrations are compelling, the primary driver for convergence will be cost savings. The temptation here will be to “boil the ocean,” precisely because the pay-off for one project will depend on the completion of another. Companies should look to identify discrete projects that can be managed to completion within a reasonable time horizon.
- What platform decisions need to be made? The popularity of enterprise real-time collaboration systems, most notably Microsoft Office Live Communications Server, provides a compelling case for standardizing on a single technology for all real-time collaboration. However, these systems do not deliver the infrastructure totality required for all IP-based communications. The IP network itself, the separate telephony network and even the traditional telephone handsets form part of this picture.
- What will happen to the consumer networks? Organizations that have relied on public IM networks, or that have simply allowed them out of expediency, will face the same issues when it comes to new real-time services. Public networks are offering competing services, often for free, directly to end users. As companies take their time to sort out their communications infrastructure, public services will likely fill the gap. For example, the VoIP, video and Web meeting services from public IM companies are improving rapidly, and companies like newly rich Skype will be targeting enterprise users. Given the footprint that these companies already have in the enterprise, it is likely that these new services will be just as popular with corporate users as IM has proven to be.
- To what extent will these systems be available to external stakeholders? Even companies that have standardized on enterprise IM systems have yet to decide exactly how they want users of these systems to connect to the outside world and more importantly how they want the outside world to connect into them. As new, more bandwidth-intensive services are made available to corporate users, the issue of internal user rights and external user access will become critical to a managed, secure environment. Enterprise servers have attempted to leverage the ubiquity and zero-fee business model of public networks, most notably Microsoft’s LCS Public IM Connectivity (PIC) offering which allows LCS users to add AOL, MSN and Yahoo! users to their buddy lists and vice versa. Other federation options are available as well, but in order for these models to work, enterprises will need to make sure they can control access to their employees. The scourge of unwanted email — Spam — has been followed by spIM and now spIT as the use of IM and IP telephony has gained traction in the enterprise.

Managing and Securing Real-Time Communications

Once the base technology decisions have been made, the need for a management and security framework will come into focus. In evaluating these decisions, it is important to ensure that vendor solutions are well positioned to meet your needs as your real-time investments accelerate. In looking at future management and security needs, Symantec is guided by several strategic guidelines.

Management and security technologies shouldn't dictate IT strategy.

Management and security are foundational elements of any IT strategy, but these technologies must be flexible enough to meet the needs of the business. When evaluating technology solutions in these areas, make sure that vendor solutions are designed to fit within a variety of environments.

Access control for real-time services is critical.

As the value and technology footprint of real-time services continues to grow, controlling access by internal and external stakeholders will be the key to controlling costs and security risks. As real-time services request more and more network bandwidth, IT will need to ensure quality of service, assign costs to individual departments based on use, and control access to internal users from external entities. Management vendors should be able to keep unwanted users out of the network and ensure that real-time services share time with other systems that access the network.

Detailed systems and user monitoring should be part of every technology deployment.

It is difficult to pre-define what reporting and use data will be needed, but monitoring of actual system use helps to evolve risk profiles and to build the business case for broadening the deployment of individual services. As individual departments request to be brought online, many organizations implement an internal charging system to assign these costs individual departments.

Each real-time service has its own set of security issues.

It is tempting to lump real-time services into a single category, but each service has a slightly different risk profile and provides different targets for malware developers. Unwanted communications behave differently over email, IM and VoIP, and although a security solution should be integrated, it can't be homogeneous. Most content-based threats blend across different systems. Viruses can originate in email, propagate over IM and eventually migrate into a VoIP network. As real-time systems converge, the threats unique to one system will bleed over into others. In order for a real-time security strategy to be complete, it must address the peculiarities of each system while understanding their inter-dependence.

Managing Instant Messaging for Business Advantage: Phase Four: A Strategic Plan for Broad Adoption of Real-Time Collaboration

The real-time network will be heterogeneous.

With every new wave of technology, the temptation exists to simply start over, but few companies are well served by a rip-and-replace strategy. More often, environments are heterogeneous. In seeking to manage and secure real-time systems, Symantec is driven by the need to adapt to complex, heterogeneous environments.

Conclusion

By following Symantec's four phases for managing IM to recognize business advantage, organizations should be able to not only meet their immediate IM management and security needs but also implement the appropriate controls to ensure the appropriate long-term IM strategy can be pursued. The nature of IM continues to evolve. Originally used for the simple exchange of text messages, IM now represents the next innovation in real-time communications. With IM, individuals can increasingly publish their presence, exchange files and establish contextual conversations. And as IM continues to evolve, audio, video and telephony will increasingly be bundled into the IM stream. With these innovations, Symantec provides organizations with the industry's leading solution for securing and managing all elements of a real-time communications infrastructure.

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 10536297