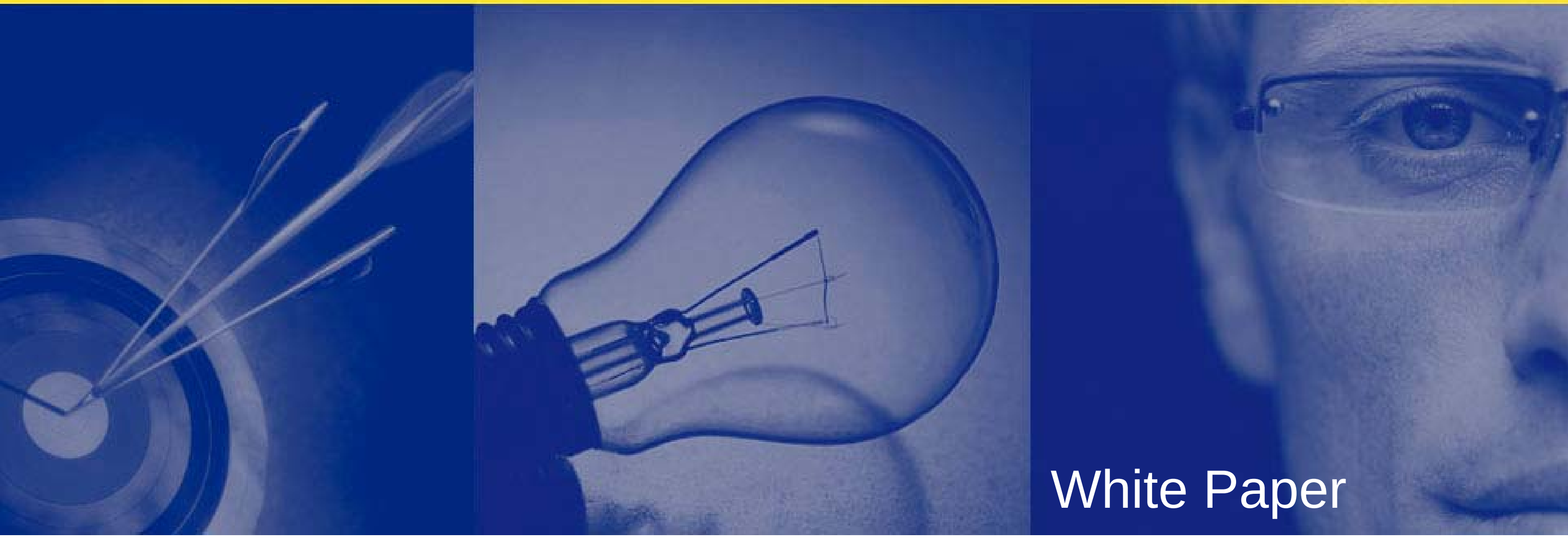
Best Practices in Instant Messaging Management

Enabling Productive, Secure and Compliant Instant Messaging Policies and Usage in the Business Environment

Written by
Quest Software, Inc.



WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
e-mail: info@quest.com
U.S. and Canada: 949.754.8000

Please refer to our Web site for regional and international office information.

Updated—October, 2008

Contents

Executive Summary

Developed in the 1990s for personal chat and entertainment, instant messaging (IM) is rapidly becoming a de facto standard for instantaneous communications within the workplace. Recent research indicates that more than 85 percent of all businesses now make use of IM. Additionally, one in three IM users now utilize IM as much or more than e-mail, and many predict that IM usage will outstrip e-mail usage within the next few years.

Workplace use of IM provides a host of benefits within the organization. Its presence features and immediacy can eliminate much of the internal churn and waste of e-mail, voice mail or office visits. It provides contact with remote employees, customers and vendors at a more intimate level than other forms of electronic communication. And overall it boosts business performance by making operations faster, more agile, and more efficient with very little additional cost.

But for all its benefits, business IM often creates substantial dangers. Most IM usage in the workplace occurs over public networks without the policies, oversight, and safeguards considered mandatory with other enterprise communications and networking systems. This casual approach opens the company not merely to diminished productivity arising from idle chat, but to security exposure from worms, viruses, and other malware; inadvertent transfer or leaking of sensitive documents; and, in the case of regulated organizations, potentially serious compliance and legal violations.

As with any organizational process or system, business IM is enhanced from the application of balanced best practices, which maximizes the benefits and mitigates the risks of IM technology. While the specifics of these best practices must be tailored for each organization’s unique needs, the general steps include:

1. Audit all IM tools within the organization.

2. Create written policies that clearly and explicitly define the acceptable use of IM.

3. Implement security systems to properly identify users and secure the network against threats such as viruses, malware, hacking, and unauthorized file transfer.

4. Adopt an IM management solution such as Quest Policy Authority to provide monitoring, management and control, and to ensure compliance and security.

5. Implement ongoing review of policies and usage to keep up with changing user needs.

The History of Business Instant Messaging

Although "chat" systems, such as the early proprietary versions of AOL Instant Messenger (AIM), and the public Internet Relay Chat (IRC), have been available since the late 1980s, the first "true" IM system—one with a simple interface and contact (or "buddy") lists that operated over the open Internet—didn't emerge until the release of ICQ in 1996. The following year AOL released a publicly available version of its AIM client, enabling its 20 million users to connect in real time with the rest of the Internet. In subsequent years, others, including Microsoft and Yahoo, released their own IM clients. Features such as file transfer, emoticons, and audio and video were added, and personal IM use reached critical mass. By the year 2000 nearly 250 million people worldwide were making use of IM.

Even though IM was first developed as a personal communications tool for interacting with friends and family, many of IM's most avid users are now in the work place. In particular, they are knowledge workers and those in technology-driven fields. These users use IM's presence awareness features (e.g., "online", "busy", "away") to stay in touch with co-workers and associates, reduce the lag time associated with other non-instantaneous communications media like e-mail and voice mail, and increase overall productivity and efficiency.

Business IM adoption has been incredibly rapid: some estimates are that in just five years, workplace IM users have tripled from 21 million to 63 million. Many analysts expect business IM adoption to continue at very high rates and predict that workplace IM usage will likely surpass e-mail within the next several years.

Due to the overwhelming speed at which ad hoc IM adoption penetrated the business environment, most organizations have embraced (or at least not prohibited) the use of IM by their employees, even while they struggle to get it under control. For example, there are now a number of secure, proprietary IM systems designed specifically for the enterprise, yet more than 90% of the IM used in business is the same open, insecure systems freely available to the general public. What's more, research reveals that fewer than half of all organizations have specified one IM system as a corporate standard. And perhaps most significantly, seven out of ten organizations have yet to establish any formal policies or implement systems to ensure its secure and appropriate use.

Business IM: Risks and Benefits

The Risks: Compromised Security, Compliance Violations, and Legal Liability

Instant messaging's rapid evolution from personal entertainment to workplace tool, combined with ignorance of how IM works, means that most IM users are unaware of the risks that IM poses to the organization. Public IM systems operate in the open where other people may be able to eavesdrop. Additionally, IM systems, both public and proprietary, often operate beyond the range of corporate firewalls and other security systems. IM risks include:

- **Information leaks** – Confidential materials, intellectual property, or proprietary information can be revealed, either intentionally or accidentally, through IM sessions or file transfers.

- **Worms, viruses, etc.** – Numerous malware programs target public IM systems and allow them to bypass standard firewalls and mail server anti-virus systems.

- **Network hacks and intrusions** – Hackers use IM operating ports to bypass other security barriers and enter the corporate network unimpeded.

- **Compliance, regulatory, or legal violations** – Organizations subject to government oversight and compliance mandates may find themselves creating legal issues by failing to properly monitor, log, and regulate IM sessions and content.

- **Productivity loss** – Idle chat can disrupt employee productivity.

The Benefits: Better All-around Business Performance

The primary reason that IM has been such a success in the business environment is that its benefits, even when weighed against the risks, are both immediate and tangible. Presence awareness allows users to see who's available without picking up the phone or walking to another part of the building. The real-time nature of the medium makes it a faster and more efficient means of getting answers and transferring documents or information than e-mail or telephone. And IM provides a direct mode of communication with co-workers, customers, and vendors that enables far closer and more personal relationships than virtually any other means of electronic communication.

Business IM also allows employees to be more efficient in their work output. Data shows that IM users engage in multi-tasking at a rate considerably higher than non-IM users. In a recent survey, 91% of IM users reported that while participating in IM sessions, they also perform additional tasks either most or all of the time.

Not surprisingly, the vast majority of employees believe that the use of IM within their organization improves productivity, external relationships, and their efficiency. More significantly, however, is that the business managers and IT personnel who are aware of the risks posed by IM overwhelmingly favor its use, noting that the added tangible business performance benefits more than offsets the potential risks.

Best Practices for Business IM

Best practices for business IM enable productive instant messaging within a secure and compliant framework. Business managers, IT staff, and corporate IM users must work together to establish balanced policies and enforcement tools to minimize security risks while ensuring maximum benefit. Best practices for business IM consists of five specific practices:

- **Discovery** – Explore and document the organization's current IM assets, policies, and needs, as well as your current IT infrastructure.

- **Create written policies** – Clearly and explicitly define acceptable and unacceptable use of instant messaging within the business environment.

- **Implement security technology** – Implement client and network systems to ensure that users are properly identified and managed and that IM access points enforce corporate usage rules. Secure the network against threats such as viruses, malware, hacking, and unauthorized inbound or outbound file transfer.

- **Implement monitoring and management systems** – Implement solutions to monitor the enforcement of written and physical security policies, and provide a means for those policies to be managed and logged for the purpose of internal audit or regulatory compliance.

- **Periodic review and modification** – Successful best management practices (BMPs) are dynamic and fluid. Active monitoring and management make it possible to adjust BMPs to fit the changing needs of the business.

Discovery

The first phase in implementing best practices for business IM is discovery. Questions to ask include:

- Who in the organization is using IM and what they are using it for?

- Do all employees need to be able to IM with people inside and outside of the organization? Do they need to transfer or accept files?

- What policies, if any, regulate aspects of business IM in the organization (an acceptable internet use or employee conduct policy, for example)?

- What compliance or regulatory requirements govern the dissemination of company information and documents?

- Does the nature of the business require a more secure form of instant messaging, or are public versions acceptable? Should the company standardize on a single IM system or are multiple systems acceptable or desirable?

- What systems and security measures are already in place? Are there any security gaps that need to be remedied?

In addition, a thorough review of the organization's existing IT systems and infrastructure in the discovery phase will help immensely when it comes time to choose a monitoring and management solution to integrate into the environment.

Written Policies

Written IM usage policies vary widely. For smaller organizations, the policy may be a "code of conduct" rather than a detailed inventory of regulations. Larger enterprises and those with regulatory requirements or oversight may have far more detailed policies. Regardless of the size of the organization, the team drafting the policy should include members from various departments, including Human Resources, IT, and Legal.

At the very least, a well written IM usage policy will:

- **Clearly and explicitly explain the organization's instant messaging objectives** – Users should know why the organization permits IM and how it is expected to be used.

- **Define expectations of privacy** – Users should be made aware that the organization has the right to monitor and log all IM sessions for corporate compliance, safety, and security reasons.

- **Detail acceptable and unacceptable uses** – An exhaustive list of permitted and forbidden activities may not be necessary, but specific examples are helpful in establishing a framework of IM behavior for users.

- **Detail content and contact restrictions (if any)** – Most organizations will want to limit the amount of idle IM chat that may occur with family, friends, and other non-business related contacts. There may also be additional issues related to information confidentiality and privacy. Some businesses may choose to block the distribution of certain types of information via live IM chat session or file transfer.

- **Define consequences for violations of the policy.** – Users should be advised of the consequences of policy violations. Generally these should be aligned with the company's personnel and acceptable use policies.

Additionally, it is recommended that a standard disclaimer be inserted into all users' IM sessions. Regardless of its content, the simple presence of the disclaimer will have considerable impact: it will remind employees not to share confidential information or engage in conduct that violates the organization's usage policies, and reiterate that all IM sessions are logged.

Security Technology

Once the written policies are complete, client and network security must be implemented using a software technology solution. Items uncovered in the discovery phase and the specifics of the written policy will help you determine what security and control areas need to be addressed. These areas should include:

- **Access control by user and IM systems** – Do you have a need for identity controls (i.e., associating IM user "screen names" with network user names or identities)? Will you be limiting access based on user requirements (e.g., prohibiting access, restricting internal or external access, or limiting remote login)? Will you be limiting or controlling the types of IM and IM activities permitted on the network? Your answers to these questions will help you evaluate solutions based on their identity management, access control, and application control features.

- **Virus, Trojan, and malware scanning** – If you will permit contact by outsiders via IM or allow embedded objects or file transfers, you will need a means of scanning for and stopping malware and other IM-based attacks.

- **Content security** – Because sessions on public IM systems are assisted by external IM networks, those conversations and any files or other exchanged materials could be intercepted by third parties—even if the conversation occurs between two users within the same company. IM security solutions can keep internal conversations within the company network and protect sensitive information.

- **IM spam (spim) filtering** – With IM usage in the workplace becoming preferable to e-mail, a growing number of IM users are being targeted with unsolicited instant messages. Many of these are not merely nuisances but also potential legal and security risks because they can be used to transmit pornographic content or payloads for phishing and other malicious purposes. The ability to halt this sort of material is a growing need and should be considered as part of any monitoring and management solution.

Many of these technology issues are no different than the security BMPs implemented for services such as web and e-mail, and should fit with your organization’s overall security system. Nonetheless, because IM systems utilize unique technology and operate in real time, it is important that your IM security needs be identified and specifically addressed by solutions tailored for business IM.

Monitoring and Management Systems

While written policies help ensure that users understand the guidelines and expectations for business IM use and technological security measures help ensure network safety and integrity, neither is effective without active IM monitoring and management to ensure that those measures are enforced. IM monitoring and management provides the crucial components that enable the organization to fully implement BMPs for business instant messaging, allowing it to reap the benefits of IM while avoiding the hazards.

IM monitoring and management systems can be implemented in a number of ways, from ad hoc do-it-yourself systems to integrated solutions from software vendors that specialize in IM monitoring and management. Most organizations quickly discover that the difficulty of implementing IM monitoring and management almost always makes a third-party solution preferable to a home-built system—especially when the third-party system integrates many of the security features outlined in the security technology section above.

While the functionality of a monitoring and management system will depend on the organization’s needs, at a minimum the system should perform the following:

- **Logging and record retention** – IM sessions (like e-mail and web access) should be stored for informational, forensic, and legal and regulatory compliance purposes. Because these records grow very quickly, support for or integration with enterprise content archiving solutions can prove highly advantageous.

- **Reporting** – Disclosure of IM activities, potential policy violations, and other information is extremely useful for human resources and numerous corporate compliance and government reporting regulations.

- **Content filtering** – If your organization has policies regarding the use of inappropriate language or the distribution of certain content or sensitive information (e.g., account numbers, credit cards, and passwords), a means of identifying, flagging or blocking, and reporting these items is necessary.

The choice of a monitoring and management solution will also depend on your organization's existing systems and infrastructure, as documented in the discovery phase. Integration must be as straightforward as possible: incompatible systems and complex installations not only add to costs and frustration, but may also create new problems and security risks—precisely the opposite of what BMP implementation should do.

Periodic Review and Modification

Once the initial four phases of the BMP are complete, there is a temptation to consider the job done and move on. But periodic review and modification of BMPs is just as important as their implementation. Businesses frequently find that their initial policies and rules become hindrances at a later date for a number of reasons—a change in the organization's structure or mission, policy changes, new security risks, and so on. Therefore, it is important to perform periodic reviews of the organization's IM policies and rules (both written and systems-based) and modify them as necessary.

In performing each periodic review, organizations should consider the following questions:

- Is the written IM policy compatible with other company policies (personnel, Internet access, etc.), and does it accurately reflect the organization's guidelines?

- Do the organization's IM users have access to the features they need to make best use of business IM? For instance, do they need to be able to transfer other types of files? Should the organization further restrict IM sessions?

- Are there new security risks that might prompt changes in IM security?

- Has the organization's direction or structure changed in such a way that a modification to IM policy is needed? For example, are there other groups—perhaps customer service, support, or marketing— that should be allowed to IM directly with customers?

The IM management system's logs, reports, and other monitoring data (in conjunction with anecdotal data from organization personnel) will provide invaluable insight into the nature of organizational IM use and help guide decision-making during the review process. Regular analysis and modification (if necessary) of business IM policies and practices will help organizations leverage the maximum benefit from the technology.

Summary

Over the past decade, instant messaging (IM) use has evolved from a consumer communication device to a robust and valuable business tool. Business IM improves teamwork, cuts needless waste, and helps organizations improve relationships with customers, vendors, and business partners in ways that no other form of electronic communications can. As a result, use of business IM is escalating at unprecedented rates and many analysts believe that IM use within organizations will outstrip e-mail use within the next few years.

Business IM, however, is not without risks. The public nature of most IM systems, along with its roots in consumer entertainment, makes it susceptible to attacks and inappropriate use. This can place the organization in situations that range from merely embarrassing to financially devastating.

To mitigate the risks and appreciate the benefits of business IM, organizations need to implement best practices for IM as for systems such as Internet use and e-mail. Best practices for business IM are implemented in five phases:

- Discovery
- Written policies
- Security technology
- Monitoring and management systems
- Periodic review and modification

Each of these phases is a critical component to successful and advantageous use of business IM. Diligent application of best practices in each phase will improve individual performance, limit associated hazards, and allow the organization to enjoy all the benefits that instant messaging technology has to offer.

About Quest Policy Authority for Unified Communications

Quest Policy Authority for Unified Communications enforces policies on and archives instant messaging and other real-time communications. Its flexible architecture blocks unwanted protocols, improves security and hygiene, protects sensitive data, and enforces regulatory compliance. Policy Authority also captures IM and file transfers, PIN-to-PIN, and SMS messages, helping IT organizations create a true compliance archive.

Policy Authority is part of Quest's suite of solutions for archiving, e-discovery, and compliance. These solutions can help you securely and efficiently manage your huge repository of data through e-mail retention and file storage optimization, messaging compliance, and policy enforcement. Quest can help you capture, retain, discover, and manage this data to satisfy legal and regulatory requirements and control storage costs. For more information, visit http://www.quest.com/unified-communications/archiving-ediscovery-compliance.aspx.

ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc., a leading enterprise systems management vendor, delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 90,000 customers worldwide meet higher expectations for enterprise IT. Quest provides customers with client management as well as server and desktop virtualization solutions through its subsidiaries, ScriptLogic and Vizioncore. Quest Software can be found in offices around the globe and at **www.quest.com**.

Contacting Quest Software

Phone: 949.754.8000 (United States and Canada)
Email: info@quest.com
Mail: Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA
Web site: www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around-the-clock coverage with SupportLink, our self-service web site. Visit SupportLink at http://support.quest.com.

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles and other documents)
- Download patches and upgrades
- Seek help from a Support engineer
- Log and update your case, and check its status

View the ***Global Support Guide*** for a detailed explanation of support programs, online services, contact information, and policies and procedures. The guide is available at http://support.quest.com/pdfs/Global Support Guide.pdf.