

# Best Practices in Instant Messaging Management

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

*an Akonix whitepaper*

**TABLE OF CONTENTS**

- ▶ **Executive Summary** ..... 1
  
- ▶ **Introduction** ..... 2
  - The History of Business Instant Messaging** ..... 2
  
- ▶ **Business IM Benefits vs. Risk** ..... 3
  - The Benefits: Better All Around Business Performance** ..... 3
  
  - The Risks: Security, Compliance & Legal Liability** ..... 3
  
- ▶ **Best Management Practice of Business IM** ..... 4
  - Implementing A Balanced Solution to Maximize Your Business IM Use** ..... 4
  
  - Discovery** ..... 5
  
  - Written Policies** ..... 5
  
  - Security Technology** ..... 6
  
  - Monitoring & Management Systems** ..... 7
  
  - Periodic Review & Modification** ..... 8
  
- ▶ **Conclusion** ..... 9

## ► Executive Summary

### **Instant Messaging Use Within the Business Environment is Growing at an Exponential Rate**

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. New research indicates that more than 85 percent of all businesses now make use of IM within their organization. Additionally, one in three IM users now utilize IM as much or more than email, and many predict that IM usage will outstrip that of email within the next few years.

### **IM Use at the Office Can Dramatically Improve Business Performance**

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 email, voice mail or trips to people’s office. It provides contact with remote employees, customers and vendors at a level far more intimate than other forms of electronic communication. And overall it boosts business performance by making operations faster, more agile and efficient with very little additional cost.

### **Business IM Use is Not Without Risk**

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 risks arising from idle chat, but to security exposure from worms, viruses and other “malware”, inadvertent transfer or leakage of sensitive documents, and, in the case of regulated organizations, potentially serious compliance and legal violations.

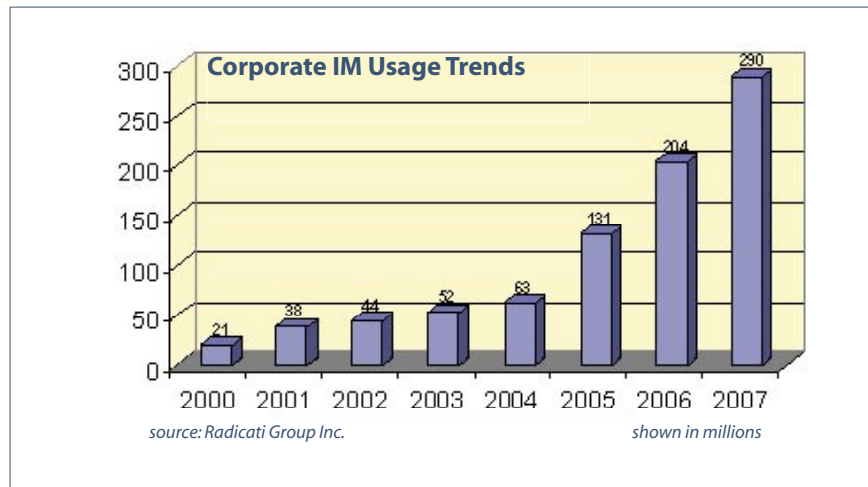
### **Maximizing Business Gains While Minimizing Risk is Easily Achievable with the Application of Best Management Practices for Business IM**

As with any organizational process or system, business IM is enhanced from the application of balanced Best Management Practices (BMPs), which maximizes the benefits of IM technology, as well as mitigating the risks. While the specifics of these BMPs must be tailored for each organization’s unique needs, the general steps include 1) audit of IM tools within the organization; 2) written policies clearly and explicitly defining acceptable use of IM; 3) the application of an IM management solution such as Akonix L7 Enterprise to provide monitoring, management and control and ensure compliance and security; and 4) ongoing review of policies and usage to keep up with changing user needs.

## ► Introduction

### 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, contact (or “buddy”) lists, and operating over the open Internet—didn’t emerge until ICQ’s release in 1996. The following year AOL released a publicly available version of its AIM client suddenly allowing its 20 million users to connect in real-time with the rest of the Internet. In subsequent years others such as 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 one quarter of a billion people worldwide were making use of IM.



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. Particularly “knowledge workers” and those in technology-driven fields. They use its 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 email and voice mail, and increase overall productivity and efficiency.

**“24% of Instant Messaging users now use IM more frequently than email.”**

Pew Internet & American Life Project

Business IM adoption has been incredibly rapid, in just five years workplace IM use has 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 most likely surpass email within the next several years.

In a nod 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, fewer than half of all organizations have even bothered to specify one IM system as a corporate standard. And perhaps most significantly, 7 out of 10 have yet to establish any formal policies or implement systems to ensure its secure and appropriate use.

## ► Business IM Benefits vs. Risks

### Leading Uses of Business IM

- 1) **Intra-Company Communication**
- 2) **Presence Awareness**
- 3) **Personal Use**
- 4) **Customer or Partner Communications**

Radicati Survey

***“A significant majority of business IM users believe that instant messaging improves teamwork and helps save time on tasks.”***

Pew Internet &  
American Life Project

### **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 the need to pick up the phone or journey 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 email 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 is available in virtually every other means of electronic communications.

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 even business managers and IT personnel who are aware of the risks posed by IM overwhelmingly favor its use noting that the added “real” business performance more than offsets the potential risks.

### **The Risks: Security, Compliance & Legal Liability**

Instant Messaging's evolution from personal entertainment to workplace tool, combined with ignorance as to how the system works (it “just works”), means that most IM users are rarely aware of the potential risks that may affect the organization. Public IM systems operate “in the open” where others, with some effort, 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 Leakage** – Either intentional or accidental revelation of confidential materials, intellectual property and/or proprietary information through IM sessions and/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 and/or Legal Violations** – Organizations with 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.

## ► Best Management Practices of Business IM

### Implementing A Balanced Solution to Maximize Your Business IM Use

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

**Discovery** – Exploration and documentation of the organization’s current IM assets, policies and needs.

**Written Policies** – Clearly and explicitly define acceptable and unacceptable use of Instant Messaging within the business environment.

**Security Technology** – Includes implementation of client and network systems to ensure that users are properly identified and managed, and IM gateways/access points enforce corporate usage rules and secure the network against threats such as viruses, malware, hacking, and unauthorized inbound/outbound file transfer.

**Monitoring & Management Systems** – Includes the implementation of solutions that monitor the enforcement of written and physical security policies, and provide a means by which those policies may be managed and logged for the purpose of internal audit or regulatory compliance.

**Periodic Review & Modification** – Far from being set in stone, successful BMPs are dynamic and should change to fit the needs and requirements of the business. Active monitoring and management makes this possible.

## Discovery

The first phase in implementing BMPs for business instant messaging is discovery. Areas to examine include:

- Who in the organization is already using IM and what they are using it for?
- Do all employees need to be able to IM with people inside and outside the organization? Transfer or accept files?
- What, if any policies already regulate aspects of your business IM (the organization's Acceptable Internet Use or Employee Conduct Policy, for example)?
- What compliance or regulatory requirements are there governing 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/desirable?
- What systems and security measures are already in place? Are there any openings that need to be remedied?

Based on the industry and culture of the organization there may be additional areas that should be explored and documented. Once the information and materials have been gathered and organized you are ready to establish written policies and implement management solutions.

## Written Policies

The content of the written IM usage policy will vary widely based on the organization. For smaller organizations the policy may be a "code of conduct" more than a detailed inventory of do's and don'ts. For larger enterprises and those with regulatory requirements or oversight, it may be far more detailed. As the scope of this policy is largely dictated by the individual organization it is important to include members from various constituents such as human resources, IT, and legal in the creation of the document. At the very least, a well written IM usage policy will:

- **Clearly and Explicitly Detail Organizational Expectations in the Use of Instant Messaging** – 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/or 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. As such the business may choose to block the distribution of certain types of information via live IM chat session and/or file transfers.

- **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, while it is not part of the IM usage policy, it is recommended that a standard disclaimer be inserted into all user's IM sessions. This can be a useful "reminder" not to share confidential information or engage in conduct that violates the organization's usage policies, and/or a notification that all such sessions are logged. Regardless of the content, the simple presence of the disclaimer will have considerable impact.

## Security Technology

Once the written policies are complete, implementation of client and network security should take place via a software technology solution. Based on items uncovered in the discovery phase, as well as those detailed within the written policies, there may be a number of security and control areas that need to be addressed. They include:

- **Access Control by User & IM Systems** – Do you have a need for identity controls (i.e., associating IM user "screen names" with network user names and/or identities)? Will you be limiting access based on user requirements (e.g., no access, internal and/or external access, remote login, etc.)? Will you be limiting or controlling the types of IM and IM activities allowed to operate on the network? If so, measures such as identity management, access controls and application feature controls will be necessary.
- **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 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 email, a growing number of IM users are being targeted with unsolicited Instant Messages, many of which 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 other services such as web and email, and should fit with your organization's total security systems. 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 & 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 the organization 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 specializing in IM monitoring and management. Most organizations quickly discover that the difficulty and detail of implementing IM monitoring and management almost always makes the 3rd party solution preferable to the “home built” systems—even more so when the 3rd party system integrates many of the security features outlined previously in the security technology section.

While the service levels and functionality of a monitoring and management system will be largely dependent on the organization’s needs, at a minimum the system should perform the following:

- **Logging and Records Retention** – Just as with email and web logging, IM sessions should be stored for informational, forensic, and legal and regulatory compliance purposes. As such records can become large and cumbersome in a very short period of time, support for or integration with enterprise content archiving solutions can prove highly advantageous.
- **Reporting** – Disclosure of IM activities, potential policy violations, etc. are 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, passwords, etc.), a means of identifying, flagging or blocking and reporting these items is necessary.

Monitoring and management system implementation will also depend largely on the organization’s existing systems and infrastructure. It is important that integration be as straightforward as possible since 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 BMPs implementation should do. A thorough systems review during the discovery phase will help immensely when it comes time to implement the management and monitoring phase.

## Periodic Review & Modification

Once the initial four phases of the BMPs are implemented and complete there is a temptation to consider the job done and move on. Yet, just as important as the implementation of BMPs is their periodic review and modification. Frequently businesses will find that policies and rules initially implemented become hindrances at a later date for a number of reasons—a change in the organization structure or mission, policy changes, new security risks, and so on. As such, 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 the periodic review, the following should be considered:

- Is the written IM policy compatible with other company policies (personnel, Internet access, etc.), accurately reflect the organization's guidelines?
- Do the organization's IM user have access to the features they need to make best use of business IM? (e.g., do they need to be able to transfer other types of files? Should they be more restricted with whom they hold IM sessions?)
- Are there new security risks that might prompt changes in IM security?
- Has the company's business direction or structure changed in such a way to prompt a modification to the IM policies? (For example, are there other groups—customer service, support, marketing, etc.— that should be allowed to IM directly with customers?)

Consultation of the IM management system's logs, reports and additional 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.

## ► Conclusion

Over the past decade Instant Messaging 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 believe that its use within organizations will outstrip that of email 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 make it susceptible to attacks and inappropriate use that can place the organization in situations that range from the merely embarrassing, to the financially devastating.

To mitigate the risks and enjoy the full gains that business IM has to offer, organizations need to implement Best Management Practices for IM just as they would for other systems such as Internet use and email. BMPs for business IM are implemented in five phases:

- Discovery
- Written Policies
- Security Technology
- Monitoring & Management Systems
- Periodic Review & Modification

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

**To learn more about implementing Best Management Practices for IM visit us at [www.akonix.com](http://www.akonix.com) or contact us at 619 615 9415 | [sales@akonix.com](mailto:sales@akonix.com)**

**For a free monitoring tool that detects and reports on IM and P2P file sharing on your network visit [www.akonix.com/ra](http://www.akonix.com/ra)**

### **About Akonix**

*Akonix is the leading provider of enterprise-class business solutions for leveraging the power of multi-network enterprise instant messaging. Akonix is widely recognized as the technology and market innovator. More than 500 customers in Financial Services, Telecommunications, Energy, Technology, Healthcare and Entertainment depend on Akonix to manage, secure and enable IM for over 700,000 enterprise users. Akonix is the preferred IM management solution of some of the world's largest companies, including Cingular Wireless, Qualcomm, EMC and ING.*