



Instant Messaging: Benefits and Threats for Business

This paper discusses the benefits IM brings to business today, in the form of improved communication, collaboration, efficiency, and cost savings. It also outlines IM threats and the security issues business leaders should be aware of so they can take the necessary steps to protect their organizations.

Table of Contents

1	Executive Summary	3
2	Ready or Not—IM is Here	3
3	Business Benefits of IM	3
4	IM Threats and Security Issues	5
5	Enterprise Instant Messaging: IM As a Legitimate Business Application	7
6	EIM: A clear choice for business	8

Instant messaging (IM) is a fact of life in 75% of small to medium-sized businesses today and is expected to be as common as email by 2009.

In the small to medium-sized business market, Osterman reports that 75% of employees now use IM.

1 Executive Summary

Instant messaging (IM) is a fact of life in 75% of small to medium-sized businesses today¹ and is expected to be as common as email by 2009.²

In some industries, IT departments and business leaders who recognize its value have deployed IM deliberately. In others, employees have been the initiators—downloading free IM software such as AOL Instant Messenger™ (AIM®) or MSN® Messenger onto their desktops without the knowledge or consent of their employers. As a result, IM is mismanaged in many organizations, with decision-makers unaware of the extent of its use or the benefits and security issues it has already brought into the workplace.

This paper discusses the benefits IM brings to business today, in the form of improved communication, collaboration, efficiency, and cost savings. It also outlines IM threats and the security issues business leaders should be aware of so they can take the necessary steps to protect their organizations.

2 Ready or Not—IM is Here

Over the past several years, instant messaging (IM) has become a force to be reckoned with in the business community. Some organizations, such as those in the financial and technology sectors, have embraced it proactively. Wall Street equity traders, for example, have made IM an integral part of their business, using instant messaging to make trades worth billions of dollars.

Geographically dispersed companies and those focused on technology have taken to IM earlier than others, but a 2006 Osterman Research survey indicates that instant messaging is already used in 93% of North American businesses. Thirty-four percent of email users also use IM, and Osterman anticipates “almost complete penetration into the email user base by 2009.”³

In the small to medium-sized business market, Osterman reports that 75% of employees now use IM.⁴ And the trend shows no sign of reversing. A 2005 study by the Pew Internet & American Life Project found that, while almost nine in ten teens now use the Internet, 75% of them use IM, compared to only 42% of online adults.

Despite the penetration of IM into the business market, it remains for many industries a consumer technology that is still under the radar. Much like cell phones and PDAs, it has most often been brought in by enterprising employees—not deployed by IT departments. Some business decision-makers are still unaware of the extent to which instant messaging is used within their organizations. They often misunderstand the benefits of IM in the workplace, as well as the security issues it presents.

3 Business Benefits of IM

IM use now spans multiple industries and demographics, and is proving to be an indispensable communication tool. Far from being the time-waster it was feared to be in the early days of its use, instant messaging offers many positive benefits for business. From improved efficiency and project collaboration to the ability to produce archived IM conversations for legal purposes, instant messaging is becoming a communication tool as valuable as email or the telephone.

IM has proven return on investment (ROI) benefits in certain situations, such as conferencing.

A study by the Radicati Group looked at the time it took employees to complete two typical daily tasks—both with and without IM—and found that companies could save an average of 40 minutes a day per user with IM. They estimated that an organization with 5,000 people could see a \$37.5 million a year savings in productivity.

3.1 Savings on telephone costs and travel time

Seasoned business leaders who have built careers on sensitive, timely phone conversations and face-to-face meetings often don't understand the value of IM. They see it as yet another electronic form of communication that, like email, lacks the immediacy and vocal modulation of a "real" conversation and can more easily result in miscommunication and employee isolation.

While those concerns are valid, and the phone and personal meetings certainly remain a core aspect of doing business, IM has proven return on investment (ROI) benefits in certain situations, such as conferencing. Most IM clients make it easy for several people to participate in the same discussion, at a much lower cost and with less hassle than setting up a phone conference. Group members can be conferenced in to such a conversation from around the world—saving on long distance charges and travel expenses. IM meetings also tend to be more efficient and less prone to straying off topic, because of the relative effort of typing versus talking.

A study by the Radicati Group looked at the time it took employees to complete two typical daily tasks—both with and without IM—and found that companies could save an average of 40 minutes a day per user with IM. They estimated that an organization with 5,000 people could see a \$37.5 million a year savings in productivity.⁵ While those estimates didn't factor in the additional costs of managing security and compliance issues, Radicati is confident that organizations would nevertheless reap "significant ROI improvements" from IM deployment.

3.2 Improved communication

IM is less intrusive than a phone call, but more immediate than email. And it has the added advantage of being able to detect presence. Users can set status messages telling others whether they are available or not, which adds to IM's value as a skillful means of communication. The employee who used to hover outside the boss's door waiting for the right moment to approach now has another informal method of getting his attention. IM offers a way to quickly resolve questions and issues as they arise, and managers open to using IM find it becomes an essential medium for receiving feedback and information from their staff.

3.3 Enhanced collaboration and improved efficiency

IM has proven its overwhelming value when it comes to gathering input from many different people in dispersed locations. These days, when your marketing staff in Chicago needs to clarify technical information from the manufacturing group in Cincinnati or Hong Kong, an IM meeting is probably the most efficient way to achieve this objective. Processes that were once agonizingly slow and inclined toward misunderstanding and errors can now be accomplished in record time.

When questions arise, the telephone is no longer an obstacle. In fact, many people use IM and the phone simultaneously. Company employees can chat with each other privately while on a group call with an external partner, for example. Instant messaging is the multi-tasker's tool of choice—most people chatting over IM do other things at the same time.

3.4 Information archiving

Archiving IM meetings and conversations has become an essential business process for most companies, since IM users don't generally just chat—they also exchange document fragments, URLs, product specifications and other information. After all, it's a lot easier to share the dimensions of the new pacemaker you've designed over IM than by phone. IM discussions can become part of a knowledge repository that everyone can access.

A 2006 study by the American Management Association (AMA) and the ePolicy Institute found that 50% of IM users in the workplace had downloaded free instant messaging software from the Internet.

3.5 Employee satisfaction

Statistics show that instant messaging is already a well-established business tool, and employers who insist on keeping it out of their workplace risk alienating a workforce that already sees its value. As the younger generation enters the workforce they will certainly demand access to IM. More employees now recognize the benefits of instant messaging for helping them get work done more quickly, and for communicating more casually with co-workers.

4 IM Threats and Security Issues

For organizations competing in today's business climate, instant messaging has become an important part of their communication strategy. The question is not whether they will allow its use, but how they'll manage the threats and security concerns IM introduces. Unmonitored, uncontrolled public IM networks – such as Yahoo Messenger, AOL AIM, and MSN Messenger – are essentially open channels between corporate networks and the outside world—a state of affairs involving an amount of risk that most business leaders are unwilling to accept.

A 2006 study by the American Management Association (AMA) and the ePolicy Institute found that 50% of IM users in the workplace had downloaded free instant messaging software from the Internet. Twenty-six percent of their employers were unaware of what has amounted to a widening security gap in their networks.⁶ As IM use grows, the number of related threats proliferates. IT departments will be forced to pay attention—whether they have deployed the IM client in question, or not.

4.1 You've seen this before: Viruses, worms, Trojans and other malware

Just as IM is another electronic communication tool for productive employees, it is also another medium for hackers, spammers, and malware-writers to exploit. And the speed at which IM threats can propagate alarms industry analysts. IM's real-time capabilities could facilitate virus infection at a rate of 500,000 computers in less than 30 seconds, according to a simulation run by one security software vendor.⁷

Many IM threats have their roots in email scams, so any lessons IT departments learned as email use matured in the past decade should be applied in the same way to instant messaging. But people are more trusting when chatting on IM because it is an informal medium used primarily to communicate with friends and colleagues. Many IM attacks compromise the IM "buddy list," a list of trusted friends the user frequently chats with. Users are used to responding to "buddies" with little or no suspicion, which makes them particularly vulnerable when they receive a message from a scammer "bot" that has co-opted the identity of a known correspondent.

As with email, IM malware usually arrives as executable file attachments or URLs that lead to websites with malicious code ready for download by unsuspecting IM users. IM communication is usually computer-to-computer so any attachments shared in this way bypass the email gateway-based virus scanning most organizations have in place. This makes IM an ideal tool for malware writers looking to distribute their malicious content.

User education will be a critical element in addressing the IM malware threat. But proper management is also important, since IM attacks are becoming particularly devious and aggressive. Some malicious "bots" impersonating buddies actually interact with suspicious users—responding positively when the user asks if a file is safe to open, for example.

4.2 SPIM—the new spam

Spam over IM, or SPIM, as it is known, targets IM users with everything from annoying ad messages to phishing scams—messages designed to look like they come from a trusted source, but that trick users into giving up private information. The Radicati Group says users are interrupted by IM junk messages about five times a day—a rate that amounted to about 1.2 billion SPIM messages in 2005. Radicati expects SPIM messages to increase by as much as 27 times a day, per user, by 2008.⁸

The Radicati Group says users are interrupted by IM junk messages about five times a day—a rate that amounted to about 1.2 billion SPIM messages in 2005. Radicati expects SPIM messages to increase by as much as 27 times a day, per user, by 2008.

Phishing scams over IM are becoming a problem. According to Gartner research, 12% of all Internet fraud was initiated via IM in 2006.⁹ Cybercrooks that started out using email for their scams are now finding it easier to catch busy IM users off guard and lure them to fraudulent websites designed to steal credit card numbers, login information, social security numbers and other sensitive data.

4.3 Identity theft and eavesdropping

Since IM traffic generally uses the public Internet, it's no great feat for someone to steal the username and password for an IM account and begin sending messages as though they were that person. We've already discussed the implications for "bots" impersonating buddies to get users to download malware, but identity theft may also happen on a smaller scale—among company employees, ex-employees, or competitors, for example. Eavesdropping—using an IM user's login information to listen in on an IM conversation he or she may be having—is a related threat of equal concern when it comes to securing company information.

4.4 Exposure of confidential data

One of the most serious threats to businesses that allow unmonitored IM use involves the potential loss of confidential data—either proprietary business information or sensitive customer or employee data.

Public IM clients don't usually include an encryption option, so any information shared in an IM conversation has the potential of being intercepted. Employees may be sitting across the room from each other, but the IM messages that pass between them are leaving and re-entering the network—passing through the corporate firewall, out into the "cloud" that is the Internet, and back. People also frequently disclose information when they are conducting several different IM conversations at once, and accidentally send a message to the wrong person.

Sales forecasts, prospecting information, or proprietary product information can be leaked in these ways fairly easily, with no malevolent intention on the part of employees. This is of particular concern for the healthcare industry in the United States, where data breaches in violation of the Health Insurance Portability and Accountability Act (HIPAA) can result in serious consequences. But the leak of valuable corporate data can be devastating for any business.

4.5 Denial of Service attacks and application vulnerabilities

Denial of service (DoS) attacks happen when resources such as your email or web servers become overloaded and can no longer function. If you haven't planned correctly, network capacity can sometimes be exceeded simply as a result of IM use. But, just as with email, attackers can cause the same thing to happen deliberately. This type of attack can also hit a single IM user, causing the IM client or the computer itself to crash.

Instant messaging clients vary in their quality and vulnerability to outside threats. The common user may not be aware of how IM client vulnerabilities can be exploited, or be cognizant of patches and updates that become available. Organizations with a large percentage of people using unmonitored public IM clients are particularly vulnerable to these kinds of attacks.

4.6 Converging threats

Instant messaging is maturing in a very different world than the one we saw when email was at a similar stage of its development. Up until the past couple of years, virus writers have been mainly individuals or computer geeks motivated by little more than a need to show off their programming skills or create general havoc.

The stakes have gone up considerably. Today, skilled programmers are hired by organized crime rings to attempt worldwide sting operations or to make “serious political statements.”¹⁰ The new targets for these attacks comprise millions of bank accounts, as well as the financial and communication systems the world relies on.

As a result of this sophisticated and targeted approach on the part of attackers, Internet threats are converging rapidly, affecting every area of the Internet, including email, the web, and instant messaging. Malware such as the SoBig.F virus and the Storm Worm work in conjunction with phishing scams and fraudulent websites to steal money and information from their unsuspecting victims. Viruses like SoBig.F infect PCs in ways that users can’t detect, with the goal of establishing networks of proxy machines hackers can use to send out spam, host malicious websites, or launch DoS attacks. These new threats have as a characteristic the ability to morph constantly, so they can avoid detection and adapt to defensive behaviors. Instant messaging users are targets for these multi-faceted attacks, as much as anyone using the Internet.

These new threats have as a characteristic the ability to morph constantly, so they can avoid detection and adapt to defensive behaviors. Instant messaging users are targets for these multi-faceted attacks, as much as anyone using the Internet.

4.7 IM platform convergence

The various instant messaging networks such as AOL, MSN and Yahoo! were developed as proprietary systems with their own communication protocols. Unlike email or the web, which work on the universal protocols of SMTP and HTML, IM clients all use different protocols, or languages, to transmit information. This has made it more complicated for people on different platforms to communicate with each other, but it’s also made it harder for malicious virus writers to attack different systems at the same time. In order to do that, they have had to, in a sense, learn several different languages.

Universal IM platforms such as Click4Me.Net, Gaim, and Adium can connect to multiple IM platforms at once—offering users a way to simplify and consolidate their IM communication. But as they gain broader acceptance, these converged platforms present a tantalizing target for scammers looking to hit a broad spectrum of IM users.

5 Enterprise Instant Messaging: IM As a Legitimate Business Application

While public IM networks are responsible for the huge growth of instant messaging technology in the workplace, most companies now recognize the advantages of investing in IM as a legitimate business application. Enterprise instant messaging (EIM) systems—secure, private IM networks installed behind the corporate firewall—give employees the ability to collaborate and communicate safely and effectively. They offer a buffer between the corporate network and the Internet cloud.

In a 2006 survey of small and medium-sized businesses, Osterman Research found that 23% plan to install an EIM product in the near future, and 23% use one already.¹¹ Security issues are a big motivator—business leaders who realize that IM is here to

EIM products such as MessageLabs[®] Enterprise Instant Messenger Service offer organizations significant advantages over consumer networks.

stay would much rather install a clean, on-premise solution behind their firewall than to continue allowing employees to access unsecured public networks directly.

5.1 Improved efficiencies, peace of mind

EIM products such as MessageLabs[®] Enterprise Instant Messenger Service offer organizations significant advantages over consumer networks. While you can still offer users the ability to communicate over public networks, the EIM encrypts this communication and creates a solid line of defense against any threat that might present itself. Only authorized users can access the network, which eliminates the risk of ex-employees or unknown users creating problems.

Over an EIM network, users can converse and exchange files with complete security and privacy. All file attachments are automatically scanned for threats, and are fully encrypted so they can't be intercepted or tampered with. EIMs also have storage and logging capabilities, helping to ensure regulatory compliance and giving organizations a way to monitor and manage IM conversations.

EIM systems can also be integrated with other applications and systems, such as WebEx and SalesForce.com—and this may be where the value of instant messaging truly begins to reveal itself. The ad-hoc use of IM in the workplace has already begun to make business processes more efficient. But when organizations integrate IM with their processes and applications in more deliberate ways, they begin to see the true value it brings to the table.

6 EIM: A clear choice for business

As business leaders begin to understand more plainly the advantages instant messaging brings their organizations, they are looking for the best way to manage this new communication tool and protect themselves from the threats it presents. EIM systems, such as the MessageLabs Enterprise IM Service, address these concerns, and place instant messaging in its rightful place in the business application environment—offering organizations a manageable tool with a recognizable return on its investment.

www.messagelabs.com
info@messagelabs.com

Freephone UK
0800 917 7733

Toll free US
1-866-460-0000

Europe
HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom

T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom

T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS
Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands

T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG
Culliganlaan 1B
B-1831 Diegem
Belgium

T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

DACH
Feringastrasse 9
85774 Unterföhring
Munich
Germany

T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999

© MessageLabs 2005
All rights reserved

Americas
AMERICAS HEADQUARTERS
512 Seventh Avenue
6th Floor
New York, NY 10018
USA

T +1 646 519 8100
F +1 646 452 6570

CENTRAL REGION
7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA

T +1 952 886 7541
F +1 952 886 7498

Asia Pacific
HONG KONG
1601
Tower II
89 Queensway
Admiralty
Hong Kong

T +852 2111 3650
F +852 2111 9061

AUSTRALIA
Level 6
107 Mount Street,
North Sydney
NSW 2060
Australia

T +61 2 8208 7100
F +61 2 9954 9500

SINGAPORE
Level 14
Prudential Tower
30 Cecil Street
Singapore 049712

T +65 62 32 2855
F +65 6232 2300

-
- ¹ "Instant Messaging Tough Enough for Business: No Server Required." Osterman Research, September 2006.
- ² "Messaging in the SMB Market, 2005-2008." Osterman Research, October 2006.
- ³ "Instant Messaging Tough Enough for Business: No Server Required." Osterman Research, September 2006.
- ⁴ "Messaging in the SMB Market, 2005-2008." Osterman Research, October 2006.
- ⁵ "Measuring IM Productivity in the Enterprise." The Radicati Group, Inc., November 2004.
- ⁶ "2006 Workplace Email, Instant Messaging & Blog Survey: Bosses Battle Risk by Firing E-Mail, IM & Blog Violators." American Management Association and ePolicy Institute, 2006.
- ⁷ Leavitt, Neal, "Instant Messaging: A New Target for Hackers." July 2005. http://www.leavcom.com/ieee_july05.htm
- ⁸ "Corporate Spim is No LOL Matter." *Newsweek*, 9 May 2006. <http://www.msnbc.msn.com/id/7691051/site/newsweek/>
- ⁹ Barlas, Pete, "Web Scammers Getting Trickier As Fraud Rises." *Investor's Business Daily*, 1 March 2007.
- ¹⁰ Espiner, Tom, "Study: Instant messaging attacks rose in 2005." CnetNews.com, 10 January 2006. http://news.com/Study+Instant-messaging+attacks+rose+in+2005/2100-7349_3-6025226.html
- ¹¹ "Messaging in the SMB Market." Osterman Research, November 2006.