A Short & Simple Guide to Managing Instant Messaging in the Workplace

an Osterman Research white paper

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Phone: +1 253 630 5839 • Fax: +1 866 842 3274 • info@ostermanresearch.com • www.ostermanresearch.com

Background

The use of instant messaging (IM) in the workplace is pervasive and is growing rapidly. Osterman Research been conducting a twice-yearly survey of IM in the workplace for several years and has found that:

- IM is now present in 90% of organizations, up from 63% of organizations in 2001.
- 24% of email users in the workplace also use IM, up from just 8% in 2001.
- 52% of organizations use IM for business applications, up from 21% in 2001.
- The 'Big Three' IM clients in use in the consumer world – AOL Instant Messenger, MSN Messenger and Yahoo! Messenger – are also the most widely used IM clients in the workplace.
- The two biggest concerns about IM use in the workplace, as expressed by three out of five IT and other technical staff members, are the security of information sent via IM and the potential for viruses and other threats to enter a corporate network through IM.

The two biggest concerns about IM use in the workplace, as expressed by three out of five IT and other technical staff members, are the security of information sent via IM and the potential for viruses and other threats to enter a corporate network through IM.

The Problem With IM in the Workplace

IM in the workplace can be an incredibly useful tool – it allows people to know when their co-workers are at their desk or available via a mobile device. It allows them to communicate in real time. It allows them to make decisions more quickly and to resolve problems more effectively. It allows people to keep track of their co-workers, knowing when it's best to contact them via telephone or serving as a pre-cursor to a telephone conversation. IM is often more useful than email because of its real-time nature and more useful than a telephone because it provides notification of another party's presence.

Interestingly, unlike virtually any other technology used by corporate employees, the deployment of IM was mostly initiated by employees, not IT. A March 2005 survey conducted by Osterman Research found that in 69% of organizations, IM was introduced without the involvement or blessing of the IT department. Instead, in most organizations users simply download their own copy of one of the popular

consumer-grade instant messaging clients, install it on their work PC and start using IM on their own. This has created three quite serious problems for organizations:

1. **Security**
   Consumer-grade IM systems completely bypass corporate defenses against viruses, worms, spyware, spam and other messaging threats. Consequently, users can easily introduce a variety of threats into a network simply through the normal use of their IM client. A variety of sources have announced that the number of IM-related threats has been increasing rapidly during the first quarter of 2005.

Consumer-grade IM systems completely bypass corporate defenses against viruses, worms, spyware, spam and other messaging threats. Consequently, users can easily introduce a variety of threats into a network simply through the normal use of their IM client.

2. **Control**
   A user of a consumer-grade IM client can choose his or her own IM 'handle' and can use it to conduct business for their employer. 'BigBadBilly' or 'CutieSue' are unlikely to be screen names that would be approved by most corporate managers.

3. **Liability**
   Most consumer IM systems do not offer any network-wide logging or monitoring capabilities, meaning that IM conversations are lost once the users end their IM 'conversations'. This is a particular problem for organizations that need to archive messages for compliance or knowledge management purposes.

What You Can Do

If IM is not managed effectively, it can create significant security and other problems for an organization of any size. Here's what any organization should do to assess how IM can be most effectively managed:

- **Become aware of the problem**
  Find out how much IM is being used in your organization. Many IT managers and CIOs assume that their users are not using IM, only to find out that there is significant IM traffic running across their network on a daily basis. Companies like Deerfield.com and others offer a detection tool that can reveal IM use (and abuse) of all the major IM platforms in your organization.

- **Assess the utility of IM**
  Just like email or any other communications medium, IM must be managed effectively. If an organization has a

requirement to archive certain types of documents because of regulatory obligations or advice from legal counsel, it is critical that IM content be included in the archived content. So, it's important to have a clear understanding of how you want IM used in your organization. new technology enables you to manage IM at many different levels:

- Monitor excessive usage
- Block IM
- Block IM except at certain times
- Block specific users while permitting others
- Restrict IM privileges
  - Employee to employee
  - Employee to customer/vendor
- Monitor and archive IM
- Archive and vault IM to compliance standards

It's also important to select tools that match the requirements of your organization – selecting an IM management system that can scale to 100,000 users is likely overkill for a 75-person firm that might one day have 200 employees.

- **Establish corporate policies about IM use**
  It's important to have a corporate policy that reinforces your technology solution, whether the policy is simply to block all IM traffic, to permit selected users to employ the technology, to allow the use of IM at certain times, to allow only internal use of IM and so forth. However, keep in mind that a policy alone is typically not enough to stop unregulated IM use and abuse.

- **Pick the right tools**
  There are a number of very good solutions on the market that can provide organizations with the security, productivity and liability control to secure use of public IM platforms. There are also a number of good enterprise-grade IM systems that have these features built-in. It's important to determine which tools your organization needs to manage IM most effectively. It's also important to select tools that match the requirements of your organization – selecting an IM management system that can scale to 100,000 users likely will provide more capabilities (and cost) than a small and mid-sized businesses (SMBs) will ever need.

The IMbrella Value Proposition

It's important to understand that good IM management is important for all organizations, not just for the Fortune 500. SMBs face the same issues with IM control and productivity loss and, in many cases, face even more problems because

the problems with IM can be magnified in smaller organizations.

Deerfield.com is focused on the SMB market and offers an evolutionary set of products that enable SMBs to detect, block, control, secure and archive IM communications. Instead of lumping all of these features into a single, expensive offering, the company's IMBrella offering allows customers to upgrade these capabilities at their own pace and as their IM management requirements grow.

IMBrella starts at just $99 and allow organizations to incrementally add as few or as many features as they want. IMBrella installs on any admin PC that has access to the network. They analyze all Web traffic via a proprietary MessageStorm technology and allow easy detection, management and archiving of instant messages. IMbrella is invisible to employees and requires no extra hardware, client applications or desktop maintenance.

The following product matrix illustrates the evolutionary capabilities of IMBrella:

Product	Capabilities
IM Detector	**Designed for companies to fully understand how much IM is occurring on their network so they can determine what to do about it.**
IM Spotlight	**Records the IM content and use of one employee (three screen names)**
IM Blocker	**Blocks all AOL, MSN, Yahoo and ICQ,**
IM Blocker Plus	**Same as IM Blocker but lets admin specify times (days/weeks/hours) when IM is allowed.**
IM GateKeeper	**Enables companies to permit specific users to send and receive IM.**
IMBrella Secure Enterprise	**For companies who want to control privileges for All IM users.**
IMBrella Secure Enterprise Pro	**For companies who want to control privileges for All IM users AND LOG all IM conversations.**
IMBrella Enterprise/ Compliance	**For public companies (SOX), NASD- and HIPAA-regulated firms**