





To take advantage of instant messaging's benefits and overcome its challenges, organizations must implement processes and technologies to manage it effectively.

Jesse Wilkins, CDIA+

Instant messaging, or "IM," is considered a dirty word in many organizations – when it is considered at all – and for good reason. As IM usage continues to grow, IM clients provide yet another vector through which organizations can be infected with viruses and spyware. In addition, employees may spend excessive time sending instant messages rather than completing assigned duties. And they may be using IM to circumvent many information technology rules and prescriptions.

IM Explained

IM applications share similar functionality. A user accesses a web-based application or downloads a client, creates an account, and logs in. Once the user is logged in, the IM system notes his/her "presence" and updates the system to reflect the user's current status. As the user's status changes – for example,

from "available" to "on the phone" – the updated status is pushed out to other users on the system that have the user listed in their contacts.

This presence information is one of the most compelling aspects of IM long-term; as applications become presence-aware, real-time collaboration becomes much simpler to set up: just look for who is currently available and set up an *ad hoc* collaborative session on the fly. Microsoft Office and Adobe Acrobat are among the applications that support this functionality today, with many more software vendors examining the possibilities presence could bring to their applications.

Sending messages is simple. Just type the message, hit "send," and the message is transmitted in real time to the intended recipient. Sending photos or other files is just as easy, and some clients include the ability to share files using drag and drop. The interfaces are fairly clean and simple.

In many organizations, IM is not implemented by the IT staff; rather, individual users download and install public chat clients from MSN, Yahoo!, AOL, ICQ, Google, and many others. According to a survey from the American Management Association and the ePolicy Institute, 50 percent of workers are downloading and installing free IM tools – but only 31 percent of organizations have a policy on IM in place.

At the Core

This article

- ▶ Discusses instant messaging (IM) usage in organizations
- ▶ Examines the challenges IM introduces to organizations
- ▶ Identifies strategies and tools to address those challenges

However, IM can also be a tremendous boon to an organization. From enabling collaboration to easing the strain of the overloaded e-mail inbox, IM can significantly increase employee productivity – if it is managed effectively.

The Four Phases of IM

IM usage in organizations can be described in four phases:

1. *Ignorance:* The organization does not know about IM, doesn't think its employees know about IM, and to the extent it thinks about IM at all, it considers it a tool teenagers use to waste time. This is perhaps the most dangerous phase because of the potential for unwary IM users to introduce viruses and other malware into the organization.
2. *Denial:* The organization determines that IM is present and forbids its further use for a number of reasons, including its potential for spyware and viruses, the amount of time employees waste using it, and, at more highly regulated organizations, the problems it presents for regulatory compliance.
3. *Acceptance:* This phase is characterized by efforts to take control of IM usage through policies and procedures. Organizations may also try to standardize on a single network and client version and begin investigating enterprise messaging solutions.
4. *Optimization:* This phase is far off for most organizations. It involves integrating IM into existing business processes and even optimizing processes around IM functionality. Part of the challenge is that enterprise IM is relatively new, and the functionality is not well-integrated into other information management solutions. This is slowly starting to change, but much work remains before

Top Business-Related Uses for IM

According to AOL's Third-Annual Instant Messenger Survey in 2005, instant messaging (IM) usage is up 19 percent year over year and is deeply entrenched at home, work, school, and on the road, with many Americans sending as many – if not more – instant messages than e-mails.

The survey revealed that 77 percent of at-work IM users feel that IM has had a positive impact on their work lives. The top reasons cited for using IM at work include to

Communicate with colleagues	58%
Get a quick answer on a business matter	49%
Communicate with clients or customers	28%
Exchange files	25%
Send and receive information while on a conference call	24%
Send URLs to colleagues	23%
Organize in-person meetings	22%
Use a chat feature for work-related conferences	19%
Organize conference calls	15%
Avoid potentially difficult in-person conversation with a colleague	12%

IM is considered a mission-critical application along the lines of e-mail.


Instant Headaches

Sending an instant message is as easy as clicking a contact in the contact list, typing the message, and clicking “send.” But using IM isn’t that simple. IM systems present many challenges for the organization that must be addressed to maximize the effectiveness of the system and avoid unnecessary risk.

First, IM is very informal. When users communicate via IM, the resulting conversations are brief, casual, and flow across any number of topics. It is not uncommon for IM traffic to feature cryptic abbreviations such as ROFL (rolling on the floor laughing), TTYL (talk to you later), or IMHO (in my humble opinion). Most IM clients also allow emoticons (“smileys”), some of which are not particularly professional.

This informality often extends to the user’s account name or “handle.” While many users are responsible in their selection of a handle, it is not uncommon to see IM traffic from “bigboyinCO” or “smurfy123.” This presents a real challenge to an organization in two aspects. Not only does the handle reflect poorly on the organization, but it also can make it quite difficult to determine later who actually sent that particular message. After all, who is going to admit that they send instant messages under the handle “HotCOGuy”?

IM networks are generally closed and do not allow users to communicate directly with other IM networks. This has been especially true regarding commercial IM networks, including AOL, ICQ, Yahoo!, and MSN. Each network created its own proprietary protocol in order to provide its own enhanced functionality and to increase its appeal versus other networks. This is similar to e-mail systems 10 years ago, when e-mail users with accounts through AOL and Compuserve, for example, could not send e-mail between the two companies’ networks.



Perhaps the single biggest **challenge** IM poses to the organization deals with **retention** of IM traffic. IM is a **format** or **medium** and not a **content type** or **record series**.

Efforts have been ongoing for a number of years to develop clients that would allow users to send instant messages across different networks. The commercial networks were quite aggressive in changing their protocols to ensure that these clients would not gain traction, but this is finally starting to change. The proliferation of different clients and the need to be able to access users employing different networks have pushed the networks toward interoperability. Last year, MSN and Yahoo! announced that they would allow their clients to send instant messages to users on either network.

In addition, in 1999 the open-source community developed an eXtensible Markup Language (XML)-based protocol for IM called “Jabber” that sought to provide interoperability and standardization of presencing and IM traffic. In 2004, the Jabber protocol became an Internet Engineering Task Force standard called eXtensible Messaging and Presence Protocol (XMPP) and has gained widespread support, including from most of the commercial networks. Google, in particular, has embraced XMPP and will allow its Google Talk client to access any IM network running XMPP.

The advent of XMPP and other standard presencing protocols, including Session Initiation Protocol (SIP) and SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE), have contributed to making interoperability at

least conceivable.

Another challenge for organizations is the sheer breadth of functionality available to most IM clients. Users can chat one-on-one or set up group or conference chats. Most of the networks provide a basic phone call capability and the ability to transmit video and audio with the appropriate equipment. Users can chat with any other users that are available on the network, meaning that they can bypass filters and ethical walls.

Users can also send files with little regard to format or size limitations – most of the commercial networks support 10MB file sizes for their free clients and 20MB or more for premium users. The networks generally provide some virus-scanning functionality, but the responsibility remains with the organization. This is an effective way to circumvent IT restrictions on file sizes and formats. And the clients allow users to transmit live URLs, which may or may not resolve to the link shown in the client. This is similar to phishing in the e-mail world.

Perhaps the single biggest challenge IM poses to the organization deals with retention of IM traffic. IM is a format or medium and not a content type or record series. Instant messages should be man-

aged the same way as e-mail, word processing documents, or paper records are – according to the content of the messages. But this is no simple task with most IM applications. IM systems do not store or retain messages in a central location; in fact, with some IM systems, once the presence is established, the traffic is exchanged directly between users in a peer-to-peer fashion.

The commercial networks provide the ability to locally archive message traffic, but this capability has its own drawbacks. On the one hand, message traffic may be stored as plaintext or XML, meaning that it is trivial to edit the contents; on the other hand, some systems use proprietary formats, which are slightly more difficult to edit but also more difficult to review and monitor. If a user chooses not to archive the traffic, there is no archive available to be reviewed.

Traffic is generally stored either by user, by conversation, or by day, meaning that there may be thousands of files to review in the event it becomes necessary to do so. It is difficult to separate record traffic from non-record traffic because of the free-flowing nature of the discussions. And the traffic is stored locally on the user's PC or laptop, which further exacerbates an already difficult situation.

It should be noted that many organizations treat IM as the equivalent of a phone call: the information is transitory and, therefore, need not be managed effectively. The key difference is that in many organizations, phone calls are not recorded or are only transcribed and summarized, while an IM client that is set to archive traffic will archive all of it – and all of that traffic is potentially discoverable.

The Perils of Prohibition

But it is not easy to eradicate IM from the organization for a number of reasons. IM is very easy to install and use. Employers that allow access to the Internet generally do not block the common search engines, such as Google, Yahoo!, and MSN – and each of these



In environments where **speed is critical**, such as securities dealing and energy trading, IM provides both **rapid access** and a **confirmation** that **someone** at the other end has **responded**.

offers links to download their network's IM client on the home page.

Another approach is to try to block IM using technology, such as by preventing employees from installing software to their computers. Most of the commercial providers also offer web-based access to their IM networks, meaning there is nothing to install and no real way to block access short of blocking the entire domain. Some IT administrators will try to block the ports IM clients use to send messaging traffic, but many of the clients exhibit port-seeking behavior; that is, they will keep trying ports until they find an open one. And some of them will use the default port for accessing the web so the traffic looks like web surfing rather than IM.

Even locking down the client PCs is not 100-percent effective because many IM applications have web-based clients. It may be difficult to lock down laptops for road warriors – particularly if the laptops are not owned by the organization. And many smart phones today support one or more IM networks, providing still another avenue to block.

While the technology challenges to blocking IM are significant, they pale in comparison to the organizational and cultural challenges. Employees who use IM frequently do so in order to be more productive, not less. IM is quite useful

in a customer service environment, where an agent on the phone with a customer can send an IM to a coworker or supervisor to request additional assistance.

More importantly, customers want IM. In environments where speed is critical, such as securities dealing and energy trading, IM provides both rapid access and a confirmation that someone at the other end has responded. This also requires that the organization support not only the use of IM, but also multiple IM clients and networks.

Policies and Procedures

A better approach to taking control of IM starts with updating information management policies to address the challenges identified above. An effective IM policy should contain guidance similar to other communications policies, including whether IM is to be used for only business activities, only personal activities, or some combination of both. The policy should identify topics that are off-limits, whether because the content is unprofessional or because it is too sensitive for IM.

The policy also should include spe-

cific guidance on whether attachments can be sent and, if so, what the limitations are. It should also address whether external communications are permitted and whether attachments will be allowed. The policy should describe whether transmissions are to be archived and how this is to be done. And if the organization chooses to add disclaimers into the message stream, this should be identified in the policy as well.

Users must be trained on the IM policy, just as with any other, and they must be reminded periodically of proper IM usage in accordance with that policy. The organization must review adherence to the policy periodically and take corrective actions as required to ensure compliance.

Tools and Technologies

Once the policy is in place and users are trained to follow it, organizations can look to technology solutions to assist in managing IM. These broadly fall into two approaches: gateways and enterprise IM (EIM).

Gateway applications and appliances offer much of the functionality that is missing from traditional commercial networks but is required for effective management of IM traffic and communications. Gateways also provide some ability for users to communicate across networks, with support for several of the most common commercial networks.

EIM solutions take a different approach, replacing the commercial networks with a single enterprise-wide client. This allows for more granular control over what functionality users have and how policies are enforced. EIM administrators can pre-populate users' "buddy lists" up to the inclusion of the entire corporate directory. And EIM solutions also provide secure encrypted communications, a key security issue for organizations concerned about sensitive communications.

Both gateways and EIM solutions include centralized archiving of supported networks' traffic; attachment fil-



tering and virus scanning; controls on content transmission and on which users and groups can exchange information; enforcement of user-naming policies and identity management; and the ability to prevent internal users from communicating to external ones. Gateways and EIM solutions can also be used together to provide the best features of both solutions.

The Bottom Line

IM is coming into its own as a

mature communications technology. Organizations would be well-served to consider the benefits it can provide in terms of efficiency, reductions in e-mail traffic, and ease of use – while at the same time putting into place the processes and technologies to manage IM traffic effectively. ■■

Jesse Wilkins, CDIA+, is a principal consultant with Access Sciences Corp., a RIM consulting firm based in Houston, Texas. He specializes in electronic records management, messaging, and collaborative issues and strategies. He may be contacted at jjwilkins@accesssciences.com.

References

"2006 Workplace E-Mail, Instant Messaging & Blog Survey: Bosses Battle Risk by Firing E-Mail, IM & Blog Violators." American Management Association and The ePolicy Institute, 11 July 2006. Available at www.amanet.org/press/amanews/2006/blogs_2006.htm (accessed 1 February 2007).

Baskin, Brian. *Google Talking*. Rockland, MA: Syngress Press, 2007.

Flynn, Nancy. *Instant Messaging Rules*. New York: AMACOM, 2004.

Piccard, Paul. *Securing IM and P2P Applications for the Enterprise*. Rockland, MA: Syngress Press, 2006.

RFC 3921, *Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence*. Available at <ftp://ftp.isi.edu/in-notes/rfc3921.txt> (accessed 1 February 2007).