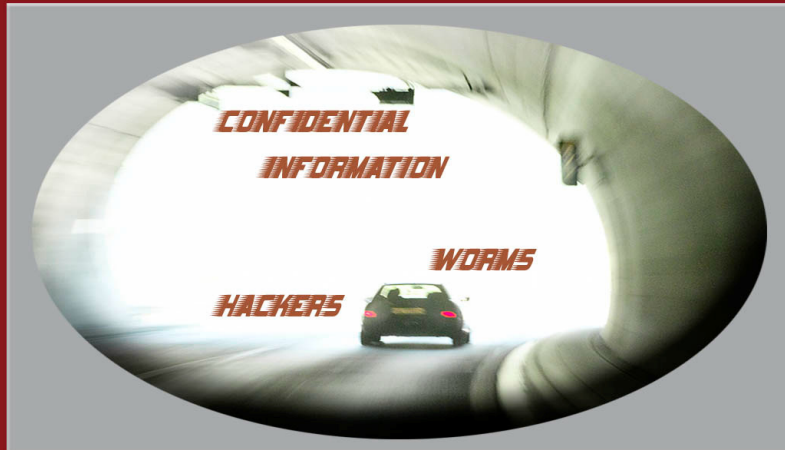


UNMANAGED INSTANT MESSAGING



**BORES TUNNELS THROUGH YOUR
CORPORATE NETWORK'S FIREWALL**

Instant Messaging Could Create SECURITY LAPSES in Your Corporate Network

*Companies Are Now
Scrambling to Get
IM Under Control*

By Boyd Zack

IS INSTANT MESSAGING beginning to replace traditional e-mail in your workplace? If so, it must be managed properly to make sure your corporation's proprietary information remains safe and secure.

Instant Messaging migrated to businesses quickly from the consumer market and is now a smash hit with corporate America. However, security lapses created in its wake have IT managers singing the blues. Why? The very features that allow key players in corporate business to handle routine communications fast and efficiently have drilled gaping holes in network firewalls that, in some cases, have placed confidential information on the Internet in full public view.

This whole mess started when corporate executives discovered instant messaging allowed key people to reach them throughout the day, thereby preventing routine business from getting bogged down. The problem is, the new system worked so well that people within the corporate environment adopted it informally and no one gave any thought to se-

curity until IT managers noticed their firewalls were being violated and confidential information was unsecured and sometimes available for viewing on the Internet.

Instant Messaging, or IM as it is known in the tech world, invaded corporate offices at an alarming rate as email became too slow and unreliable for critical communications. With the need to 'work at the speed of business' and the influx of SPAM, newsletters and opt-in services, e-mail communications no longer foot the bill.

Where just a few years ago, most business people could expect a response to e-mail within a few minutes or hours, today we often wonder if our messages reach their desired recipients through the gauntlet of SPAM filters and flood of non-urgent messages. IM delivered an immediate solution to the problem.

Currently, 85% of corporations across America use some form of IM and it is rapidly becoming the communication norm for businesses. A 2004 Pew Internet & American

Instant Messaging migrated to businesses quickly from the consumer market and is now a smash hit with corporate America. However, security lapses created in its wake have IT managers singing the blues.

Life survey revealed that more than four in 10 online Americans use instant messaging. That reflects about 53 million American adults who use instant messaging programs. About 11 million of them IM at work and they are becoming fond of its capacity to encourage productivity and interoffice cooperation. Where once we turned to the phone, and then to e-mail, IM has proven to be fast and efficient for urgent communications.

While most technology gains come from the top down, or from the IT department out, IM has experienced more of a grass roots deployment. Users are freely downloading public IM tools such as AIM, Yahoo Messenger and MSN Messenger for corporate use. According to IDC, the IM industry is expected to double in size to become a \$2.4 billion a year business by 2007.

The issues public IM tools bring to corporations are multifaceted and run the gamut from IT related concerns to corporate privacy leaks. When corporate communications are flying across the Internet in non-encrypted, plain text format, simple port monitoring and packet sniffing programs can intercept messages with ease. Public IM tools also employ central archiving of messages on the provider's networks, making them prime targets for hackers to attack.

By opening ports on corporate networks, public IM tools expose private networks to dangerous and potentially damaging threats. Communication ports allow for traffic to flow in and out of networks. Unchecked, these ports can open networks to attacks. These can range from simple file exploitation to complete denial of services.

Downloading and installing unauthorized software on systems has ramifications that should not be overlooked. Every application loaded onto a machine has the potential to conflict with other applications present on the system. Without proper testing of how software programs interact within existing environments, conflicts that arise can result in lost time and resources.

The introduction of consumer products into the corporate environment frequently results in loss of productivity. When seeking to increase productivity, companies consistently look for tools that will provide benefit. The problem with turning to consumer products is that they simply were not designed for corporate use. When looking for a corporate phone solution, rarely will the home use phone system foot the bill. Corporate IM solutions should not be viewed any differently than other productivity tools being introduced into the business environment.

So, if consumer public IM tools introduce too many security concerns, what is corporate America to do about their

IM needs? With the cat out of the bag, there is no turning back! Corporate IT managers must act now to ensure that their networks are secure and their users have a reliable, industrial strength IM tool at their disposal.

One approach is to employ an IM manager that sits on top of the public IM programs. This approach allows IT managers to manage and control instant messaging while continuing to utilize the public tools. These tools allow for local storage of message history and enable a level of virus checking that reduces some of the risks of public IM. However, they do nothing to address the fact that corporate communications are flying freely over the Internet in plain sight.

Another approach is to employ a secure instant messaging solution designed specifically for business. Tools such as *Jabber™*, IBM's *Sametime™*, Microsoft's *LCS 2005* and R.B. Zack & Associates' *IMiN™* address business requirements far better than public IM programs. Security, functionality and compliance requirements are all forethoughts rather than afterthoughts for each of these tools.

With Sarbanes-Oxley (SOX) and other regulatory concerns, some companies are adopting IM logging as an attempt to satisfy their retention requirements. With public IM tools, messages are stored on some remote server out of the control of the corporate communications officer. This means that in order for the communications being sent and received by these public tools to be acceptably retained, third party tools are being adopted to run on top of the public IM and record all corporate communications.

Currently, 85% of corporations across America use some form of IM and it is rapidly becoming the communication norm for businesses.

Secure IM solutions are likely to become the next generation of tools in the IT arsenal to properly and effectively manage corporate communications. Public IM opens holes in corporate firewalls allowing for unwanted intrusion in to private networks. Public IM exposes potentially confidential corporate information to public communication lines (the Internet) in unencrypted, unsecured plain text. Public IM can introduce potentially dangerous virus and worm threats to networks through attachments, trojans and hijacked messages. Secure IM is the only fail-safe approach to deal with the dangers of public IM use in the corporate environment.

When employing secure IM solutions, accessibility, encryption, availability and use can be controlled through an internal administration area. Secure IM allows corporate IT teams to control and manage instant message communications in much the same way as they manage other corporate communications. Tools such as IMiN can be configured to use the highest level of encryption for mes-

sages traveling outside the corporate network, and minimal or no encryption for messages that never leave the network. This means that any messages that travel across public communication lines cannot be accessed, even if they are intercepted in transmission, and that internal IM traffic need not take the resources required for encryption and de-encryption while safe within the network. Secure IM also enables corporations to be in compliance with regulatory mandates for communication retention.

With SOX requirements for corporate communications monitoring and retention, free wheeling public IM use within corporations simply will not fly. SOX regulations require that corporate communications be retained for a period of time. While IM logging tools such as IM Manager™ allow for retention of communications, they do nothing to prevent messages from flying across the Internet in plain view. IM logging tools can be useful in gaining compliance, as well as effective with strong policies in place that prohibit the transmission of confidential information in the form of IM.

Corporate tools designed for secure instant messaging for business come in several forms with differing benefits and drawbacks. Jabber is an open source solution that has the benefit of being an open source platform. It also has the drawbacks that are inherent in open source solutions. While the source code is available to IT departments, it is also available to potential hackers who are always looking for exploits to attack. IM Logics IM Manager™ affords the benefit of message logging and interfacing with several IM protocols. It also has the drawback of relying on outside services to relay messages and track presence awareness. IMiN™ has the benefit of running securely within the corporate network, yet lacks the interface to public IM tools such as Yahoo Messenger and MSN Communicator.

When looking for a corporate IM solution for business, the IT manager must be sure to be aware of what will work for their company. Ease of use, presence awareness, history retention and security are only a few of the characteristics that must be addressed. If the primary concern is with an open interface, Jabber may make sense. If the primary concern is executive acceptance, then ease of use must be number one and IMiN™, with the one-touch-response technology, must be considered. If the primary concern is one of security for messages traveling over the

Internet, then a solution must be implemented that incorporates an encryption mechanism that will keep corporate information safe.

Other aspects to consider when selecting a secure corporate IM solution include ease of maintenance, deployment and administration. Any large-scale operation, with hundreds or thousands of desktop machines to support, fully understands the need for automated updates and deployment features such as Active Directory integration. Software that is designed to detect newer versions and automatically install updates will lessen the burden on IT staff required to keep systems up to date.

Instant messaging is here and must be dealt with to keep networks up and running smoothly. Getting IM under control is no longer a luxury, but a requirement in corporate America. The risks of public IM to corporations are real. The benefits of secure instant messaging for business are very exciting!

Boyd Zack is the President of R.B. Zack & Associates, a Torrance-based company with over 20 years experience in the development, implementation, maintenance, and support of custom business software.

Get Your Crucial Messages Instantly While Keeping Your Network Secure!

Locate your colleagues wherever they are

Real Time Communications

Quick One Touch Keys

Announce Calls

Secure Instant Messaging For Business

IMiN™ is a new offering from R.B. Zack & Associates, Inc.

**To learn more, please visit our web site
at www.ebs-imin.com or call (310) 303-3320 x126**