By Laurie MacDonald, Kenneth Fougere, and Kenneth Sousa

Peer reviewed

Laurie MacDonald lemac@bryant.edu and Kenneth Fougere are Professors of CIS and Kenneth Sousa an Assistant Professor *of CIS* at Bryant University.

Abstract

Instant Messaging technology has the potential to be a valuable communication tool at many levels of the business enterprise and is already in use by employees in 85 percent of North American companies. Worldwide business use of IM is expected to reach 670 million in 2008. IM is a primary means of communication for college students and many institutions are learning to exploit IM to improve communications. However, instant messaging presents some serious security risks. This paper will review some of the major security risks and recommend management practices to enhance the level of IM security. The security posture of internal staff plays a major role in an organization's security. A survey of IM business users conducted by the authors indicates that a higher level of security is found at companies with sound management practices.

Introduction

The use of Instant Messaging (IM) in business has already reached significant proportions and will continue to grow. The research firm Radicati has found that employees in 85 percent of North American companies use IM on a regular basis and the number of IM users worldwide is expected to reach 670 million in 2008, up from 362 million today (Gonsalves). IM provides fast, flexible communication and can be a valuable business asset. Many business people are learning that IM can be a real benefit through improved communications. Virgin Atlantic Airlines learned this lesson in 2002 when a tropical storm threatened the delivery of key parts to a disabled plane. Sterling Courier Services used IM to coordinate the delivery schedule to land in Barbados during a lull in the storm (Shein).

According to researchers at the Gartner group, IM has the potential to improve performance at many levels of business processes, and they recommend that businesses adopt IM as a communication tool using corporate versions of IM (Caplan Grey; Foo). IM use is expected to account for 60 percent of all data messaging by businesses by the end of 2005 (Abraham). While this growth is ongoing, IM does present some potentially serious security risks. IM establishes a persistent, long-lived connection to another PC, as compared to the relatively short-lived connections for web-browsing. This can create an opening for hackers and viruses to enter a business' network (Brandel).

IM Security

IM provides an inviting target for hackers because it is generally less protected than other Internet applications such as email and Web browsing. It is a relatively new technology, and many users are not prepared to use it safely. A security flaw found in Yahoo IM allowed a hacker to cause a buffer overflow by transmitting a file with a long name. A buffer overflow allows a hacker to run malicious code on a target computer (Saunders). Yahoo moved quickly to patch the security flaw, but there are other problems with IM. A total of 25 IM worms have been identified since 2002, and the number of attacks on IM increased by 400 percent from 2002 to 2003 (Gaudin; Greek). An attack using IM has the potential to spread malware at incredible speeds. Worms typically ping IP addresses looking for vulnerable machines. "Code Red" needed 14 hours to ping all possible IP addresses, and the "Slammer" worm improved that time to 20 minutes. Using buddy lists, an IM attack could spread across the Internet in seconds (Keizer).

There is no intrinsic audit-trail to protect sensitive documents that might lead to Sarbanes-Oxley infringements for the organization and other privacy issues (Abraham; Anonymous, *Why Instant Messenger Security?*). All email users are familiar with spam, but some are unaware of the IM version of spam, nicknamed spim. An example is "Osama Found", which was spread on AOL Instant Messenger as spim (Bird). Spim can easily overcome a users PC and clog servers (Regan). "Osama Found", also called "BuddyLinks", is a game that gets permission from users to send ads to all the

addresses on their IM buddy lists. It is not a virus or any other type of malware; rather it is spim or adware and is a perfect example of how quickly malware could be spread via IM. The standard virus protections used with email are typically bypassed by IM (Hurley).

There is a serious effort underway to fight spam, as is evidenced by the passage of the CAN-SPAM Act by Congress in 2003. However, this legislation refers only to email spam and never mentions IM. Spammers are likely to move from email to IM as the government and Internet Service Providers (ISP) continue to crack down on e-mail abuse (Bird).

Importance of Information Systems Security

Information security has traditionally been focused on employees, but the widespread use of the internet has changed the focus of security concerns. Today IT managers are increasingly concerned about the security and authenticity of these systems. Information security is noted as one of the top ten technologies for 2006 by the American Institute of Certified Public Accountants. Information security technology includes hardware, software, procedures, policies, and user education (Anonymous, *Top 10 Technologies 2006)*.

A study by the Computer Security Institute (CSI) revealed that a significant number of corporations and government agencies (74 percent) reported a security breach within the last twelve months *(*Anonymous*, Csi/Fbi Computer Crime and Security Survey*). Of more importance, a significant number of respondents (26 percent) reported that they do not know whether or not their organization was the victim of a security breach. The priorities of information systems management are often unclear in relation to the importance of security issues. The strategic and organizational importance of web-based information systems may provide the rationale for increasing a security infrastructure (Aber; Nelms).

There has been a continuous increase in security threats, and that trend is expected to continue (Radcliff). New threats are devised almost daily by hackers *(*Anonymous*, Security Specialists Report Cybercrime Losses Down for Third_Straight Year*). Clearly, it is the responsibility of an organization to implement basic security procedures (Nelms). A well trained user is the first line defense against threats to the information system.

Academic institutions can gain the benefits of IM but will not be immune from the security threats posed by this technology. Sound management of the technology and security awareness training for faculty, students, and staff is essential.
Academic institutions should address IM quickly because their students have already adopted IM as a primary means of communication (Baker). Among the many potential uses of IM in academic institutions are recruiting and admissions, group projects, and student-faculty conferences (Cohn). Some institutions are already using IM as part of their admissions process. At Boston University admissions counselors use IM to answer

questions from prospective students. Truman State University's admissions office has been using IM for four years (Haberkorn). The Office of Undergraduate and Graduate Admissions at Mount Aloysius College provides a list of AOL Instant Messenger screen names on their web site and invites prospective students to use IM to contact admissions representatives *(*Anonymous*, Instant Messaging for Real Time Conversations*).

The key to IM security, as with all information security, lies with management of the technology and how it is used by staff at all levels. Managers at all levels must be champions of information security and ensure that all employees are trained to understand the importance of security (Pearlson and Saunders). IM requires effective management for an organization to achieve the benefits offered by this technology (King).

A Sound IM Security System

A sound IM security system should be an integral part of an organization's overall information security system. A sound system begins with a formal security policy that spells out the allowed uses of system resources. This is a critical step in developing a secure information system (Ciampa). A well-written and consistently enforced security policy acts as the basis for all security practices and allows the organization to respond quickly and effectively to any security incident (Anonymous*, Developing an Information Security Policy*). Volonino and Robinson (Volonino and Robinson) state that an "acceptable use policy" will limit system misuse and reduce exposure to legal liability in the event of a security breach.

IM providers are making an ongoing effort to improve the security of IM, but sound management practices should be in place no matter how many improvements are made to the technology (Betts; Anonymous*, Why Instant Messenger Security?; Reiss*). A framework for IM security management includes the following:

Acceptable Use Policy

The first step in allowing IM within the organization is to implement an Acceptable Use Policy. Employees should be made aware that IM can only be used with the express permission of management and confidential information should never be sent via IM.

Block IM

It is good security practice to disable all unnecessary services, and IM should be viewed under this rubric. Start by blocking all IM traffic, and add functionality as proven needs arise. Add rules to the firewall to block messages, file transfers, and access to all popular IM servers.

IM Training and Security Awareness

The inbound security threats posed by IM should be understood by all members of the user community. Training in the acceptable use of IM should be an integral part of an overall security training and awareness program. Implement procedures to monitor IM to enforce the organization's "acceptable use policy". Trained and alert users are the best defense against threats to your systems.

Firewall Protection

Use a gateway product to route messages on the organization intranet and to interface with outside IM clients. This proxy server can scan for viruses, filter for sensitive content using a keyword list, and archive all messages to a database.

File Transfers

Collaboration on documents and spreadsheets is a common and important and useful practice, but unless files attached to IM are being scanned for viruses, then files transfers should be blocked. If file transfers are going to be allowed, users should be prompted before any transfer occurs.

Known Users

Decide who in the organization has a valid business reason for using IM and disallow it for everyone else. Consequences for unauthorized use will be made clear in the "acceptable use policy" (see above).

Spam Blocking

IM from unknown users should be blocked to protect users from social engineering, inappropriate content, and messages that are simply a waste of their time.

Desktop Protection

Antivirus software, personal firewalls, and anti-spyware software at the desktop level are the last line of defense against IM delivered malware. These basic protections should be installed on all local machines.

Even companies with security policies need to keep in mind that employees play a major role in information security, and their behavior can frustrate technological safeguards (Volonino and Robinson). Employees constitute one of the most serious threats to an organization's information security (Whitman and Mattord). Therefore, trained and alert users will remain the best defense against hackers, viruses, and spim. Security awareness training and a strictly enforced Acceptable Use Policy are the foundation for the secure use of IM.

Research Methodology

A research study conducted by the authors explored the use of instant messenger software within an organizational context. A survey questionnaire was designed by the authors to gather responses relating to security measures employed by businesses using instant messaging. A survey was used to explore the use of instant messaging and the associated security implications. For the purposes of this survey, two categories of questions were used to create a survey instrument consisting of eighteen questions. Each section was used to gathered information on the organization (five questions) and technology infrastructure (thirteen questions). Information gathered in the section about the organization being surveyed concerned demographic data relating to its size, industry type, and whether instant messaging software was utilized. The other section's questions gathered information about the security procedures and various software features enabled with instant messaging software.

In order to administer an effective and accurate survey instrument, nine members of the target group were asked to participate in a pre-test survey for evaluation and review. Each of the participants was asked to provide feedback on the readability and content of the survey. Their feedback responses were evaluated and, when appropriate, applied to the final survey document. The changes made as the result of the pre-test increased the clarity, validity and accuracy of the instrument as the focus of gathering measurement data.

The population used to administer the survey consisted of 490 business professionals who were also part-time graduate students enrolled in MBA and MSIS programs at Bryant University. Each member of the population received an email at their business address asking for their participation in this research that included a hyperlink to the web-based survey instrument. Responses to the survey were stored electronically for subsequent retrieval and analysis.

Discussion

A total of 125 responses were received through the web-based survey administration, a 25.5 percent response rate. The distribution of responses by industry activity is shown in Table One (below). The majority of the survey respondents (53 percent) were employed by three industries: financial services, manufacturing and education. However, respondents employed by manufacturing organizations did not show a proportionate use of instant messaging software. Based on the survey data, the computer software and services industry has adopted the use of the software at a rate greater than manufacturing.

Table One: Use of Instant Messaging Software by Industry

Industry	Response Percent
Manufacturing	14%
Construction	1%
Utilities	2%
Computer Software/Services	7%
Education, Training	10%
Healthcare, Medical	9%
Banking, Insurance, Financial Services	29%
Government, Military	8%
Wholesale, Trade	1%
Hotel, Restaurant, Hospitality	1%
Accounting, Consulting	6%
Legal Services	1%
Retail	3%
Other	10%

The results for the thirteen questions addressing the IM security environment are displayed in Table Two (below). The results show that the approach to IM security is mixed. Some of the recommended IM security management practices noted above are followed, while many are not.

Table Two: Percent Reporting (n = 39)

Question	Yes	No	Do Not Know
A documented IM policy is published and enforced	41.0	46.2	12.8
Security training is provided for the safe use of instant messaging	12.8	66.7	20.5
Information technology department supports IM software	64.1	25.6	10.3
File transfers through IM are supported	28.2	46.2	25.6
Instant messaging is maintained behind a firewall	64.1	15.4	20.5
Instant messaging is supported by a gateway or proxy server	46.2	33.3	20.5
Software patches are implemented regularly for IM services	41.0	30.8	28.2
Spam blocking has been implemented by IM	33.3	33.3	33.4
All IM sessions are logged	33.3	30.8	35.9
Messages are filtered for content	17.9	46.2	35.9
Virus scanning is applied to messages	28.2	33.3	38.5
Messages are archived for storage	28.2	38.5	33.3
Messages are encrypted	17.9	46.2	35.9

On the plus side, 64.1 percent of respondents reported that their company's IT department supports IM software applications. This is one of only two instances were a clear majority reported sound security practice. The second is the 64.1 percent who reported that IM is maintained behind a firewall. Additional positive results, but not clear majorities, were found for file transfers, which are prohibited at 46.2 percent of the respondent's companies; the use a gateway or proxy server by 46.2 percent of respondents; and 41.0 percent who said that software patches are implemented regularly for Instant Messaging services.

Spam blocking and logging of IM sessions are enforced at only 33 percent of the respondent's organizations. Forty-one percent of the respondents indicated that they had a published IM policy which is enforced at their company. However, 46.2 percent reported that no such policy is enforced at their company. The results for other IM practices recommended in this paper are a clear indication that IM security is not being addressed at many of the organizations surveyed. 46.2 percent reported that IM message content is not filtered, and only 17.9 percent said that such filtering is done. 28.2 percent reported that IM is scanned for viruses, while 33.3 percent reported that no virus scanning is in place. Archiving of messages was reported by 28.2 percent, and encryption was reported by only 17.9 percent of those answering the survey. An overwhelming majority (66.7 percent) indicated that no security training is provided for the safe use of IM.

Table Three (below) presents a comparison of companies that have documented IM Policy in effect (n =16) and those with no policy in place (n = 23).

Table 3: Percent Reporting (n = 39)

Question	Policy	No Policy
Security training is provided for the safe use of instant messaging	31.3	0.0
Information technology department supports IM software	100	39.1
File transfers through IM are supported	12.5	39.1
Instant messaging is maintained behind a firewall	87.5	47.8
Instant messaging is supported by a gateway or proxy server	81.3	21.7
Software patches are implemented regularly for IM services	75.0	17.4
Spam blocking has been implemented by IM	50.0	21.7
All IM sessions are logged	62.5	13.0
Messages are filtered for content	43.8	0.0
Virus scanning is applied to messages	50.0	13.0
Messages are archived for storage	62.5	4.3
Messages are encrypted	43.8	0.0

Table Three reveals that there are a number of major differences in the security of their instant messaging applications. The IT department supports IM software at all companies with a policy versus only 39.1 percent with no policy. Security training is under utilized at all of the companies with no training at any of no-policy companies. The 31.3 percent providing security training is hardly encouraging. Approximately three times as many non-policy companies (39.1 percent) allow file transfers via IM compared to companies with an IM policy (12.5 percent). Significant majorities of the respondents working under a documented IM policy were noted for using IM behind a firewall (87.5 percent), supporting IM by a gateway or proxy server (81.3 percent), and implementing software patches (75.0 percent). Each of these is much higher percent than at the non-policy companies. Logging of IM sessions (62.5 percent) and archiving messages (62.55) are the only other security measures that were reported by a majority. While 43.8 percent of the companies with an IM policy encrypt messages and filter them for content, none of the no-policy companies do so. Spam blocking and virus scanning has been implemented for IM by 50.0 percent of the companies with a policy. These measures are employed by 21.7 percent and 13.0 percent respectively of the no-policy companies.

Conclusions

Instant Messaging is a powerful and useful communications tool that companies are still learning how to exploit its potential. As we learn new ways to use instant messaging, we must start to address the security threats inherent in this technology. Staff charged with managing the institution's technology can provide technological safeguards. The survey data gathered for this study demonstrate that the existence of a

documented and enforced policy that spells out the acceptable use of instant messaging is an often ignored first step in ensuring the security of IM software.

REFERENCES

Aber, R. "A Comprehensive Approach to Security." *Business Communications Review* 33.5 (2003): 17.

Abraham, Harold. "Top Ten Technologies for 2005". 2004. *NextInnovator.com*. Available: http://nextinnovator.com/index.php?articleID=3003&sectionID=18. June 18, 2004 2004.

Anonymous. "Csi/Fbi Computer Crime and Security Survey". San Francisco, CA: *Computer Security Institute*, 2003.

---. "Developing an Information Security Policy". 2001. *JISC*. Available: http://www.jisc.ac.uk/index.cfm?name=pub_smbp_infosec. May 14, 2006 2006.

---. "Instant Messaging for Real Time Conversations". 2004. *Mount Aloysius College*. Available: http://www.mtaloy.edu/admissions_chat.htm. June 28, 2004 2004.

---. "Security Specialists Report Cybercrime Losses Down for Third Straight Year". June 10, 2004 2004. *Computer Security Institute*. Available: Security Specialists Report Cybercrime Losses Down for Third Straight Year. June 26, 2004 2004.

---. "Top 10 Technologies 2006". 2006. *AICPA*. Available: http://infotech.aicpa.org/Resources/Top++10+Technologies/Top+10+Technologies+2006/. December 6, 2006 2006.

---. "Why Instant Messenger Security?" 2004. *Zone Labs*. Available: http://www.zonelabs.com/store/content/company/corpsales/imSecurity.jsp. May 26, 2004 2004.

Baker, Andrew. "Instant Messaging Becoming Part of College Culture". 2004. webpage. *Elon University, The Pendulum Online*. Available: http://www.elon.edu/e-web/pendulum/Issues/2004/3_18/features/aolim.xhtml. June 1, 2004 2004.

Betts, Mitch. "Sidebar: More Tips for Boosting Im Security". July 14, 2003 2003. *Computer World*. Available: http://www.computerworld.com/printthis/2003/0,4814,82915,00.html. May 26, 2004 2004.

Bird, Drew. "Think Spam Is Tough? Try Fighting Spim". June 8, 2004 2004. *Instant Messenging Planet*. Available: www.instantmessagingplanet.com/enterprise/article.php/3365281. June 18, 2004 2004.

Brandel, Mary." Plug Im's Security Gaps". June 8, 2004 2003. *Computerworld*. Available: http://www.computerworld.com/printthis/2003/0,4814,82943,00.html. May 26, 2004 2004.

Caplan Grey, Maurene. "Instant Messaging (Im): Gartner Gives Insight". 2004. CT *Technology Council*. Available: http://www.ct.org/News/CTCNews.asp?Path=220. June 18, 2004 2004.

Ciampa, Mark. "Security Awareness: Applying Practical Security in Your World". Cambridge, Massachusetts: *Course Technology*, 2004.

Cohn, Ellen R. "Instant Messaging in Higher Education: A New Faculty Development Challenge". 2002. *webpage*. Available: http://www.ipfw.edu/as/tohe/2002/Papers/cohn2.htm. June 1, 2004 2004.

Foo, Fran. "Enterprises Should Embrace Im: Gartner". November 12, 2003 2003. *ZD Net.* Available: http://www.zdnet.com.au/news/business/0,39023166,20280890,00.htm. November 1, 2004 2004.

Gaudin, Sharon." Im -- a Threat to Network Security". June 24, 2004 2004. *eSecurity Planet.com*. Available: http://www.esecurityplanet.com/trends/article.php/3373251. June 18, 2004 2004.

Gonsalves, Antone. "Free Im Is Hard to Beat in the Enterprise". June 13, 2004 2004. webpage. *The Radicati Group*. Available: http://www.radicati.com/cgi-local/news.pl. June 18, 2004 2004.

Greek, Dinah. "Instant Messaging Falls Prey to Hackers". 2003. *Vnune*t. Available: http://www2.vnunet.com/News/1144318. June 26, 2004 2004.

Haberkorn, Jen. "Colleges Reach out Via Instant Messaging". June 24, 2004 2004. *The Washington Times*. Available: http://washtimes.com/business/20040623-114522-1105r.htm. June 28, 2004 2004.

Hurley, Edward. "Aim 'Scumware' No Buddy of Mine". February 12, 2004 2004. *SearchSecurity.com*. Available: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci950178,00.html. June 1, 2004 2004.

Keizer, Gregg. "Symantec Warns That IM Worms Could Devastate Business". June 18, 2004 2004. *Information Week*. Available: http://www.informationweek.com/story/showArticle.jhtml?articleID=22100814. June 23, 2004 2004.

King, Nelson. "Chatting up an Im Management Strategy". 2004. *Serverwatch.com*. Available: http://www.serverwatch.com/tutorials/article.php/10825_3405751_2/. December 6, 2006 2006.

Nelms, Clinton F. "Computer Security." *The National Public Accountant* (2003): 30.

Pearlson, Keri, and Carol S. Saunders. *Mananging & Using Information Systems: A Strategic Approach*. Hoboken, NJ: John Wiley & Sons, Inc., 2006.

Radcliff, Deborah. "Security under the Gun." *Computerworld* 36.23 (2002): 36.

Regan, Keith. "Instant Messaging Creates Security Headaches for Enterprises". March 8, 2004 2004. *TechTarget.com*. Available: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci954061,00.html. June 1, 2004 2004.

Reiss, Francis J. "Instant Messaging Security Concerns and Recommended Best Practices Sans". May 19, 2003 2003. *SANS Institute*. Available: http://www.giac.org/practical/GSEC/Frank_Reiss_GSEC.pdf. June 23, 2003 2003.

Saunders, Christopher. "Yahoo! Clamps Down on Im Security, Mulls Upgrades". January 13, 2004 2004. *Instant Messenger Planet*. Available: http://www.instantmessagingplanet.com/public/article.php/3298941. June 1, 2004 2004.

Shein, Ester. "Will Im Pay?" May 4, 2004 2004. *CFO.com*. Available: http://www.cfo.com/printarticle/0,5317,13507|M,00.html?f=options. June 18, 2004 2004.

Volonino, Linda, and Stephen R. Robinson. *Principles and Practices of Information Security*: Protecting Computers from Hackers and Lawyers. Upper Saddle River, NJ: Pearson Prentice Hall, 2004.

Whitman, Michael E., and Hebert J. Mattord. *Principles of Imformation Security*. Cambridge, MA: Thomson Course Technology, 2005.

http://www.westga.edu/~bquest

A journal of applied topics in business and economics