



November 2004

META Group Says 57per-cent of Employees Use Work Instant Messaging for Personal Reasons, Tells Employers to Develop an “IM Policies” to Regulate Use

Instant messaging (IM) is most frequently used at work, not at home, according to a survey of 300 global organizations released by META Group, a leading provider of information technology (IT) research, advisory services, and strategic consulting. However, META Group cautions that just because messaging takes place at work does not mean it is work-related. According to the survey, 57per-cent of respondents use IM at work for personal reasons. Perhaps more surprising are findings that suggest 56per-cent of respondents use IM at home for business purposes.

"Organizations should view these numbers as alarming," said Ted Tzirimis, senior research analyst at META Group. "Although IM can be a valuable tool for real-time communication and collaboration, it can also have a viral effect when not regulated. Organizations must implement strategies to harness the value that can be derived from sanctioned use of IM while limiting personal use of the application."

According to META Group research, companies have taken a different approach toward managing personal use of IM than they have for e-mail and phone use. Although only 3 per-cent and 5 per-cent of companies prohibit personal use of phone and e-mail respectively, nearly 16 per-cent of companies have banned the use of IM completely. Similarly, while 68 per-cent of companies allow limited use of e-mail for personal reasons, only 44 per-cent allow the same for IM. Finally, over 35 per-cent of companies have no official policy regarding instant messaging. META Group believes that this approach fundamentally ignores the inevitability of IM use within the enterprise. In fact, research suggests that, by 2008, enterprise IM use will become as pervasive as e-mail.

"The good news for companies is that, although policy creation is not a silver bullet to stop unsanctioned IM use, it is easy and relatively inexpensive," said Tzirimis. "Moreover, our survey suggests that it can also be a fairly effective measure for controlling use of IM."

Survey findings indicate that just under half of all respondents (49 per-cent) would comply with a corporate policy banning the personal use of IM. Forty-one percent of those polled would limit personal IM use to emergency situations, while only 10 per-cent indicated they would ignore the ban and continue to use IM regularly.

While organizations wrestle with corporate policy and continue to search for ways to harness the value and limit the risk inherent in IM, users continue to recognize the benefits

ITAA E-LETTER

For more information: Mark Uncapher, Senior Vice President & Counsel, *INTERNET Commerce & Communications Division*; Information Technology Association of America, 1401 Wilson Blvd. #1100 Arlington, VA 22209; 703-284-5344-direct, 703-525-2279 fax; muncapher@itaa.org; Division Website <<http://www.itaa.org/isec>> ITAA E-Letter <<http://www.itaa.org/isec/pubs/ecurrent.cfm>> Association text links <<http://www.internet-association.org/>>

ALL RIGHTS RESERVED

of messaging. According to the survey, the IM benefits most frequently cited by respondents can be divided into three categories — efficiency, presence, and cost savings:

- **Efficiency:** Faster response than e-mail (78 per-cent), fast problem resolution (74 per-cent), and multitasking (71 per-cent). Closely related are the ability to get someone's attention (62 per-cent), to reach someone who has not returned a voice or e-mail message (37 per-cent), and to gather information (32 per-cent).
- **Presence:** The ability to see if someone is online/available/free (63 per-cent).
- **Cost savings:** Reduced expenses by not using long-distance calling (37 per-cent).

META Group analysts caution, however, that more widespread and varied use of IM could lead to increased network vulnerability. Although 95 per-cent of work IM use is still limited to messaging, more than 41 per-cent of users are leveraging IM for file transfer functions. The file transfer function should be alarming to CIOs, since it places an enterprise at risk for potential viruses, worms, Trojan horses, and disclosure of IP address information to potential hackers.

CIOs must also be aware of the growing threat of SPIM (i.e., SPAM for instant messaging). Although 72 per-cent of respondents have yet to receive a SPIM message, those that have average 2.4 SPIM messages per day. META Group expects this number to increase dramatically as IM becomes more prominent and connectivity with other systems becomes easier. As SPIM increases, it will represent the same type of drain on resources as SPAM's effect on e-mail. Moreover, the real-time speed with which malicious packages can be propagated is a major issue that CIOs must address.

"CIOs must begin to fully explore options for managing IM," concluded Tzirimis. "They must weigh the risks of inaction against the realities of current use and the potential benefits of embracing IM. An IM policy is a good first step, but it is only that. The more difficult step is discerning how to successfully implement and use IM within the enterprise."