

Tackle Instant Messaging's Security Risks -- Now

David Mitchell Smith

Instant messaging can improve communication and productivity, but it has high security risks. Gartner urges enterprises to develop effective security measures immediately to avoid potentially severe risks.

NEWS ANALYSIS

Event

On 11 October 2001, Gartner warned of security risks to enterprises as more and more employees use free commercial instant messaging (IM).

Analysis

IM is growing rapidly (see *Research Note AV-14-0650 "Instant Messaging: The Sleeping Giant"*). Some 200 million users worldwide have signed up for IM IDs on the major free services. Gartner estimates that by 2003, 70 percent of enterprises will have workers using such services. In one sense, this trend is good. Like e-mail before it, IM has tremendous potential for improving worker productivity. Properly managed and integrated into business workflows, IM can dramatically increase a company's ability to operate as a real-time enterprise. Here are just some of IM's uses:

- As an adjunct to traditional customer relationship management (CRM) systems IM can give immediacy and intimacy to customer interactions that e-mail cannot.
- In many software development environments, programmers have made IM the collaborative communication tool of choice.
- During conference calls, IM serves as a useful back channel for remote participants.

But, also like e-mail, IM represents a potentially severe security risk. Free IM systems introduce a host of security concerns: instant messages are transmitted as clear text, using simplistic, proprietary and unsecure protocols. Furthermore, messages enter corporate networks through nonstandard TCP ports. Unlike e-mail systems, IM attachments cannot be easily scanned for viruses.

After e-mail use in business became widespread, it took more than 10 years before enterprises began to address security, reliability and business policy effectively. To avoid repeating the painful and costly lessons taught by e-mail, Gartner urges enterprises to develop effective enterprisewide IM security policies and procedures now. Management attempts to quell IM use — even in the face of legitimate security concerns — would likely trigger an officewide revolt. The inevitability of IM use, with workers often using more than one commercial IM system, makes it all the more important for managers to develop protocols for IM within the enterprise.

Analytical Source: David Smith, Internet Strategies

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509