

Entrepreneur

solutions for growing businesses

JANUARY 2003

MANAGEMENT

Instant Mess

smart moves: GRAB THE SPACKLE. INSTANT MESSAGING IS THE LATEST CRACK IN YOUR SECURITY.

RAPID GROWTH IN INSTANT MESSAGING IS causing equally rapid growth in risk for any business with employees who use it. Theft of confidential information, infection by computer viruses, invasion by hackers and potentially devastating lawsuits are just a few of the risks cited by experts on the dangers of workplace proliferation of IM, as it's popularly known.

By Mark Henricks

next step: The ePolicy Institute has sample electronic communications policies as well as studies of the risks arising from e-mail and other Internet usage at www.epolicyinstitute.com.

Use of IM at work doubled last year, according to figures from research firm Jupitermedia. ComScore Media Metrix Inc., another technology-trend-tracking firm, says more than 17 million Americans used IM at work in June 2002, up from less than 14 million in November 2001. Other analysts say that by the end of next year, IM will be used at work by someone in nearly every U.S. company.



ILLUSTRATION © J.T. MORROW

Reducing Your Risk

Controlling the rampant growth in IM use—and risk—is a challenge. The big IM services, those from AOL, MSN and Yahoo!, use protocols capable of slipping through most corporate firewalls. Even monitoring IM use by employees can be a tricky and costly solution, requiring the purchase of expensive and sophisticated security software. “You have a bad combination for business users,” warns Michael Gartenberg of Jupitermedia.

Given the risks and constraints, small companies should try to limit IM risk with policies that attempt to reduce

employees’ exposure to instant danger. Flynn says the ideal instant messaging policy should focus first on controlling the content of messages.

Content policies should outline specifically banned language, such as profanity and threats, as well as taboo topics. Corporate secrets, personal information or comments about fellow employees, potentially slanderous digs at rivals, and just about all types of jokes should be on the list, Flynn says.

Also restrict the people who can be communicated with via IM. Instant messages can include file attachments that may host

destructive computer viruses, so IMing should be limited to known, trusted correspondents. For instance, you may approve IMs between employees, but forbid messages to customers, suppliers, government regulators, news media and members of the public.

It's also a good idea to limit the times and places in which IM can be used. Firms may allow employees to use IM

only after hours, during lunch and other breaks, or for specified amounts of time, Flynn says.

Make sure your IM policy is written and disseminated to employees. Ideally, get everyone to sign a statement testifying that they have seen and understand the policy as well as the reasons for having it, and penalties, such as disciplinary action or termination, for violators.

An important last step is to train your employees in how to use IM without exposing the company to undue risk. Only about a third of companies that have electronic communications policies train employees to implement them, Flynn says. "You need to make it very clear to your employees what is appropriate and inappropriate use."

Reprinted for web use by permission of Entrepreneur Magazine, ©2003 all rights reserved. For Subscription Information Call 1-800-274-6229.

Reprinted by Scoop ReprintSource 1-800-767-3263