

Messaging Creep

Beware the instant messenger

Like it or not, instant messaging (IM) is coming. According to some researchers, two-thirds of all organizations in the United States will adopt enterprise IM by the middle of 2007. While I usually take projections like this with a grain of salt, a recent internal survey here at Bentley College in Massachusetts revealed that 38 percent of our administrative staff was already using an IM tool we had enabled without any fanfare or endorsement just months earlier.

Instant messaging is a natural for the business world for the same reason email was adopted so readily: it's an effective way to



By Traci Logan

Instant messaging is a natural for the business world.

share information. As businesses embrace new technologies, however, employees inevitably exploit them. So what exactly does the forthcoming era of IM mean for IT and the organizations that have to manage its impact?

From the perspective of enterprise infrastructure and operational practices, IM mirrors email in many ways. The real twists and turns will be found on the other side of the equation when the choices employees make create a new set of dilemmas, which will hinge on corporate culture and education as opposed to infrastructure.

As with email, the informal nature of IM creates a false sense of refuge in the workplace precisely because it is used so casually outside of work. Employees will fall prey by forgetting this distinction; organizations will fall victim by forgetting that IM content can and will be used as evidence in legal proceedings.

With IM's entrenchment in the workplace will come software services intent on managing this activity—services designed to assess how quickly an employee is responding or how much time is being spent on an IM thread. There will even be

Web-based messaging systems designed to leave no traces. It isn't enough, however, to rely on regulatory requirements or software to force businesses to cast a larger shadow over personal privacy and retention of electronic communications. Businesses must adapt by developing their own understanding of how these forms of communication can and will influence their corporate culture. Too many organizations have permitted a publicly embarrassing incident to be the catalyst for change and self-examination. The recent IM case involving former United States Senator Mark Foley provides a superb example, not only of poor judgment by an individual, but also of an allegedly collective carelessness about managing it.

Just as identity theft heightened our duty to protect personal privacy, our legal exposure with regard to technology-enabled personal expression ought to deepen our responsibility to educate employees. Computing use policies should be reviewed and updated regularly, but this measure alone is hardly sufficient. Employees must be told at orientation—and frequently reminded by their managers—that email and IM content transmitted via company resources is neither confidential nor private. Management training must include illustrative cases established around themes of virtual communication, right along with the more familiar subjects of diversity and sexual harassment. In addition, organizations must assess employees' behaviors and attitudes about personal boundaries and privacy as part of the annual performance review process.

We must acknowledge both the value and consequences of technology in the workplace, as we instill in our employees an active curiosity about the same. ■

▶ Read online:
www.symantec.com/ciodigest/thinktank/logan

Traci A. Logan is vice president of information technology and vice provost of academic affairs at Bentley College near Boston, Massachusetts.