BUSINESS NH
MAGAZINE

Submit Ads

Send your ad files to us online.

Submit ▶

Email Updates

Sign up for email updates for when the new magazine comes out.

Sign Up ▶

Upcoming Events

Business of the Year Awards Luncheon
May 19, 2009
11:30 am - 1:30 pm
Sign Up ▶

News

Monitoring Web Surfing at Work

Published Friday, April 24, 2009
by MATTHEW J. MOWRY

It's just a couple of minutes to check that stock I bought. Five minutes to check if my bid on e-Bay won. It won't hurt, right? And if I periodically check my Facebook or Yahoo! Sports page, there's no harm in that.

But all those minutes can add up throughout the day or week. In fact, 30 to 40 percent of Internet use in the workplace is not related to business, according to IDC, a Massachusetts-based provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets.

And it could go up. As the popularity of social networking services like My Space and Facebook continue to increase, Keith Bamford, CEO of Daystar Computer Services in Portsmouth, says employers have more reason to be concerned about productivity issues and what employees are actually doing during work time. "As an owner, that's the stuff I worry about," he says. "We're only starting to scratch the surface of community sites like Facebook. It's a real detriment to the office."

No one wants to be Big Brother, but at a time when companies are downsizing and productivity is essential for survival, monitoring Internet usage might be one way to ensure productivity and limit the security exposure of computer networks. As it is, non-work related Internet surfing results in up to a 40 percent loss in productivity each year, according to The Gartner Group, a Connecticut-based IT consulting firm.

Bamford says his firm has seen a slight uptick in inquiries from customers for such technology. However, he says its been primarily large businesses that actually implement a system. Small businesses often question whether they want to spend the money for such a service. "There's tons of solutions out there; everything from free products to localized applications to managed applications," he says. That includes new products coming on the market to monitor e-mail that can be paid for on a monthly basis, says Brian Wheeler, president of Resolve Technology, a Dover-based provider of outsourced IT services.

Content filtering technology allows a business to prevent employees from entering chat rooms, block them from certain Web sites and stop streaming radio, which eats up bandwidth, says Kirk Simione, president of Technology Seed in Londonderry. Such technology can also provide employers with a wealth of information on their employees' Internet activity. "You can receive automated reports about how long people have been online, what sites they have visited and if they tried visiting blocked sites," Simione says.

But before monitoring and/or blocking access to certain Internet

sites, employers must insure access to needed data. "You need to make sure employees have access to the information they need, but not have access to data they don't" says Tom Strickland, president of Sequoya Technologies Group, LLC in Peterborough. "An employee who opens information they don't need puts that data at risk." Strickland says he sees more demand in the small business market for managing the security of a network than requests for monitoring Internet access.

As for legal issues employers should consider, Laurel Van Buskirk, a labor and employment attorney with Devine Millimet law firm in Manchester says the best practice is to notify employees before monitoring their Web and e-mail activity. Under state and federal law, private employers can monitor e-mail and Internet activity on their systems, as well as voice mail, as long as employees have been notified and the company has implied consent. (Recording phone conversations legally requires the consent of both parties.)

Van Buskirk says employers need to craft a written policy that makes clear to employees that the company can monitor their activity on the company's computers and phone systems as those systems belong to the company. The policy should clearly outline what employees can and cannot do when it comes to e-mail and Internet use on company time and equipment and what the consequences will be if they violate the policy. Companies should be explicit that employees can have no expectation of privacy when using company equipment. She also recommends companies have an attorney review the policy before implementing it. Buskirk says companies should make sure every employee receives the written policy, whether it is through an employee handbook, written memo or other form of notification. "You then need to follow the policy consistently," she says.

Send this page to a friend

Show Other Stories