

Keeping tech toys away from workers

Curtailing use of personal technology is a balancing act for Kevin Rabin.

As office manager at Libow & Shaheen LLP in Boca Raton, Rabin must ensure the firm's 12 employees and work stations are focused on the practice of law. But he's also a realist; people also use the company's computers and Internet access to surf the net, check personal e-mail or make travel arrangements.

Reasonable use of the company's computers or Internet access is fine.

"In the day of the Information Age, to suppress access to information is not a good idea," Rabin said. "But within the confines of the work environment, you need to set certain standards for productivity."

If an employee spends time surfing the Web, visiting online dating sites or downloading music to his iPod using the company network and Internet access, is that acceptable?

The office is rife with consumer technology, devices, Web sites and services, many of which have no place in the workplace. Time wasted surfing and playing with gadgets also saps productivity.

Removing or transferring

data can place confidential or proprietary information at risk. Moreover, downloading large files like music or pictures consumes hard-drive space and valuable Internet bandwidth, said Andrew Judge, CEO of Grove Networks Inc., a Miami-based IT consulting firm.

"Today's small business computer environment is often subject to various threats, for which business owners often have few resources to prevent," Judge said.

Today's younger work force is accustomed to shooting photography or videography using cameraphones and sending those images to friends or posting them to sites like MySpace or Facebook. Yet such images can compromise corporate security. Bans on such products are becoming widespread in sensitive locations, like corporate network facilities and government buildings.

The issue of appropriate technology use also exists in corporate telework scenarios. Employees with company-issue laptops or Internet access at home via company-provided ISP or wireless broadband card often use the computer for a child's schoolwork or family use. This can expose the com-

puter and company network to viruses and attacks.

In another telework scenario, an employee might install on the company-issued computer instant messaging, screen savers, toolbars or other unauthorized software. That software could include tracking applications, or could conflict with software pre-installed by IT on the device. Because IT doesn't know of the unauthorized installation, they might face issues resolving conflicts.

Banning software installations, use of portable storage devices, and access to peer-to-peer file-sharing sites can lessen a company's exposure to outside threats.

CableOrganizer.com runs SurfControl. The Web content filtering software restricts employee access to "objectionable" destinations.

"Too many Web sites offend major groups of employees. It is our responsibility to protect employees from sites that would likely offend them," said Paul Holstein, founder of the Fort Lauderdale-based provider of wire and cable management solutions.

Next time: Writing appropriate technology use policies.



JEFF ZBAR
BIZ TECH

BANNING TECHNOLOGY

WHAT: Consumer technology, tools and practices in the workplace sap productivity and threaten the business.

COSTS: Range from free strategies to off-the-shelf software applications to setting reasonable standards for use.

