PROCESSOR

Tech & Trends

Click To Print

General Information
August 20, 2004 • Vol.26 Issue 34
Page(s) 19 in print issue

Spies Like Us

Reduce Liability With Workplace Monitoring, But Keep Your Employees Informed

In its early days, workplace employee monitoring conjured up images of the most intrusive types of corporate privacy invasion. Tales of keyboard monitors that could flag a worker who didn't spend every waking minute typing spread through the industry, seeming to foretell an Orwellian future where every action of an employee could be scrutinized.

In reality, while this kind of microscopic surveillance does happen in certain sectors, such as call centers, a broader need for a less intrusive form of monitoring has become more necessary in the current age of viruses, lawsuits, and increased productivity goals.

"The motivations are quite a number, and they're usually legitimate motivations," says Jeremy Grouber, legal director for the National Work Rights Institute. "Probably the most often cited reason for employer monitoring is productivity, wanting to make sure that employees are working when they're on the job and that they're not, as often times employers will say, spending eight hours a day on the Internet for nonwork related purposes. But, there are a lot of other reasons why employers might want to monitor. They have issues with potential legal issues, sexual harassment worries, potential theft of trade secrets, issues with excess use of bandwidth, but generally probably the most often cited reason has to do with productivity."

Erick Rohy, senior product manager at Websense (www.websense.com), points out that with the rise of P2P file sharing, there are even more legal problems that a company can face. According to him, organizations such as the Recording Industry Association of America have been taking legal action against companies, as well as their employees, when they discover illegal peer-to-peer file sharing being hosted in the workplace. "Appropriate filtering can also protect employees from malware and viruses, according to Rohy. One example he gives is the recent spate of phishing spam. "We actually have a category in our database called the Security Premium Group that will actually block people from going to phishing sites. And so you could be completely fooled by the email and you could be clicking on it thinking, 'Wow, I better enter my PIN number before my account gets deactivated.' Well, Websense will actually protect the employee by blocking access to that fraudulent site."

Tools Of The Trade

There are several ways that employers can monitor their employees' use of company computers and the Internet. The most publicized technologies are keyboard monitors and screen capture tools, such as SoftActivity's Activity Monitor (www.softactivity.com) or TrueActive Software's TrueActive Monitor (www.winwhatwhere.com). These allow management to peruse the keystrokes

entered on a computer or see what the employee was looking at. Statistics can also be gathered on productivity. Sometimes a keyboard monitor is used in conjunction with scanning software in environments such as legal firms, where it is important to track the potential transmittal of sensitive information. Mark Hewitt, network administrator at law firm Cooper, White & Cooper, points out that information can leave the building in many ways. “There’s ways around that. It’s kind of funny: The new things that are coming up that are more of an issue are CD burners and USB drives more than the Web.”

Filtering and monitoring Internet activity is a less intrusive but still effective means of reducing liability for a company. Websense Enterprise is a typical example of this type of product. It runs on a Windows, Linux, or Solaris server and intercepts traffic entering and leaving a company. It can be configured to block access to certain classes of sites and to monitor the sites that employees visit. The product automatically keeps up-to-date on what sites are offering pornography, sports, news, financial services, scams, etc. The employer can then choose which types of sites to allow. It also can monitor and block P2P and instant messaging traffic. Websense Enterprise costs around $15 per user in 1,000-user quantities.

Another example of an Internet monitor tool is Spectorsoft’s SpectorCNE (www.spectorsoft.com), with a cost of $495 for a 10-computer license. It differs from Websense in that it also provides keystroke monitoring functionality and is installed on the employee’s computer, rather than on a centralized server on the network. SpectorCNE is geared more toward monitoring of employees than blocking inappropriate action.

Transparency Is The Key

Surprisingly for a privacy-focused country, employees in the United States have very few rights in regards to workplace monitoring. “First of all, most employees don’t know that they’re being monitored,” says Grouber. He points out that there is no legal requirement in most states to notify employees of monitoring, and when notification is given, it is usually along the lines of, “We reserve the right to monitor at any time, at all times, for any purposes.”

According to Grouber, with workers spending more and more time at the office to meet productivity goals, they need to be able to keep their lives running, as well. An employee may need to call a doctor or make an appointment for his child. “You know the truth is if employees worked from 9 to 5 exclusively every day, this would become less of an issue, but the truth is that the lines between home and work began evaporating a long time ago.”

Grouber continues, “Part of the solution is certainly for employers to give substantive notice of their monitoring practices. That means that employers tell employees what they’re monitoring, when they’re monitoring, for what purpose they are monitoring so that employees have a specific understanding of what’s going on in the workplace.” He also believes that a reasonable-use policy is a smart practice for any company, laying out how and when employees can use their computers and telephones for noncompany activities. “With the advances that we’ve seen in monitoring technologies, they can now be customized to employers’ reasonable use policies so that employees can have both the privacy and the availability to conduct some small amounts of personal business.” ■

by James Turner

Liabilities Facing Companies

Is someone in your company downloading porn? Trading the latest in music via P2P file sharing? They could be setting you up for a lawsuit or exposing

themselves to identity theft. Here are a few of the ways that things can go wrong.

Inappropriate Web Use
• Lawsuits stemming from hostile work environment claims (pornography, hate sites)
• Loss of productivity

Email, Instant Messaging
• Loss of trade secrets, intellectual property

P2P applications
• Bandwidth hogging
• Copyright violations

Phishing
• Release of personal and corporate information

Copyright © 2009 Sandhills Publishing Company U.S.A. All rights reserved.