

THE



AUTOMATED



AGENCY



REPORT

This article reprinted with permission from the May 2005 (Volume 21, Number 5) issue of *TAAR, The Automated Agency Report*.

Who Watches the Websurfers?

Protect your business from hackers and cyberslackers.

by Michael A. Gold and Jim D. Bauch

It's 10:00 a.m. Do you know where — in cyberspace — your employees are?

An increasing number of companies are turning to monitoring software to find out. A 2004 survey by the American Management Association found that 60% of companies use some type of software to monitor their employees' incoming and outgoing e-mail — an increase from the 47% who did so in 2001.

The monitoring software available on the market today is capable of keeping tabs on more than just

e-mail. Employers can obtain reports on Web sites visited, as well as monitor or simply block the operation of instant messaging programs, spyware, file-sharing software, keyloggers, and other security threats.

Should you monitor your employees' Internet use?

You may not need much convincing of the practical benefits of monitoring your employees' use of the Internet. "Cyberslacking" — personal use of the Internet during work hours — is so common that the Oxford Dictionary of English now recognizes the term. Your IT department has probably had to contend with viruses and other malicious code spread through employee downloads, e-mails, and, most recently, instant messaging. There's also a good chance that on at least one occasion your network has slowed to a crawl while nearly everyone in the company viewed that "cute" animation that someone helpfully forwarded to all of his or her co-workers.

If employees know that their Internet use is being monitored, they tend to be more prudent in their computer activities.

But there are also good legal reasons for tracking your employees' cyber-activities.

Legal obligations

First, depending on the nature of your business, you may actually be under a legal obligation to take appropriate security measures. Industries like banking and medicine are subject to statutes and regulations that require them to make sure their employees are complying with rules for handling private information like financial or medical records. Even if you aren't in one of these industries, you may be doing business — or hoping to do business — with someone who is, and who needs assurances that your firm is willing and able to honor those restrictions.

In fact, many of your company's contracts may already require you to maintain the confidentiality of a customer's data. Even without such a provision, you could be held liable for the consequences if that information is, for example, leaked in an employee's e-mail, or stolen by a hacker who gained access to your system when that "cute" animation was downloaded and distributed.

You don't want to find yourself in a deposition or a trial being asked what you did to

prevent such a thing from happening. And if you do find yourself in that situation, you certainly don't want the answer to be "nothing."

Prevention

Second, an ounce of prevention is worth a pound of cure. If employees know that their Internet use is being monitored, they tend to be more prudent in their computer activities.

For example, one study found that 50% of employees reported being cautious about what they write in e-mails because of possible monitoring. This is a good thing: people tend to treat e-mail too casually, making off-the-cuff or out of context remarks that they would never put in a paper memo — even though e-mails are every bit (no pun intended) as permanent as a paper memo, if not more so. This is why e-mails are often a gold mine of ammunition for an adversary in litigation. If your employees start to think twice before they click "send," it could save you both embarrassment and money.

Similarly, you might think that common sense and simple courtesy to colleagues would keep workers from viewing or downloading pornography at the office. But one survey of 350 companies in the United States,

United Kingdom, and Australia showed that one-third of employees had used their company's Internet access to download pornography. Not only does this put the employer's computer system at risk of infection by viruses, spyware, and other threats, but it also makes the employer vulnerable to a lawsuit alleging a "hostile work environment" in violation of antidiscrimination law. That risk is further compounded if the employee, like the one-third of those surveyed, has e-mailed adult content to co-workers and others. Monitoring software can deter such inappropriate conduct, or at least alert management so the offender can be dealt with promptly.

Protection

Third, the information tracked by monitoring software could help you defend yourself in a lawsuit. For example, if you have to fire an employee for cyber-slacking, the ability to document exactly how much work time he or she was spending on the Internet could be critical if the employee claims the firing was discriminatory. Or, if an employee is secretly (he thinks) preparing to move to a competitor by downloading or forwarding proprietary information like client

Solutions

There are a variety of products on the market that help monitor and manage Internet usage. An area that often gets confused is the difference between monitoring and blocking. Many firewall solutions allow for the complete blocking of sites, but this is not the same as Internet monitoring. Blocking can be far too restrictive and difficult to manage in a dynamic business environment. There are three primary categories when looking at Internet monitoring and management solutions: desktop software, server-based software, and a network appliance.

Desktop software is an application that is loaded and maintained on every workstation in the organization. This solution usually carries a low cost to implement in a single office environment and can be installed and managed by an average user. However, this solution does not scale as the organization grows and becomes difficult to manage with a large number of workstations. The reporting is usually done from the same computer that the data was collected on and therefore may be difficult to retrieve while the user is working. Software bugs and incompatibilities with other applications can make installation difficult. Also, as users become more and more technically proficient, this type of solution can be detected and disabled by the end user.

Server software is loaded onto a new or existing server attached and integrated into the network. Initial costs for this type of solution may be lower than other options. This solution scales well for most businesses and allows for centralized management of all desktop clients and reporting. Some things to consider with this type of solution are: supporting hardware for the software may increase costs; software bugs and incompatibilities with existing software applications may make installation difficult; performance may be slower than an appliance-based solution because there is a requirement for an underlying operating system. Finally, this type of solution requires attention when mak-

ing changes to the network and often requires the installation of client software on workstations, which can increase support costs.

A network appliance is a solution that includes everything in a single box. There is no software to install on either a server or the workstations, and no additional hardware is needed. This solution may have a higher initial cost than other solutions and may require the assistance of a skilled technical person during the installation process. This solution will have the best performance because the hardware and software combination are dedicated and optimized to perform a unique set of tasks. Once installed, there is minimal technical management required, which means minimal maintenance costs. This type of solution scales very well for organizations of all sizes and provides centralized management and reporting. There is no underlying operating system to update and maintain. Finally, it is difficult to detect and circumvent because it is integrated into the network infrastructure.

With any of the options discussed above, if an organization is going to implement a solution, it is important that certain criteria are met. The solution should, at a minimum, monitor and manage the market leaders in instant messaging, peer-to-peer networking (P2P), and Web mail as well as the day-to-day browsing habits of network users. Managing your employees' Internet usage must provide measurable results from increased employee productivity and reduced exposure to litigation while providing a service that is scalable and manageable, delivering the return on investment demanded in today's business climate. A monthly fee structure that is based on the number of users being monitored helps reduce the large capital outlay traditionally associated with implementation of network-wide software. Whatever solution is selected, it must provide management with the tool it needs to monitor employee Internet activity from a corporate, managerial or individual level, in real time, and in a secure environment.

Nobody relishes the role of Big Brother. But what your employees do on your computer system is your business, and the risks of ignoring what they do are too great.

lists, monitoring software can provide an early warning and give you the evidence you need to obtain an injunction or other remedy from the court.

What about privacy?

Do employees have a right to privacy in what they do with their employer's computers or Internet access? Generally speaking, the answer is "not if you tell them that they don't."

You should check with your attorneys on the laws of your state, but typically privacy rights depend on whether or not the worker had a "reasonable expectation of privacy." This makes it very important that you clearly communicate to your employees — and have them acknowledge in writing — that company computers (including any company-issued laptops) and systems are property of the company, and are subject to monitoring by the

company.

As a practical matter, you wouldn't want to keep the existence of monitoring systems secret anyway. Remember, the main purpose of having a monitoring system is to deter improper use of company computers, not to play "gotcha" on unsuspecting employees.

Of course, you should also take steps to make sure monitoring software isn't abused. Limit access to the software and its reports to those who need it, and limit its use to what is necessary to make sure your policies are being complied with. Good monitoring software will allow you to customize what is detected and reported.

Implementing a policy

In addition to making your employees aware that their use of company computers can be monitored, you should have a clearly

stated and well-communicated policy on what is appropriate or inappropriate use.

Where you choose to draw the line will depend a lot on the nature of your business, the concerns your IT department has, and your management style. For example, many businesses ban the use of instant messaging programs like AIM or MSN Messenger because they can pose a security risk and often drain productivity, while others actually use such programs for some business communications.

It's also important to craft a policy that you're prepared to enforce: a moderate policy that is fairly and consistently applied is much better — from both a legal standpoint and for employee morale — than a strict policy that is routinely flaunted and selectively applied. For this reason, most businesses don't object to occasional personal use of email or the Web as long as it doesn't interfere with work or contain inappropriate content. Unless you're prepared to discipline every employee who pauses to type a quick hello to a friend or to check the sports scores on ESPN.com, your policy should allow for some similar leeway.

Summary

There's no putting the genie back into the bottle: the Internet

is an essential tool for modern workers, and insurance agencies are no exception. "Today it would be virtually impossible to interact effectively with carriers and insureds without it," noted Craig Fuher, CEO of iPrevision, Inc., a provider of Internet security solutions.

But, Fuher observes, "as with all technology, broadband Internet access requires an effective management approach to ensure Internet connectivity is

being used in the most efficient manner for the organization."

Nobody relishes the role of Big Brother. But what your employees do on your computer system is your business, and the risks of ignoring what they do are too great. You wouldn't allow employees to have access to the cash drawer without appropriate internal controls and accountability. Why would you allow them unfettered access to your computer systems in a business

world where information is just as valuable as cash? ♦

Copyright ©2005 Michael A. Gold, Jim D. Bauch, and JMBM. All rights reserved.


Michael A. Gold is a partner and a member of the Information Technology Group in the Los Angeles office of the law firm of Jeffer, Mangels, Butler & Marmaro LLP. **Jim D. Bauch** is a litigation associate at the firm.




YES, I'm interested in receiving TAAR. Please...

Subscription Order Form

- Enter my subscription: \$179 (U.S. Funds) for 12 issues (\$129 agency rate).
- Send me a FREE SAMPLE copy to review before I order.

Name _____ TEL _____
 Company _____ FAX _____
 Address _____ E-Mail _____
 City/State/ZIP _____

Check Enclosed Bill me Credit Card 

   Expiration Date _____

 Card Number

Mail or FAX to...
The Automated Agency Report, Inc.
PO Box 6218 • Broomfield, CO 80021-6218
 TEL 303.404.0457 • FAX 720.294.9797
www.taareport.com

Print Cardholder Name _____
 Signature _____

The Automated Agency Report (TAAR) provides Independent Agents with the insurance technology information they need to more effectively manage and grow their agencies. Annual subscriptions are \$129 for agencies, \$179 for all others. For more information or to request a sample issue please go to www.taareport.com or call 303.404.0457.

© Copyright 2005 by The Automated Agency Report, Inc. All rights reserved. Reproduction, by any means, of material appearing in TAAR, The Automated Agency Report is strictly forbidden without permission. ISSN# (0888-8205). TAAR, The Automated Agency Report is published monthly by The Automated Agency Report, Inc., 9711 Independence Way, Westminster, CO 80021. Periodicals Postage Paid at Broomfield, CO and at additional mailing offices. For more information, see www.taareport.com

