C A S E   S T U D Y

Cyber-Slacking Kills Productivity

By **David A. Fertell**

The Internet has transformed the way insurance companies do business. Pushing papers has been replaced by mouse-clicks and keystrokes. Insurance agents now use the Internet to research and process quotes, communicate with underwriters via email, issue payments and bind coverage. As many agencies have discovered, however, Internet efficiency does not come without a price. Just as employees once ran up phone bills making personal calls, agencies are now dealing with the growing problem of Internet misuse.

The insurance industry is not alone. Based on a study of 500 U.S. corporations, government agencies, financial institutions, medical institutions and universities, the 2002 Computer Crime and Security Survey reports that seventy-eight percent of respondents detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of email systems).

For financial institutions, productivity losses are only the tip of the iceberg. Internet abuse also includes the transmission of sensitive customer data such as Social Security numbers. This directly violates a provision of the Gramm-Leach-Bliley Act, which dictates that insurance companies must disclose how they use their customers' personal information. It is the agencies' responsibility to ensure that proprietary information is protected or they could face serious legal ramifications.

These issues drove Glasgow Hicks Company, an independent insurance agency in Wilmington, NC, to monitor Internet use. According to president and CEO, Charlotte Hicks, "You walk by employees' desks and see them furiously typing away, apparently hard at work. In reality they may be trading stocks or emailing jokes to friends."

Hicks asked Todd Brown of Cornerstōn Solutions, a firm specializing in outsourced technology consulting, to install software to monitor her employees' online habits. Brown's initial software choice, however, was difficult to manage because it worked on the premise of creating "allow" and "block" lists that dictated where employees could go online. Reflected Todd Brown, "It was a nightmare.

> **"While checking email use, I noticed one employee was sending up to 80 personal emails per day. After showing her the report, I didn't have to say another word."**

Every time an agent tried to visit a new web page, I had to manually make a change. It was incredibly frustrating for the agents and very time consuming for me."

Hicks and Brown knew there had to be a better way. They next tried Pearl Software's Pearl Echo® Internet Management Software. Pearl Echo provides employees with unfettered access to the Internet and then reports back on the sites they have visited. In addition to monitoring web browsing, Pearl Echo monitors most common forms of Internet communications including the content of email, chat, file transfers, news group postings and instant messaging. Pearl Echo can also be set to monitor keywords and phrases to protect privacy and the dissemination of confidential information. Charlotte Hicks recalled, "Our software investment paid off right away. While checking email use, I noticed one employee was sending up to 80 personal emails per day. After showing her the report, I didn't have to say another word. The problem was immediately resolved." Glasgow Hicks' employees were also relieved.

Instead of being blocked from many sites that were not on the "allow" list, they could now freely look for quotes or research new policies.

Like most Internet monitoring or filtering applications, Pearl Echo includes browser-based reports that make it easy to view corporate network activity. Charlotte Hicks runs her own reports to see what her agents are doing. Commented Hicks, "Since the new software has been installed, I have saved at least 5 hours per week. Now I glance at reports once a week—from my own desktop—to make sure that everyone is sticking to our Internet use policy."

Glasgow Hicks has an Acceptable Use Policy (AUP) in place to communicate what is acceptable for employees to do online. According to Hicks, simply having the policy and software in place acts as a deterrent to misuse.

"No one can say they didn't know the rules," observed Hicks. "An AUP is a must so that people know exactly what they can and cannot do online."

Although Glasgow Hicks has a zero tolerance policy for personal Internet use at work, other companies may choose to allow some personal access. For example, agencies can use a software application like Pearl Echo to restrict personal use to certain times of the day—during lunch, for example. Allowing employees to shop online at lunchtime sometimes prevents extended lunch hours. It also boosts morale by allowing employees to send email correspondence to family or accomplish online errands.

Some companies also monitor telecommuting employees who log onto the corporate network from home. With Pearl Echo's Global Internet Management (GIM) feature, workstations can be completely detached from a private network. Todd Brown explained, "If Glasgow Hicks allows employees to work from home via laptop, Pearl Echo's GIM feature will manage access regardless of how or where people connect to the Internet."

Internet monitoring software is a proactive way for agencies like Glasgow Hicks to conserve network resources and safeguard sensitive customer information. "Unfortunately, most insurance agencies don't realize they need monitoring software until they have been burned," lamented Charlotte Hicks. "The Internet is a great tool yet is also one of the biggest temptations for goofing off. Our strategy is to prevent abuse before it ever happens."

For more information about Pearl Software, Inc. please contact us at (800) 732-7596 or www.PearlSoftware.com