

SEATTLE POST-INTELLIGENCER

http://seattlepi.nwsourc.com/business/228317_email14.html

Companies hire e-mail sleuths**Aim of monitoring is to stop employees leaking trade secrets**

Tuesday, June 14, 2005

By DAVID HO
COX NEWS SERVICE

NEW YORK -- Corporate concerns about trade secrets leaking out through electronic cracks have led firms to hire staffers to scrutinize outbound e-mail and step up efforts to track employee Internet use.

More than a third of companies with 1,000 or more employees already have workers who monitor e-mail, and another 26.5 percent plan to hire new e-mail watchers, according to a survey by Proofpoint Inc., an e-mail security firm based in Cupertino, Calif.

About a third of companies use software to automatically scan e-mail for corporate secrets or content deemed offensive, the survey found.

"Employees should have no expectation of e-mail privacy in the workplace," Keith Crosley, Proofpoint's director of market development, said yesterday.

Companies reported their leading motivation for monitoring e-mail was worries about leaks of secrets and intellectual property.

More than a third of companies have investigated a suspected e-mail leak of confidential information in the past year, and a quarter have fired people for misusing e-mail, the survey of more than 300 firms found.

Having a dedicated staff reviewing e-mail means the monitoring is likely constant and not focused on investigating a particular person or incident, Crosley said. Such monitoring often samples message traffic because of the enormous amount of e-mail sent from a typical company.

"E-mail is the worst way to communicate information that's confidential, potentially embarrassing, extremely personal or that could in some way harm you, your family, your friends or your employer," said Nancy Flynn, executive director of the ePolicy Institute, a Columbus, Ohio-based consulting firm.

Another motivation for increased e-mail surveillance is the threat of lawsuits. One in five employers have had e-mail subpoenaed by courts or regulators, according to a separate 2005 study released last month by the ePolicy Institute and the American Management Association in New York.

"E-mail today is the electronic equivalent of DNA evidence," Flynn said. "If you don't want to pick up the newspaper tomorrow and read your e-mail message or you don't want to hear it read on CNN tomorrow, don't send that message."

It is legal for U.S. companies to monitor employee e-mail and Internet use on corporate equipment and networks.

More than three-quarters of companies monitor employee Web surfing, and more than a third track worker keystrokes and the time spent at keyboards, the ePolicy survey found. About 65 percent of companies use software to block connections to certain Web sites.

Companies also are concerned about instant messaging programs that can circumvent the protections of corporate networks, creating a channel for confidential information to reach the public Internet, Flynn said. Compared with e-mail surveillance, few firms use technology to monitor, block or archive instant messages.

She said it is "a whole new level of security threat."

With the increase in monitoring, more firms are establishing policies for electronic communication in the workplace, she said. More than four in five have policies governing personal e-mail and Internet use, and about one in five have rules about blog postings.

"Companies with good legal advice are telling their employees when they come through the door about monitoring policies," said Chris Hoofnagle, director of the Electronic Privacy Information Center's San Francisco office.

Hoofnagle said there is the potential for abuse where e-mail is read by curious technical personnel.

Ideally, he said, "you should only engage in monitoring where employees are suspected of wrongdoing."

On the Web:

Proofpoint: www.proofpoint.com

ePolicy Institute: www.epolicyinstitute.com

American Management Association: www.amanet.org

Electronic Privacy Information Center: www.epic.org

© 1998-2005 *Seattle Post-Intelligencer*