Human Resource Executive

NOVEMBER 2001 • $8.95

Security

Establishing and enforcing policies for e-mail and Internet use and abuse are the only real ways to thwart inappropriate or compromising communications.

Mischief Breakers

Nancy Flynn, executive director of the ePolicy Institute in Columbus, Ohio, and the author of The ePolicy Handbook

BY MAURA C. CICCARELLI

Twent-20 New York Times Co. employees in the company’s Norwalk, Conn., business office were fired for sending around a series of lewd e-mails. Two Baltimore Smith Barney executives lose their jobs for electronically transmitting pornography. Dow Chemical in Midland, Mich., terminates 50 workers for e-mail abuse. Employees and contractors at the Merck & Co. pharmaceutical giant face disciplin and potential dismissal for inappropriate e-mail and Internet usage.

Hair was pulled up when these stories flashed across the news over the last three years. While on the face of it the actions taken by the companies seem extreme, perhaps even hideous, the reality is it’s not a laughing matter. It’s a legal one.

When the American Management Association surveyed 1,209 members earlier this year, it found that nearly 60 percent monitor Internet connections, almost 60 percent store and review e-mail messages, and 40 percent store and review computer files. About 70 percent of those companies cited legal liability as their top reason for monitoring employees.

That’s because employee misuse and abuse of e-mail and the Internet is starting to play a significant role in workplace issues, says Nancy Flynn, executive director of the ePolicy Institute in Columbus, Ohio, and author of The ePolicy Handbook published by the AMA.

"Sendency e-mails are common in workplace harassment cases," says Flynn. "There’s no one who’s not affected.

Patricia J. E. Hope, president and founder of Litigation Management and Training Services in Long Beach, Calif., says e-mail is a "hot topic because it’s so easy to misuse. People run at the fingers instead of running at the mouth. They’d write things that they’d never say out loud."

And that can lead to trouble. In the AMA survey, 13 percent of respondents reported having been involved in lawsuits and 8 percent reported that employees e-mail and Internet communications records were subpoenaed in connection with the cases.

The need to monitor employees was also tied to security concerns (both of the company’s computer resources and of their competitive information), legal compliance and productivity measurement or performance review.

The bottom line is that companies are being more vigilant of how their employees use electronic assets. So what should companies do in response to this increased threat? Should they take the road chosen by the New York Times Co.? Does Chemical and the others, or go down a different path?

Thou Shalt Not

The first thing a company concerned about e-mail security and propriety should do, says Flynn, is establish an e-policy. Without it companies have no legal standing to monitor employee use of e-mail, the Internet or other network assets owned by the company.

That’s because the Electronic Communications Privacy Act, passed in 1986, says people—including employees—can expect privacy in their electronic communications unless they’ve been informed otherwise. (Also known as the wiretap act, that’s the technicality that got Linda Tripp in trouble.)

A typical policy, such as the one implemented by Pacific Life & Annuity Co., a financial and insurance services firm based in Newport Beach, Calif., includes the following:

"All company equipment including computer systems, computer software, devices, electronic mail (e-mail), voice mail and other physical items are for business use only. By placing information on the company’s computer systems, the employee grants the company the right to review, edit, delete, copy, reproduce and distribute such information. Employees are encouraged and advised to keep personal records and personal business at home, as the company does not guarantee privacy for information contained on the computer, electronic or telephone systems. The company reserves the right to search any computer, electronic or telephone systems utilized at work. Inappropriate or offensive use of e-mail and the Internet is against company policy. All employees and contractors of Pacific Life and its subsidiaries are required to..."
comply with the company’s policies regarding these matters.”

It’s short, sweet and packs a wallop of implications for those who attain the privileges, as seen in the cases including the companies described above.

“Warning not given to people who send anything inappropriate,” says Karen Wyle, spokeswoman for Pacific Life’s human resource department.

“Our management has always been concerned about inappropriate use of the Internet from a productivity standpoint,” says Alan Brown, vice president of information technology services at Pacific Life. “If there’s some small amount of personal usage, we’re not going to fuss about that. We block those sites where we feel there could be issues.” (See the sidebar for more.)

Moll Flynn, “Employers need to make it clear that their policies that managers are not reading employee e-mail because they’re nosy. In training, they should make it clear to employees that the company is trying to protect its business. They should also state in their policy that they only approve messages going to get involved in monitoring, and a company needs to stick to that. You can’t allow anyone to be in a management position to read e-mail messages.”

According to the AIA survey, 89 percent of employers are establishing policies, but the rub is they aren’t following through on two important requirements: notification and education.

Only 50 percent have employees sign off that they have read and understood the policy. That could hold a company in trouble in court. Without official notification, an employee might have a case for invasion of privacy, according to the ECPA.

Rules of Restraint

Because so many companies are grappling with the issue of e-mail and Internet abuse, technology frequently provides the solution.

At Pacific Life in Newport Beach, Calif., software blocks access to categories of adult and gambling sites.

“We had to implement technology so that if there was suspected abuse, we could do something about it,” says Alan Brown, vice president of information technology for the company.

It’s interesting to note that the company originally blocked entertainment, shopping and travel sites but then cancelled that rule because it found employees were using those sites to buy business supplies or make travel arrangements. “We don’t want to stop employees from doing their jobs,” he says.

With no access to sites that could cause problems, there’s no chance of violation. While software that blocks particular sites is a no-brainer, preventing e-mail abuse requires more sophisticated technology.

James Hulbert Industries, a building materials company based in Mission Viejo, Calif., has turned to such technology to police employee e-mail. Mail Marshal, an enterprise-level e-mail content security and control product, scans incoming mail for viruses or markers that indicate if the message carrier contains inappropriate pornographic material, and it also allows the company to block external transmission of e-mails that contain confidential company information using a search criteria for key words or phrases.

One problem is that employees are being solicited by unsolicited sites, getting hotmail messages and things like that. Folks are calling us and asking if it could be stopped,” says Lee Siminger, Mail Marshal’s vice president of sales.

“Around the holiday season, people can especially be offended by what comes across their e-mail systems,”

Mail Marshal allows the company to control what’s in and isn’t acceptable to receive,” says Siminger. “Our policy is more about distribution of information.”

On the Track

While notification is necessary for legal purposes, training is essential on the practical level. You don’t want to have to fire people who don’t understand the rules on inappropriate e-mail and Internet use.

Unfortunately, 54 percent of the AIA respondents said they had no e-mail policy training programs. Among the minority of companies that do have programs is Moores & Co. based in Whitehouse Station, N.J., which ironically instituted a companywide standards-based e-mail training program in February 2000 just before the filings mentioned above; the two-year implementation period.

“E-mail is a hot topic because it is so easy to misuse. People run at the fingers instead of running at the mouth. They’d write things that they’d never say out loud.”

Yet they are so aware of e-mail that they’ve developed an e-mail policy that includes an e-mail policy.

Attorney Michael Overtly, partner in the e-business and information technology group of Policy & Larner in Los Angeles, agrees, saying the issues raised in the beginning of this article involved mostly low-level employees. “But, when a company’s senior manager or top executive violates an e-mail policy, the employer had better be ready to fire them,” says Overtly, the author of E-Policy: How to Develop Computer, E-Policy, and Internet Guidelines to Protect Your Company and Invaluable Assets.

It’s tricky to have a firm policy and also protect a company’s investment in a valued employee, so some companies have taken more creative approaches than discipline and firing. One company posted on the lunchroom bulletin board lists of offensive sites visited by each department. Another links e-mail and Internet abuses to a loss of bonuses. Another company added bonuses for employees who are effective in their use of Internet/e-mail resources.

“One company has an approach I’m uncomfortable with,” says Overtly. “Managers charge the employee for the time he or she was engaged in a contentious activity. I think that’s a horrible hard,” he says.

Most companies use a warning system, which starts with a conversation with HR, moves to a letter and, for an officer of the company on the second of three and ends in firing on the third of three. The administrative employees were fired in the New York Times case if they forwarded the questionable e-mail. But if they read it and didn’t report it, they were disciplined.

Cases such as that one were a wake-up call for companies like Pacific Life: “Our new policies have to do with any problem,” says Wyle. “It’s like a pre-emptive strike.”

Send questions or comments about this story to breitbart@compuserve.com.