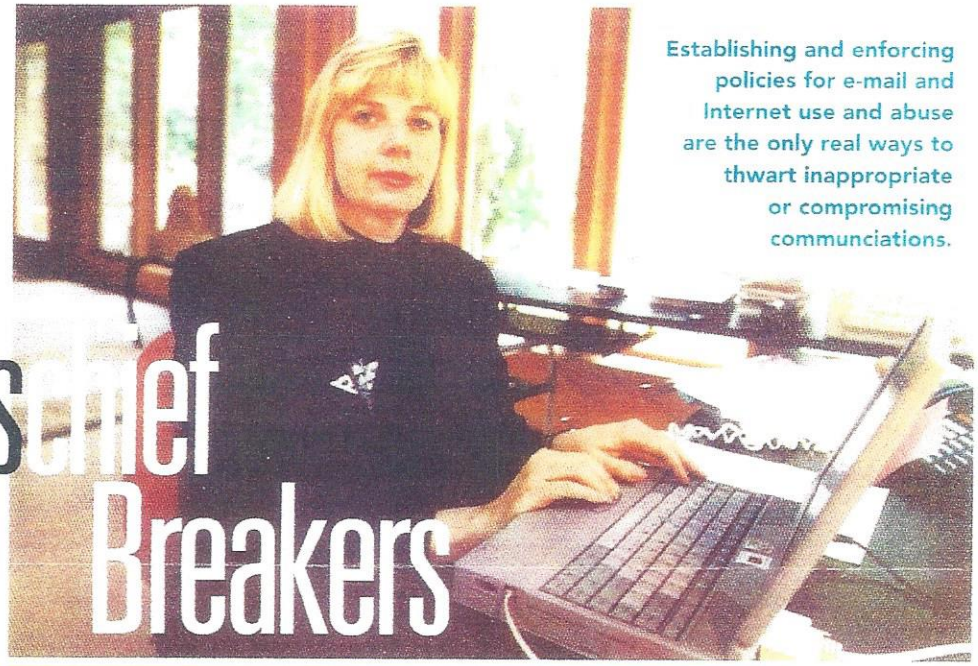
NOVEMBER 2001 • $8.95

Human Resource Executive®

Security



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

Mischief Breakers

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

BY MAURA C. CICCARELLI

Twenty-two New York Times Co. employees in the company's Norfolk, Va., business office are fired for a sending around a series of bawdy e-mails. Two Salomon 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 discipline and potential dismissal for inappropriate e-mail and Internet usage.

HR ears perked 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 ludicrous, the reality is it's not a laughing matter. It's a legal one.

When the American Management Association surveyed 1,627 members earlier this year, it found that nearly 63 percent monitor Internet connections, almost 47 percent store and review e-mail messages, and 36 percent store and review computer files. About 70 percent of those companies cited legal liability as their top reason for e-monitoring employees.

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

"Smoking-gun e-mails are common in workplace-harassment cases," says Flynn. "There's no 'he said/she said' element."

Patricia Eyres, president and founder of Litigation Management and Training Services in Long Beach, Calif., says 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."

And that can lead to trouble. In the AMA survey, 15 percent of members reported having been involved in lawsuits and 8 percent reported that employee e-mail and Internet connections records were subpoenaed in connection with the cases.

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

The bottom line indicated by the survey and the headlines is that companies are being more watchful 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., Dow 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 e-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, diskettes, 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, republish 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 abuse the privileges, as seen in the cases involving the companies described above.

"Warnings are given to people who send around anything inappropriate," says Karen Wylie, 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.)

Adds Flynn: "Employers need to make it clear in their policies that managers are not reading employee e-mail because they're nosy. In training, they should let employees know that the company is trying to protect its business. They should also state in their policy that only approved persons are going to get involved in monitoring, and a company needs to stick to that. You can't allow everybody in a management position to be reading e-mail messages."

According to the AMA survey, 80 percent of employers are establishing policies, but the rub is they aren't following through on two important requirements: notification and education.

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

On The Same 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 impact of inappropriate e-mail and Internet use.

Unfortunately, 64 percent of the AMA respondents said they had no e-policy training programs. Among the minority of companies that do have programs is Merck & Co. based in Whitehouse Station, N.J., which ironically instituted a companywide standards-and-values training program in February 2000 just before the firings mentioned above; the two-year implementation will train the company's 65,000 employees around the world.

"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."

Carole Johnson, director of HR and payroll at BCBG Max Azria, an apparel manufacturer based outside Los Angeles, has had more than her share of experience with e-policy violations by employees.

Currently BCBG is implementing a new e-policy covering e-mail, voice mail, Internet use and company property use. While reviewing e-mails at a previous company—also an apparel manufacturer—Johnson dealt with everything from Whitewater to Miss Piggy.

"In one case, a woman tied up one of our network printers printing out all 476 pages of the Starr Report," says Johnson. "I had to deal with another woman who received an e-mail that she forwarded on to various employees featuring Kermit the Frog and Miss Piggy in a compromising position."

In the Muppets caper, Johnson gathered the employees involved in a conference room and the topic turned to workplace harassment. "I explained that not everyone has a level of comfort [with such material] and that they needed to be careful that they did not offend co-workers. I also said it was a gross misuse of company resources."

In another case, an employee sent the widely disseminated Neiman Marcus chocolate-chip cookie recipe to the entire employee population of another company. "I told her, 'What you did, whether it was intentional or not, had terrible consequences for the company that received it, tying up their network resources unnecessarily,' " she says.

After the employee received the warning that any further violation would result in termination, the inevitable happened: "One month later," says Johnson, "she was downloading and distributing an e-mail—10 things women do better than men—that was inappropriate. We terminated her."

Johnson will be training BCBG supervisors on the e-policy, which is part of a new employee handbook. "It's important to talk to managers about the importance of consistency [in applying the e-policy rules] because otherwise, we have no handbook."

Eyres, whose company trains managers about legal risks, has seen companies combine e-mail training with harassment prevention. "An e-policy is not really a stand-alone policy. In the case of harassment, there can be a telltale e-mail trail," she says. It's all connected.

Pacific Life has classes that address e-policy issues as part of its overall curriculum. "Word Management" concentrates on what you should and shouldn't write in letters and e-mails, which touches on the issues of workplace harassment. "Workplace Issues" helps employees develop sensitivities to a diverse workforce, including the problem with downloading and sharing jokes that may be offensive to some.

Shades of Gray

While there are cases that are clear-cut, some e-policy violations are not easy to identify or weigh.

"Where we see the biggest problem is where it says in the policy that absolutely positively no personal business is allowed," says Eyres. "If you have a good employee who gets a personal e-mail, is it a violation? Yes. Do we discipline [him or her]? Probably not. Then you have another performer who isn't so great, and he or she gets invited to his or her class reunion. Do you then discipline him or her?

"In order to have a fair employee practice, you have to say that no one is above the rules and no one is beneath the rules," she says. "When there are ambiguities, we have to really sit down and think about what is it that we want to say is appropriate and inappropriate. If we have cases in which enforcement is inconsistent then they can say, 'I'm being picked on. It must be my …' fill in the blank: age, sex, disability."

Attorney Michael Overly, partner in the e-business and information technology group of Foley & Lardner in Los Angeles, agrees, saying the cases cited in the beginning of this article involved mostly low-level employees. "But, when a manager, senior manager or top executive violates an e-policy, an employer had better be ready to fire them," says Overly, the author of *E-Policy: How to Develop Computer, E-Policy, and Internet Guidelines to Protect Your Company and its 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, he says. One company posts 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 bonus compensation for groups of employees who are effective in their use of Internet/e-mail resources.

"One company has an approach I'm uncomfortable with," says Overly. "[Managers there] charge the employee for the time [he or she was] engaged in a nonbusiness activity. I think that's unduly harsh," he says.

Most companies use a warning system, which starts with a conversation with HR, moves to a letter from an officer of the company on the second offense and ends in firing on the third offense. 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 little to do with any problem," says Wylie. "It's like a pre-emptive strike."

Send questions or comments about this story to hreletters@lrp.com.

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 that," 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 Hardie 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 content security and control product, scans incoming mail for viruses or markers that indicate if the message is spam or 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.

"Our problem is employees are being solicited by unwelcome sites, getting hotmail messages and things like that. Folks are calling [us] and asking if it could be stopped," says Lee Sininger, HR manager for the company. "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 "is and isn't acceptable to receive," says Sininger. "Our policy is more about distribution of information."