HR Magazine

October 2008

Special Report: HR Technology

Stay Ahead of the technology Use Curve

Start by developing comprehensive workplace technology policies.

By Bill Roberts

It's hard to stay ahead of the curve on creating technology use policies when what you want to govern changes at lightning speed. But keeping a broad, forward-thinking approach to such policies will help protect your company. Organizations need policies that govern employee use because each new technology opens a virtual can of worms full of legal, ethical, security and productivity issues.

"Technology is developing so quickly, and in so many directions, that any policy that goes into specifics about cell phones or e-mail or instant messaging is going to be out-of-date before it is written," says John Greer, senior vice president of human resources at Smart Financial Credit Union in Houston, and vice chairman of the International Association for Human Resources Information Management board. "The policy has to be broad enough to deal with the issue of data privacy and other things without talking about the specific devices."

Anthony J. Oncidi, a partner and chairperson of the labor and employment committee in the Los Angeles office of Proskauer Rose LLP, understands that frustration, but he cautions, "These technologies are not so revolutionary that you can't get a bead on them." Whereas cell phone technology is not going to change radically and texting might become richer in content, these factors should not deter technology-specific policies.

Organizations should address policy on two levels, says Kent Anderson, managing director of Envurve LLC in Portland, Ore., a technology risk and security management consultancy. He encourages companies to develop a general framework that deals with privacy, appropriate use, intellectual property protection and other broad issues, as well as statements detailing practices for each technology. The statements should be reviewed at least once a year, preferably twice, and in some cases quarterly in organizations that are quicker than others to bring on new technologies. Anderson and others say the responsibility for these policies falls to many stakeholders.

Below, Oncidi and Joseph L. Beachboard, a partner in the Los Angeles office and chair of the client services committee at Ogletree, Deakins, Nash, Smoak & Stewart PC, examine some flash points in technology policy, discuss common risks and offer some guidance.

Regulating E-Mail

E-mail continues to be fraught with legal, ethical and productivity issues. One problem: Users think of e-mail the way they think of oral communication—as informal, not as a medium that sticks if the wrong words come out. But written e-mail, stored on hard drives, is not like oral communication: A wrong word or phrase offered inadvertently, mischievously or angrily can have legal repercussions.

An impromptu e-mail exchange between a supervisor and an HR specialist about a problem worker could be used in court to support the employee's claim of retaliation. Unless recorded, the same exchange orally has no afterlife.

The courts are slowly defining the legal risks of e-mail, but gray areas remain. "Given that existing law is largely tailored to more traditional means of communication, employers often confront uncharted legal waters in managing and regulating employee use of e-mail," Beachboard notes.

As much as employees need a clear use policy that the company enforces, they also need training and regular reminders not to write messages they do not want permanently recorded and to edit e-mails for tone before sending them. Diversity training should include an e-mail component emphasizing the need for racial, gender and other sensitivities in electronic communications.

Instant messaging (IM) is on a trajectory to replace e-mail as the main form of electronic communication. The problems are similar to e-mail, only more so because IM's real-time, instantaneous nature makes such messages seem less formal than e-mail. "Psychologically, employees think IMs are less traceable, and therefore they become more free-form," says Oncidi.

IM and its first cousin, cell phone texting, pose myriad problems: security of transmissions, reduced productivity and potential liability for offensive messages. The problems increase with the speed of transmission and the fact that many workers install the necessary software on their computers without the employer's knowledge—all issues a policy must address.

Blog Rules

Blogging can be a useful tool for knowledge sharing among workers, partners and customers. But employers can be at risk when employees blog outside the enterprise. There are hundreds of blogs about individual companies, with workers, former workers and others weighing in on all kinds of topics—including some that may breach proprietary, confidentiality and privacy rules.

Despite the obvious risks, "I'm not sure that many employers understand the need for a blogging policy," says Oncidi.

As for wikis, a first cousin of the blog, most HR professionals don't even know how many exist in their enterprises. Motorola, for example, conducted an audit recently and found more than 3,000 wikis on its intranet. Wikis carry many of the same potential problems as blogs and require similar policy attention.

What and How Employers Monitor

In a 2007 survey of 304 employers:

- 65 percent use software to block connections to inappropriate web sites, up from 27 percent in 2001.
- 96 percent block access to adult sites, 61 percent to game sites, 50 percent to social networking sites, 40 percent to entertainment sites, 27 percent to shopping and auction sites, and 21 percent to sports sites.
- 18 percent use URL blocks to stop employees from visiting external blogs.
- 45 percent track content, keystrokes and time spent at the keyboard.
- 43 percent store and review computer files.
- 12 percent monitor the blogosphere to see what is being written about the company; 10 percent monitor social networking sites.
- 43 percent monitor e-mail; 73 percent of them use technology tools to automatically monitor e-mail, and 40 percent assign an individual to manually review e-mail.

Source: 2007 Electronic Monitoring & Surveillance Survey, co-sponsored by the American Management Association and The ePolicy Institute.

Twittering is another phenomenon employers may need to address. The micro-blogging free service allows users to text updates called tweets to their friends who sign up to follow their feeds on computers, cell phones and personal digital assistants (PDAs). As with other new forms of electronic communication, managers must determine the possible risk from twittering. For example, employees

may twitter about what product they are working on at the office, how HR is treating them during a layoff or if the boss is giving them a hard time. These real-time updates can show raw, unfiltered emotion that could be detrimental to the employer. So far, there has been little or no guidance from the courts about twittering.

Policing Social Networking

Facebook, LinkedIn and other social networking sites pose two types of risks. First, workers on social networking sites might disclose confidential, proprietary or private data to the detriment or legal risk of the employer. **Oncidi suggests that a use policy "at least acknowledges the existence of social networking sites and tells the employees that if they use them, they are still bound to confidentiality and proprietary information requirements."**

Employers cannot bar employees from using Facebook when they aren't at work, but according to Oncidi and Beachboard, they can demand that workers not identify themselves as employees of a particular company or issue disclaimers that they are not speaking for the company.

Appropriate use policies can be written to cover all of the above: e-mail, blogging, wikis, social networks and Internet use in general, including sites inappropriate to access from the workplace. Employers are more on top of the inappropriate web sites, with about two-thirds saying they use software to block certain web sites, according to the *2007 Electronic Monitoring & Surveillance Survey*, co-sponsored by the American Management Association in New York and The ePolicy Institute in Columbus, Ohio.

The second risk that arises from social networking sites can also be an issue with blogs and web sites: Privacy questions surface when employers search social networking and other web sites for information about current employees or candidates. (For more on collecting information on employees, see "How Deep Can You Probe?" in the October 2007 issue of *HR Magazine*.)

Locking Down Data

Despite headlines underscoring the problem of data theft, many policies don't address the issue. "There is still a lot of room for education," says Oncidi.

Most organizations have made progress in protecting networks and data in desktop computers and servers in the office, but they haven't done as much to secure data on laptops and other mobile devices. If employees take data home, then employers must consider encryption of the file or hard drive.

Oncidi warns of carrying laptops across international borders. Customs and immigration officials have a right to inspect and confiscate laptops, presumably when concerned about terrorism or other illegal activities. A policy could require employees to back up data elsewhere before they cross borders and, if proprietary information was collected during travel, to send it home before passing through customs.

Mobile Security

Employers that focus their data protection policies only on laptops are ignoring the next variations of the problem.The media don't report much about loss of confidential data from cell phones, PDAs, iPods or USB drives, but it is only a matter of time. These devices are also used for texting and e-mail, so policies should reference them.

Before an employer gives PDAs to workers, it should "think about how this impacts wage and hour rules," warns Oncidi. "If the employee has consistently left the office at 5 p.m. and now has to take e-mails from his boss at all hours, then how do you compensate him?"

In addition, attorneys representing persons injured by drivers using cell phones for business-related calls have begun to sue the drivers' employers, frequently winning sizable settlements. The plaintiffs claim the employer is vicariously liable because the employee talking on the cell phone was acting within the scope of his employment. They also frequently claim the employer is directly liable for encouraging or condoning cell phone use while driving without appropriate safeguards. Many states now have hands-free cell phone laws.

Beachboard says at least one law firm is marketing itself as the expert in these suits. He advises, "If you do not have a comprehensive policy in place addressing cell phone use while driving, it is highly recommended that you draft and implement one."

Consistency Counts

The biggest risk is any disconnect between policy and practice. "Writing a policy and putting it in a desk does nobody any good," says Anderson, adding that the connection between policy and practice protects you in court.

The courts appear willing to give employers great latitude in monitoring, regulating and dictating how, when and where workers can use these tools—if an employer can prove to the court that it applies and enforces its policies consistently. "HR people have to get over the fear of technology and start appreciating its capabilities," Greer urges. "We have to know how people use technology and address those issues."

The author is contributing editor for technology at HR Magazine.