Learn boundaries for employee surveillance

Jacksonville Business Journal - by Mark Szakonyi Staff Writer

In these lean times, employers want to make sure their employees are working hard, aren't opening them up to lawsuits and — most of all — aren't leaking sensitive information.

The challenge is how companies can monitor their employees' e-mail, text messages and phone calls without running afoul of the law. More than a quarter of employers have fired workers for misusing e-mail and about a third have fired workers for misusing the Internet, according to a 2007 **American Management Association** report.

"The most important thing is to have a written policy disclosing what your surveillance practices are," said Chanley Howell, a partner in **Foley & Lardner LLP**'s intellectual property department in Jacksonville.

When it comes to e-mail, employers have the right to monitor any communication done on their computers. If data is handled on the company's server, then it is legally under the purview of the employer. Nonwork e-mail systems and social networking site communication isn't, however.

That's why it is important to have employees sign an agreement either forbidding the use of such e-mail systems or sites or giving permission to their employers to monitor them. The monitoring of keystrokes through software enters a grey legal area, Howell said, so it's good to have language pertaining to that type of surveillance in the agreement signed by employees.

"I recommend blocking Facebook and other social networks," said Bob McKenzie, president of **McKenzieHR**.

Companies that he has advised have dealt with everything from circulation of obscene e-mail to chain-letter e-mail. Their presence in the office opens the employer to sexual and racial harassment lawsuits, besides wasting workers' time.

Despite the publicity surrounding such e-mail, it continues. A California mayor recently resigned after admitting to sending an e-mail depicting a watermelon patch at the White House.

Employers can have their information technology workers monitor employees' e-mail and Internet usage. Smaller companies can opt to buy monitoring software that generally ranges from $30 to $100. Well-rated software includes Spector Pro, SpyAgent and Net Spy Pro.

Employers' rights regarding surveillance begin to get murkier when it comes to monitoring employees' text messages. If the text messages are used on company-provided phones or service, then employers generally have a right to monitor them, Howell said. But this is where having a secure usage agreement is essential.

A lack of a clear one is what thrust an incident of a California policeman's sex-themed text messages to his girlfriend and wife to the **U.S. Supreme Court**. The policeman was told by his department that any additional texts over a set limit would be paid for out of his pocket.

But when the department looked at the content of his text messages, he argued that it violated his Fourth Amendment right to be free from unreasonable search and seizure, according to a Security Management magazine story.

“You can allow them to make personal texts on their phones during breaks and when it’s a necessity, “ McKenzie said.

It is illegal for employers to tap workers’ phone calls, but they can monitor how much time employees spend on calls and whom they’re talking with, Howell said.

McKenzie said monitoring doesn’t always pay off when the worker is still employed. If an employee leaves abruptly and is suspected of taking business contacts and other information, it’s worth checking their communication activities before they left.

In the interest of protecting company information, McKenzie suggests creating a policy regarding USB drives connected to personal computers. Not only can they be used to transport data outside the office, they also can introduce viruses into a company server.

Often images of Big Brother are brought up when companies discuss surveillance with their employees. McKenzie recommends taking this approach with workers:

“We are looking to protect our assets, and people are part of that. If trade information gets out, we could all lose our jobs.”

mszakonyi@bizjournals.com | 265-2239