Employers beware: Layoffs may result in theft of information

A recent survey for Symantec Corp., an Internet-security firm, suggests that 60 percent of all employees who left their employers last year took some data with them.

INTELLECTUAL PROPERTY

ERICA HARRIS

Given the number of layoffs triggered by the economy, this statistic could have tremendous meaning for a vast majority of employers.

As information becomes increasingly electronic, it becomes increasingly portable, making misappropriation easier to accomplish and harder to detect. The "secret sauce" for many companies is no longer secured in a company's safe, but rather resides on a company's server. Data can be downloaded to pocket USB drives and can be uploaded to portables accessible via the Internet. Customer contacts can be found in employee cellphones and blackberries, and key pricing information is shared with salesmen who travel frequently and thus carry the information with them on their laptops.

Compounding problems of accessibility and vulnerability are changing societal perceptions about the way electronic information is viewed, used and shared. Younger generations are accustomed to doing research on the Internet and using what they find there for their own benefit. Copy and paste functions are used freely to incorporate information found on the Web into their own work.

As a result, younger generations are more apt to view information as something that is free and legally "customized" by the user. Contacts in a blackberry are taken and used without any thought to whether the customer lists from which the information originated are proprietary to their employers.

As the economy contracts, more employees will have the incentive to take their employer's information. Those employees who want to start their own competing businesses will want the head-start, and employees who want to work within the same industry see their employer's contacts as something they can parlay into a new job often with a direct competitor.

Employers are wise to protect their proprietary trade secrets and competitive information in any environment but should be particularly sensitive to these issues in today's market. Employers need to escort employees from their offices as soon as they are notified of their termination. Log-on information, passwords and access cards need to be deactivated immediately after an employee is terminated.

Because employees often learn of their terminations through informal channels or seek to transfer information in advance of layoffs, employers should consider what advance measures can prevent or at least help detect the misappropriation of information. Software can track downloads and place restrictions on what data blocks can be transferred.

Because employees often learn of their terminations through informal channels or seek to transfer information in advance of layoffs, employers should consider what advance measures can prevent or at least help detect the misappropriation of information.

Similarly, employers should make sure their employment contract includes obligations to protect confidential information and remedies for the failure to do so. Because the damages arising from a misappropriation of proprietary information are often hard to measure, employers should address when injunctive relief would be appropriate. Where proving misappropriation would be extremely difficult, noncompete provisions may be necessary.

The current economic market is making every aspect of running a business more difficult. Employee theft of intellectual property and other confidential information is simply one more growing challenge for Houston employers. ■

ERICA HARRIS is partner at Susman Godfrey LLP, a commercial litigation firm.