Do You Know Where Your Company's Sensitive Information Is?

Publication
4.29.09

According to a recent survey, information you believe is confidential may also be in your competitor's offices. A report from the Ponemon Institute details that companies are doing a poor job preventing former employees from stealing data. Some details from the report should give every employer cause for concern, particularly in this time of sharp staff reductions.

Approximately 945 former employees were contacted for the survey, and the answers should trouble any employer who has lost employees in the last year: 59 percent of those who were terminated or who voluntarily left employment stole sensitive and confidential company data; the most frequent reason for taking the information (67 percent) was "to leverage a new job"; 69 percent of respondents reported finding a new job, and of those, 2 out of 3 use the information in their new job; and of those who admitted to taking data, 61 percent of employees reported having an unfavorable view of their previous employer, versus 26 percent with a favorable view of the previous employer. The actual information taken included e-mail lists (65 percent), non-financial business information (45 percent) and customer information, including business contact lists (39 percent). The method of capture was reported to be CDs or DVDs (53 percent), data transferred to a USB memory stick (42 percent), attaching documents to an e-mail sent to a personal e-mail account (38 percent).

The report describes the problem, but what's an employer to do? From a legal perspective, there are two essential sources of protection of trade secrets/confidential information: the Uniform Trade Secrets Act (UTSA) and common-law principles used in various states. The rules are not uniform and each state's statutes should be consulted for details, but the UTSA defines a trade secret as information that 1) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use, and 2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Unless you have paid attention to both parts of the equation, a court isn't going to be of much help in limiting the use of important information carried to your competitor by a former employee. There are steps for instituting a credible information protection strategy. These steps won't guarantee that you will never lose important confidential information to departing employees, but consideration of the problem and implementation of controls will certainly make it much harder for a departing employee to do what so many other departing employees are doing in this struggling economy.

This article appeared in the April 29, 2009 issue of *The San Diego Daily Transcript*.

This article appeared in the April 27, 2007 issue of *The San Diego Daily Transcript*.

Related People

Christopher C. Hoffman
Regional Managing Partner
858.597.9610
Email