Beware: Sensitive Data is a Frequent Target

Publication
7.03.09

Where is your company's sensitive information at this very moment? You may say that it is in the company's files locked in someone's office or in a certain directory on the company's server. I hope you're right. But according to a recent survey, information you believe is confidential may also be in a number of other places, including your competitors' offices. A Ponemon Institute report suggests that employers may be losing much more sensitive and confidential information than they imagine. The report describes the problem, but what can an employer do? As an initial matter, you should identify for yourself what information is most essential to the way you do business. Or, in other words, "What information would I most not want my competitors to know about?"

From a legal perspective there are two essential sources of protection of trade secrets and confidential information: the Uniform Trade Secrets Act and common-law principles of theft and breaches of loyalty. Since the law is generally designed to help those who help themselves, what should an employer do to help itself in this area? Here are a number of areas recommended to start from to institute a credible information protection strategy:

- Consider requiring employees to sign confidentiality agreements, non-solicitation agreements, covenants not to compete and assignment-of-invention agreements.
- Implement appropriate security policies that address use of computers, e-mail, voice mail and the Internet.
- Train company employees in the policy and proper handling of company confidential information, and their security responsibilities.
- Secure the physical environment, which includes steps such as restricting access to servers, routers and other network technology, to those whose job responsibilities require access.
- Secure the company's computer systems and network by limiting access to sensitive information to only those who have a need to know or use the information.
- Protect company information upon an employee's termination by disabling all accounts and access privileges of the terminated employee and changing all access codes and VPN (virtual private network) and dial-in numbers.

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 July 3, 2009 issue of the *Daily Journal of Commerce.*

Related People

Richard R. Meneghello
Chief Content Officer
503.205.8044
Email