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

Insights
4.01.09

(Labor Letter, April 2009)

A recent report suggests employers may be losing much more sensitive and confidential information than they imagine.[1] The report's conclusion – "Companies are doing a very poor job at preventing former employees from stealing data. . ." seems amply confirmed by the results of its survey.

Some details from the report should give every employer cause for concern, particularly in this time of sharply increased staff reductions. Approximately 945 former employees were contacted during the survey and the answers should trouble any employer who has lost employees in the last year.

Of the employees surveyed:

- 59% of those who were terminated or who voluntarily left employment, stole sensitive and confidential company data;
- of those who took data, 79% said that they were aware that company policies did not permit them to take the data but they took it anyway;
- the most frequent reason for taking the information (67%) was "to leverage a new job";
- 69% of respondents reported finding a new job, and of those, 67% use the information in their new job; and
- employees' views of their former employer influenced the frequency with which they took data. Of those who admitted to taking data, 61% of employees reported having an unfavorable view of their previous employer, versus 26% of those with a favorable view of the previous employer.

The actual information taken was email lists (65%), non-financial business information (45%), and customer information, including business contact lists (39%). The method of capture was reported to be CDs or DVDs (53%), data transferred to a USB memory stick (42%), attaching documents to an e-mail sent to a personal e-mail account (38%).

Show Them You Care
The report describes the problem, but what is an employer to do?

As an initial matter, you should identify for yourself what information is most essential to the way you do business. Stated another way, "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/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.

As you can see, the formula has two parts, information which has actual or potential economic value because it is not generally known and information which the employer has taken steps to protect. 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.

Since the law is generally designed to help those who help themselves, what should an employer do to help itself in this area? Listed below are a number of areas we recommend as a starting point for instituting a credible information protection strategy:

1. Have employees sign confidentiality agreements, non-solicitation agreements, covenants not to compete and assignment-of-invention agreements which are lawful in your particular jurisdiction.
2. Implement appropriate security policies which address use of computers, email, voice mail and the internet; which define physical and electronic access to trade secrets; which cover telecommuting and employee privacy concerns; and which control vendors and third-party access to confidential information.
3. Train company employees in the policy and proper handling of company confidential information, and their security responsibilities.
4. 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; keeping an equipment inventory; locking file cabinets and offices that store sensitive information; labeling all documents containing trade secret or confidential information as "Confidential"; cross shredding all paper documents containing sensitive information; and making sure that all magnetic media data is erased before discarding
5. 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, and keep audit logs of all access requests to critical systems and sensitive information.
6. 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 possibly VPN

access privileges of the terminated employee and changing all access codes and possibly VPN (virtual private network) and dial-in numbers; examine the employee's computer or laptop to determine if the employee has accessed or copied sensitive information in recent months; conduct an exit interview during which you remind the employee of continuing obligations not to improperly use company confidential information and get the departing employee's agreement not to do so. Ask the employee if he or she has any company confidential information.

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.

Implementing controls will help ensure that your departing employees are the 41% of individuals who do NOT take confidential information with them. Also remember that state laws concerning protection of trade secrets or confidential information, non-compete and non-solicitation covenants, etc. are not uniform – one size definitely does not fit all in this situation.

Of course, your Fisher Phillips attorney will be glad to provide further information appropriate to your jurisdiction.

---

[1] *Data Loss Risks During Downsizing: As Employees Exit, So Does Corporate Data*, released by the Ponemon Institute.