CFO

Inside Baseball and Out, Companies Need to Protect Trade Secrets

High-level and high-profile executive moves – such as baseball general manager Theo Epstein's switch from the Red Sox to the Cubs – should inspire companies to revisit their employment agreements.

by Debra Squires-Lee – October 27, 2011

Every member of Red Sox Nation is wondering how Theo Epstein's move from Boston to Chicago will impact next baseball season. To what extent will the former Sox general manager apply what was at one point a winning strategy to his new job as president of baseball operations for the Cubs?

If they did their job right, the senior executives in the Boston club curbed Epstein's ability to tap into its secrets to create a successful 2012 team in the Windy City. If Epstein was privy to any proprietary, secret, statistical method for analyzing baseball talent, that method could be considered a trade secret. If he uses that method to benefit the Cubbies, the Sox could try to fight its wrongful use, but that would be costly. The expense of litigating a trade secret case can be game changing. The cost of the lost business advantage if the Cubs start using Sox' secrets may be season ending.

A high-profile employment change, such as Epstein's, serves to remind companies of the importance of protecting trade secrets. Protection of these assets before senior talent leaves a company is key. It is always easier to prevent a catastrophe than to clean one up. This article addresses steps CFOs can take to ensure that trade secrets are identified and protected within their companies' relationships, and with current and former employees, as well as suppliers. These steps are well worth the investment when weighed against the costs of disclosure or litigation.

Identify your trade secrets. Massachusetts defines a trade secret as "any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it." The Uniform Trade Secret Act (adopted in 45 states but not Massachusetts) defines a trade secret similarly, and requires the information be subject to "reasonable" efforts to "maintain its secrecy." In other words, a trade secret must be secret. Information that is generally known, easily replicated, or widely disseminated is not a trade secret. Once your company has zeroed in on its trade secrets, they should be cataloged, with specificity.

Implement safeguards. These protections should include: limiting employees with access to certain information; requiring employees to sign in and out of restricted areas; and stamping documents and data as "highly confidential" or "trade secret." Failure to take these steps may lead employees, a business affiliate, or even a court to conclude the company did not try to keep the information, in fact, secret.

Be careful of sharing data. Specifically identifying your company's key trade secrets allows companies to put their talent and business affiliates contractually on notice that the pertinent information is considered a highly competitive trade secret. The matter can get difficult when outside parties are involved.

For example, consider the work involved in reaching an agreement with an OEM vendor. The product requires collaboration between the customer and supplier and may include the sharing of trade secrets, such as during the testing and analysis of prototypes, exchanges between scientists, and the disclosure of specific methods of production that may impact the customer's requirements. Trade secrets that are "shared" in these scenarios risk losing their "secret" status. The best mechanism to protect those shared secrets is a confidentiality clause that clearly identifies what trade secrets may be disclosed and what the customer can and cannot do with them. Clarity is key, and specificity can avoid a fight down the road about whether the information was or was not shared, and whether the information was, in fact, a trade secret.

The same is true when discussing a merger or acquisition with a potential suitor or target. While any well-drafted non-disclosure agreement (NDA) should include a catch-all provision to prevent the use or disclosure of any confidential, non-public information that may be shared during negotiations, companies may want to spell out any trade secrets in the documents as well. The NDA could specify that certain trade-secret processes, machine set-ups, designs, or statistical methods might be disclosed and that the NDA prohibits any use or disclosure of that information.

The same strategy applies to formalities companies use with employees. Companies could identify specific trade secrets that executives may be privy to in employment agreements. For example, if the Red Sox indeed use a secret Moneyball method, then its contract with Epstein should have carved out precisely what method of statistical analysis the team claims as a trade secret. It should have also detailed that Epstein could not take, use, disclose, or rely on that method of analysis for another team.

Debra Squires-Lee is a partner in the litigation department of Sherin and Lodgen LLP. She is a native Bostonian, and thus a certified member of Red Sox Nation. She is also an experienced trial lawyer who represents businesses in complex commercial litigation with significant experience defending companies against claims of trade secret misappropriation.