Financial Times Columnist Gets It Wrong: Trade Secrets Are Worth Protecting

Insights
11.02.10

Just in time for Halloween, *The Financial Times* columnist Lucy Kellaway ran a column entitled, "The Thief, His Victim and the Company Laptop," in which Ms. Kellaway shared her thoughts about the folly of trying to protect trade secrets residing on a company's computers. Ms. Kellaway's article focused on a recent failed attempt to steal a Bank of America Merrill Lynch employee's company-issued laptop. From her perspective, Ms. Kellaway felt the failed theft presented a timely reminder of "the sinister side of corporate life, the futility of all office security measures, and the fact that there are very few corporate secrets worth making such a song and dance about anyway." Why? "There is no magic ingredient to success that can be found on a nicked laptop," Ms. Kellaway wrote. "Success is a complicated formula and cannot be easily stolen."

On these points, Ms. Kellaway is mistaken. As the use of computers in the workplace has spread, so too has digitization of corporate trade secrets. And computers and digitization are tools of efficiency – that are sometimes turned against the companies that use them. Years ago, employees masterminded the removal of boxes of documents out of a corporate office in the wee hours of the morning when it was dark and the theft might go unseen. Such machinations and physical efforts are no longer necessary. An employee can use a flash drive or e-mail to transfer thousands of times the number of documents that the employee could fit into the boxes used years ago. Contrary to Ms. Kellaway's view, trade secrets, formulae and other proprietary information can be very easily stolen. In many instances, it's literally thousands of pages in one keystroke.

More haunting than the ease with which trade secrets can be stolen is how much damage can be done by one employee's inside job. Some of the best examples are the high profile cases of computer programmers who wrote the computer code for high-frequency trading systems for Wall Street firms. In one recent case involving Goldman Sachs, one of its former programmers allegedly copied hundreds of thousands of lines of source code for Goldman's high-frequency trading system, transferred them to an outside server in Germany, then met with a new employer, which would hire him to oversee a competing trading system. When he went to work for the new employer, he allegedly brought Goldman source code with him. The code made possible the software that allowed investment companies to initiate trade orders based on information that is received electronically, before human traders are capable of processing the information they observe. The programmer is now facing criminal charges for his alleged theft of this code. Contrary to Ms. Kellaway's view, this is a secret worth keeping.

Businesses like Goldman protect trade secrets like this code because these assets have economic value. While Ms. Kellaway acknowledges the possibility that a trade secret can generate revenue in the case of client account information, she has underestimated the wide range of trade secrets that are income-generators for businesses. Every day across the country, litigants struggle to protect trade secrets ranging from computer code embedded in Microsoft Excel spreadsheets, to industrial production line schematics, to client lists laced with sensitive client information, just to name a few.

The most savvy companies know the productivity and revenue value of these assets so well that they know how much money to invest in security, pre-litigation and litigation efforts to enforce and protect their rights to these assets. Rest assured that if these assets had no value, then companies would not waste the time, human resources and budget in the litigation to protect them. And if companies took Ms. Kellaway's parting advice – "[t]he way to protect your secrets is to conduct your business in a perfectly reasonable way so that they can be of no conceivable interest to anyone" – there would be no trade secrets left to protect.

Brent Cossrow is an attorney in the Fisher Phillips Employee Defection & Trade Secrets Practice Group. Mr. Cossrow's practice focuses on e-discovery and other electronically stored information issues. As always, please feel free to share your thoughts and questions in the comment space below.

Related People

Brent A. Cossrow
Partner
610.230.2135
Email