How In-House Counsel Handle Rogue Employees

Jennifer Williams-Alvarez , Corporate Counsel

October 18, 2017

When an employee leaves a company, he or she may inadvertently or maliciously walk out the door with valuable intellectual property. Files may accidentally end up on a personal device or a disgruntled employee may **transfer trade secrets** to a thumb drive to later use at a competitor.

No matter the intention, the reality is that the biggest threats to a company often come from inside. And while it's all but impossible to completely eliminate this risk, there are a number of ways in-house counsel can limit the damage.

It starts with, to the extent possible, locking down the data when the situation warrants it, Jody Riger, senior corporate counsel for employment, labor and ethics at Sun Chemical Corp., said on a panel Tuesday at the **Association of Corporate Counsel's annual meeting**.

If an employee who's had access to a lot of information gives notice and won't say where they are going, but there's suspicion it might be to a competitor, there are essentially two options, she said: "We'll either accept the notice … and cut off all access to our network," within a day, depending on the employee. Or, "There are some employees that, you know what, good employee, good relationship, maybe going to a supplier or customer, [and] you want to maintain a good relationship, so we'll let the employee work out their notice period."

With respect to trade secrets, specifically, Riger said these are kept "under lock and key" by not only requiring that certain employees sign a general confidentiality agreement when hired, but for one current project, they also sign an internal confidentiality agreement. Those involved can only speak to one another about this project as a means to provide "extra protection," she said.

Quickly taking away all access provided by employee identification cards is a "first line of defense," said panelist Courtney Manzel, managing privacy counsel at Sprint Corp. Also helpful is to remind employees of their obligations, both when they join and leave the company, she noted. "When somebody is hired, they are apprised of their confidentiality obligations with respect to data … and then when they leave, if necessary, there would be a letter reminding them of those obligations that copies their new employer."

If there's a major concern that a particular person has a lot of sensitive information, Manzel said there's always an opportunity to rely on forensic tests on computers and other devices.

And then, of course, "education is key," said Ari Sherwin, corporate intellectual property counsel at The Sherwin-Williams Co., not just to prevent losses, but also because it can be helpful to point to in litigation. Sherwin noted a **2016 case that came** down in favor of an employer that took reasonable measures to secure trade secrets "because they provided training to their employee—not just inboarding, but once a year—and they also had password-protected computers that could only be accessed by people working on specific projects that relate to the work. And finally, they had their employees sign confidentiality agreements."

Sherwin added: "If you take those measures and you mimic the case law, it can help you."

Jennifer Williams-Alvarez is based in New York and covers corporate law departments.
