As featured in Seattle Business

LANE POWELL

Don't Be the Next Headline

Protect your company's trade secrets!

WITH UNCERTAINTY SURROUNDING PATENT LAW in the middle of this tech boom, it's no surprise that legal headlines continue to highlight jury verdicts and court orders awarding millions of dollars for trade secret theft. When valuable company assets include business plans, source code, algorithms, customer lists, formulas and marketing and pricing strategies, developers must look beyond run-of-the-mill, old-school "widget" protection. Cue trade secret law, a quickly growing body of national and state law that protects any secret that derives independent economic value from not being generally known.

The perils of trade secret disclosure and theft warrant immediate attention. Trade secret laws impose steep damages for misuse, not only for losses but potentially for attorneys' fees as well. And for willful and malicious misappropriation, courts can award "exemplary" damages in an amount up to double the underlying damages award. However, the biggest consequence can mean game over — an injunction can prohibit a business from use of materials belonging to a prior trade secret owner. In the reverse scenario, if a company allows trade secret disclosure, the trade secret asset may be lost for good. As an example, it would be hard to imagine a more devastating loss for a startup software company than its source code becoming public.

And don't let the door hit you on the way out, either. Companies failing to shut off access once an employee announces a resignation risk complete trade secret loss.

Despite these serious consequences, trade secret protection does not attach automatically. As the range of "protectables" widens, so does the need for strong yet specific legal protection mechanisms. Agreements are the starting point, including certain noncompete provisions in employee agreements, nondisclosure agreements with outside vendors and partners, and new language mandated by the May 2016 Defend Trade Secrets Act, which protects trade secrets on a federal level.

Aside from agreements, companies often risk trade secret disclosure by failing to protect their developments on a practical level: via their information security measures, physical access to documents and company methods, and reminders to employees in the form of reviews and documented conversations. With so many employees traveling and working remotely, companies must also consider limitations on remote access so that trade secrets don't slip through the cracks.

And don't let the door hit you on the way out, either. Companies failing to shut off access once an employee announces a resignation risk complete trade secret loss. The keys to avoiding this pitfall include proper exit interviews and immediate review by an IT security team to turn off all future access and preserve all documents accessed in the few days before the transition.

So take stock. Review and audit your potential trade secrets to understand what kind of inventory you are dealing with. Get your agreements up to par, redoing outdated nondisclosure agreements and employment agreements to include more recent required language. Evaluate your current protection mechanisms from an outsider's view:

- How easy would it be to access your pricing agreements?
- What are your server protections?
- Do all employees need access to customer lists?
- Could any visitor see your new process in action?
- Do you have document and data protection policies?

Trade secret protection is technical yet intuitive; if any of the protection suggestions make you nervous, you probably need to seek more robust protection.

TIFFANY SCOTT CONNORS is a shareholder at Lane Powell and works with companies to secure and protect their IP assets from the get-go, counseling clients in IP protection and defending their rights through trial. Reach her at connorst@lanepowell.com or 206.223.7267.