PROTECTING CONFIDENTIAL INFORMATION WHEN SHELTERING IN PLACE

As employers adjust their policies to maintain business operations and enable workers to work from home, they should also take steps to mitigate the risks of trade secret misappropriation.

By David A. Prange and Christopher K. Larus | April 07, 2020

The COVID-19 pandemic has caused many state and local governments to issue orders directing workers to shelter in place and direct businesses to allow workers to work from home. Even when not ordered to do so, companies throughout the United States have quickly adapted to allow their employees to work at home. These accommodations often include allowing employees remote access to a broad range of company information. They also may put company trade secrets and other highly confidential information at risk. As employers adjust their policies to maintain business operations and enable workers to work from home, they should also take steps to mitigate the risks of trade secret misappropriation.

Federal and state trade secret statutes, and state common law, almost universally require that a trade secret owner take reasonable measures under the circumstances to protect a trade secret. Another quality of a trade secret is that the information is not generally known or easily discoverable through proper means by the public. Read together, courts have interpreted these statutes to require a company to exercise continued diligence in applying protective measures to keep information as a trade secret. Similarly, contractual provisions protecting company confidential information many times extend only to information that otherwise does not become publicly available. Again, to protect confidential information, and like a trade secret, the owner of the information should take continuing steps to keep the information confidential.

Increasing Risks. Shifting a company's workforce to operate almost entirely with remote access may increase risks to the company's confidential information and trade secrets. For example, in many cases companies implement security procedures for information access based on information or employee location. Implementing a wholly remote workplace may make such restrictions on information access impractical to maintaining employee productivity, which potentially leads to unanticipated or ad hoc relaxation of location-based security procedures (for example, allowing information access through a remote access point). Allowing greater access can increase the risk of unauthorized access to sensitive company information, even from unintended activities of household members. A lapse in protection, for example, temporary changes to policies to facilitate information sharing, can result in placing such information at greater risk of misappropriation; it may also mean in a later dispute that the information is not considered a trade secret (or confidential information).

In addition, increased remote accessibility to company information presents greater cybersecurity risks. In many instances, the wireless routers, computer hardware and modems employed in homes are less secure than the hardware used to implement corporate networks. Home networking software may lack current security patches or bug fixes utilized in on-premises systems, potentially providing a security hole in the home network that may be exploited. In other instances, the potential presence of corporate information on a computer connected to the network can be at risk through phishing activity targeting other members of an employee's household. Clicking on a phishing email even by a different household member can lead to the unintended consequence of providing broad access to the family network on which the employee is connected.

Risk Mitigation. Companies can mitigate these risks as they accommodate broader remote employee activity. Companies should consider approaching the issue with a documented plan providing some detail on changes to how company trade secrets and confidential information may be accessed during a period of extended remote activity by company

employees. Companies should consider identifying changes to the types of information that may be accessed remotely or the protocols for accessing that information. Many times companies are making these decisions rapidly in response to changing government directives and public health information. While this may make a proactive written plan unfeasible, companies should still consider generating a contemporaneous document detailing the implemented plan and changes, whether temporary or permanent, so there is record of the decisions made. From a litigation context, when the protectability of information as a trade secret may be challenged and memories have faded, this documentation may be used to demonstrate the protective measures that have been taken and adapted over time. A defendant may argue that the deviations from the initial plan were unreasonable and meant that the information was not protected with reasonable measures. But having contemporaneous documentation of the plan and decisions may be used by the trade secret owner to rebut that argument and create a story that the shift in protection policies was a measured and reasonable response to the events at hand.

Companies should consider implementing additional employee training to address cybersecurity risks. Such training may include directing employees to refresh home networking hardware with newly available firmware updates, as well as reset networking and administrative passwords to make networks more secure and passwords more difficult to guess. Companies should also consider implementing minimum hardware standard requirements for home network systems that will interface with company systems. Employees could also be refreshed on best practices for cybersecurity and data safety steps and the risks of phishing. Training may also focus on improving employee awareness of how company information is being transmitted, particularly when communicating with other business partners. Employees should continue to rely on company-based communications systems instead of other private email services. In communications with other companies, employees should likewise be sensitive to the addresses to which they are sending sensitive company information.

At some point, people will return to the workplace. Despite best intentions through proactive corporate policies and conscientious employees, there still may be instances of corporate confidential or trade secret information being saved to off-site locations. Employers should consider developing a reentry plan for its employees. This plan could include having employees search personal machines upon the return to work and deleting company information that may be found. Employers should further remind employees to return physical trade secret information that employees may have used while working from home. The company should also consider documenting these activities with sign certifications from each employee that these activities have been completed. The certification acts as a record for the company to use to track compliance.

Trying to be reasonable. The overall goal for an owner of trade secrets or other confidential information is to protect the information using measures that later may be deemed reasonable under the circumstances. If at a later date the information is the subject of dispute, a fact finder may consider whether any changes implemented for protecting company confidential and trade secret information were still reasonable. If they were not, the lack of reasonable efforts to maintain the confidentiality of trade secrets could lead to a loss of protection. On one hand, taking no additional precautions or instituting ad hoc security measure changes in the present circumstances may be met with greater skepticism by a fact-finder as to whether newly implemented procedures were reasonable under the circumstances. On the other hand, implementing a plan with defined steps and procedures can provide helpful documentation in the event of any future dispute. Having this type of documentation helps persuade a fact finder that the measures adopted were reasonable and thought through, ultimately helping to demonstrate that, despite changes, the protective measures are still reasonable under the circumstances.

David A. Prange is a partner at Robins Kaplan and leads the trade secrets subpractice. His practice focuses in complex business litigation with an emphasis on intellectual property, including patents, trade secrets, trademarks, and licensing disputes in federal and stat courts across the United States.
DPrange@robinskaplan.com

Christopher K. Larus chairs the national intellectual property and technology litigation group at the firm. For more than 25 years, he has helped his clients protect their IP rights. He tries complex trade secret, patent, trademark copyright, and licensing cases in courts around throughout the United States and in both national and international arbitration.
CLarus@robinskaplan.com