Safeguarding Trade Secrets With A Newly Remote Workforce

By **Daniel Melman** (March 23, 2020, 2:17 PM EDT)

Daniel Melman

As governments race to stem the spread of COVID-19, many companies are encouraging, if not mandating, that their employees work remotely.

While this is a sensible measure designed to minimize transmission of the virus, it also presents certain risks to the security and protection of a company's trade secrets and other confidential information.

Some employees may, unfortunately, seek to exploit the current situation for nefarious ends and misappropriate the company's trade secrets — often its most valuable intellectual property assets — while other employees may simply be careless or lack necessary knowledge and training to prevent the inadvertent disclosure of confidential information.

Trade Secrets Law Primer

Trade secrets are a very important part of any company's IP portfolio. Virtually every business, in any industry, possesses trade secrets; however, unlike patents, copyrights or trademarks that are publicly recognized and registered with the government, companies tend to overlook trade secrets because both their creation and continued existence depend on secrecy and because trade secrets usually constitute nothing more than information or know-how.

It is this failure or inability to grasp the full extent of a company's trade secrets that often leads to the misappropriation or other loss of trade secret protection that can severely and negatively impact a company's value. Indeed, experts estimate that the total theft of U.S. trade secrets accounts for anywhere between $180 billion to $540 billion per year.

There are four basic elements that must be present in a trade secret. First, a trade secret must consist of information. The types of information that have been protected by trade secret law are virtually limitless but generally fall within either technical or business information.

Examples of technical information trade secrets include computer algorithms, specialized formulas, plans and specifications (such as for specialized equipment), manufacturing methods and techniques, as well as negative know-how (e.g., processes and designs proven not to work through expensive research).

Examples of business information trade secrets include sales methods, marketing strategies and business opportunities, distribution methods, raw material sourcing and customer lists.

The second element of a trade secret is that it must derive economic value (actual or potential) from the fact that it is secret and cannot be put to use by others including competitors. Third, the information cannot be generally known by other persons or entities in the industry who could realize economic value from its disclosure or use.

Fourth, and critically important, the information must be treated as a secret and be the subject of what the law deems reasonable efforts to maintain its secrecy. In other words, for information to acquire and maintain trade secret status, its owner must exercise

reasonable efforts to maintain its secrecy. What constitutes reasonable efforts is an extremely fact intensive inquiry that depends on a myriad of circumstances and continues to be an evolving area of law.

Over the past several years, as cultural attitudes toward remote working arrangements have shifted, many companies have been proactive in implementing and enforcing robust policies and procedures as well as employee training programs as part of their reasonable efforts designed to protect confidential information, including trade secrets.

Many companies, however, remain behind the curve, and still other companies are facing an unexpected and new reality with entire offices now operating remotely in the face of the COVID-19 pandemic. To that end, below are a few practical measures that companies can and should immediately implement, or refresh themselves on, while their employees are required to work remotely.

Of course, these measures are targeted only toward remote working issues; a more holistic approach should be undertaken to eliminate or minimize trade secret vulnerabilities in connection with a company's other work processes, e.g., business dealings with vendors, partners and customers.

Clear Guidelines and Expectations

The first step in protecting company proprietary and confidential information is to ensure that all employees are made aware that data security is a company priority and that employees have an active role in making sure that the company's confidential information is not mishandled.

Companies should clearly identify and mark business information that they consider confidential or a trade secret and ensure that employees are aware and understand the difference between the company's confidential and nonconfidential information.

For example, companies should consider integrating electronic alerts or pop-up windows that remind employees of the company's confidentiality procedures and policies when they access proprietary networks and should clearly identify databases containing highly sensitive and trade secret information and data.

If creating formal policies and procedures under current circumstances is not feasible, then a plainly worded email or memorandum issued to all employees, setting forth the company's expectations regarding the access, usage and protection of the company's confidential information is a reasonable intermediary step.

Security Infrastructure

Although the degree of security measures that a company should undertake to protect its computer networks and infrastructure will ultimately depend on the particular industry, sensitivity of the information and the scope of permissible access, among other factors, a certain baseline level should be expected.

For example, access to the company's confidential information and trade secrets should be restricted to only those employees with a specified business need. Administrative safeguards, such as password protections or other authentication good practices, should be implemented.

Whether a company is using a cloud-based sharing system, virtual private network, or some other network-access method, the company should also monitor and record (in compliance with applicable laws and regulations) their employees' access to sensitive databases containing trade secret information and should regularly check for unauthorized access or other irregular activities (e.g., downloading unusually large amounts of data, transmission of confidential information to an employee's personal email account or deletion of network data).

The company should establish management protocols for identifying, reporting and addressing any breaches or inadvertent disclosures of confidential information so that appropriate mitigation and remedial actions can be considered and undertaken. It is critically important to act quickly when a breach or misappropriation of confidential information and trade secrets is discovered or suspected.

Remote Security

Employees who work remotely should be instructed and expected to take precautions to maintain the security of confidential information. Hard copy confidential documents and other confidential company property should be treated with the same attention to formality and security as when working in the office and stored in a manner to protect against inadvertent disclosure.

Companies should ensure that their employees conduct company business only on work-issued devices or on private devices with appropriate and up to snuff cybersecurity software. Similarly, employees should be instructed that work-related email and other electronic communications should be conducted exclusively via work-issued email addresses.

Employees should also be cautioned to never use public Wi-Fi hotspots to conduct any confidential business dealings. And, they should be provided with assistance in undertaking measures to protect their home Wi-Fi networks, including password protection and limiting access.

Social Media Policy

Many companies encourage their employees to actively use social media to increase contacts and to interact with current and potential customers. Indeed, the internet and social media have redefined how many companies do business.

While such social interaction is often critical to a company's marketing and client outreach efforts, it also poses potential risks for the inadvertent (or even purposeful) disclosure of confidential information because of the lowered level of formality associated with social media communication.

Crafting and disseminating a social media policy that clearly instructs employees on the permissible limits of discussing and handling confidential and other highly sensitive company information on social media platforms is another important consideration in the overall effort to protect a company's trade secrets.

COVID-19 has forced many companies to implement new remote working arrangements. While such arrangements present inherent challenges to securing and protecting confidential and trade secret information, these issues can be handled through proper planning and training.

Every company with a substantial remote workforce should analyze its weak spots and determine how it can reduce the potential for inadvertent disclosure or willful misappropriation of its confidential information and trade secrets.

Daniel J. Melman is a partner at Pearl Cohen Zedek Latzer Baratz LLP.