BRINKS GILSON & LIONE
100 YEARS OF IP LAW

THINK FORWARD

5 Tips for Protecting Your Trade Secrets While Working from Home

By Daniel Parrish, Mark Remus

May 15, 2020

Working from home is no longer a short-term inconvenience. It is the new reality and will likely persist for many even as states lift their respective shelter-in-place orders. With employees working from home, there is an increased risk that a company's valuable trade secrets can be inadvertently disclosed, protections lost, or even stolen. Companies must remain vigilant to protect their trade secrets, not only to prevent trade secret theft in the first place, but also to show that the company took reasonable measures to protect those trade secrets and that they are entitled to trade secret protection under the law. The following are five tips for companies facing these challenges:

1. Address Unique At-Home Risks

Companies have less control over their information when employees work from home. Steps should be taken to address these differences and safeguard information so that the same standards for protection of confidential information apply while employees are working from home (or another remote location) as when employees work from the office. Steps to consider include, among others:

- Security requirements for home Wi-Fi networks, including sufficient password protection, limiting in-network discovery and sharing, and requiring a Virtual Private Network (VPN) software to access sensitive company files.
- Require use of multi-factor authentication for access to network resources.
- Restrict the use of portable memory devices to store or download confidential information.
- Periodically collect employees' computer log files for portable memory devices installed, and inquire about new devices.
- Limit the ability to print documents and, if printing is allowed, provide instructions or tools to destroy confidential documents and instruct employees not to dispose of them in the trash.
- Monitor remote downloading of confidential information from company servers and take action against suspicious activity.
- Require employees to turn off active listening devices at home, such as Amazon's Alexa and Google Home.

2. Train Your Employees

Companies should educate their employees about the need to protect confidential information and steps they should take to protect that information when at home. This training is particularly important during work-from-home conditions because of the unique challenges and potential technical solutions

discussed above. Employees should be reminded how to identify documents containing confidential information, how to handle those documents, and the importance of handling that information properly. Particular attention should be paid to educating employees about the risks presented when working from home, such as being cognizant of others in their home being able to see confidential documents or overhear confidential conversations. Employees should understand that trade secrets can be lost not only through malicious theft, but also through carelessness. Where possible, employees should be encouraged to work in a private space to which other members of the household do not have regular access. Where private space is unavailable and/or other members of the household may overhear conversations in a teleconference or video conference, employees should use headphones or headsets to limit information that might be overheard and to minimize the context within which it could be understood. Any training need not be formal; it can be done in small groups or communicated through email. Save any written communications to employees to preserve evidence of measures taken to protect your trade secrets.

3. Identify Key Trade Secrets

Protecting *every* trade secret a company owns in the midst of a global pandemic can be a daunting task, but prioritizing protection of a targeted set of the most important trade secrets is more manageable. Companies should identify the trade secrets that are the most valuable and/or whose loss would present the greatest risk to the company. This allows the company to focus resources on protecting the trade secrets that are most important and it communicates to employees where they should focus their care and attention. It is also necessary to identify *what* you are protecting in order to determine *how* to effectively protect it. Once those key trade secrets are identified, it is also beneficial to conspicuously mark documents disclosing those trade secrets in order to put employees on notice that those documents must be handled with utmost care and consistent with the company's policies and procedures for such documents. Such marking can include physical marking of the documents in addition to pop-up windows that caution an employee when they access confidential information. Most document formats also permit password protections and/or restricted capabilities for editing and accessing. Use these built-in capabilities liberally.

4. Limit Who Has Access To Information

It is advisable to limit access to company trade secrets to only those people who need to know the information to do their job. Simply put, the more people who know a secret, the greater the risk that it won't stay a secret. Companies can control who has access to certain information by limiting access to particular servers or folders and/or requiring passwords to access particular information. For particularly sensitive information, consider granting access on an as-needed basis. If an entire department has access to a company's "crown jewel" trade secrets, they may be at risk of inadvertent disclosure or theft. The Coca-Cola recipe is famously only known and accessible to a small handful of employees.

Protection of confidential information is only as strong as its weakest link. Your employees are not the only ones working from home – your customers, suppliers, and vendors are in the same boat. Just as you limit access to confidential information internally, you should also limit disclosure of trade secret information to third-parties. If it is necessary to disclose confidential information to third-parties, you should have explicit agreements in place (confidentiality agreements, non-disclosure agreements, etc.) that protect that disclosure and ask recipients for assurances regarding what they are doing to protect your information. To the extent confidential information must be shared with third parties, companies should track exactly what files and information is shared, and ask for the return of (or destruction of) such information from the third party when the agreement expires or the business is completed, similar to treatment of confidential documents under a protective order in litigation.

5. Apply Technical Safeguards, But Make Them Reasonable

There are a myriad of technical options available for companies to safeguard their information, including passwords, firewalls, encryption, multi-factor authentication, etc. A company should consult with its

internal or external experts to identify and implement reasonable technical solutions to limit access to and distribution of a company's trade secrets.

Technical solutions cease to be effective however, if they are so burdensome that employees work around them by communicating outside of a company's secure systems, such as through text, private email or cloud services. For this reason, companies should balance the benefits of a particular solution against the practical reality that the solution should not be so burdensome that it forces employees to work outside of the company's approved methods of communication.

Key Takeaways

There are no bright line rules for which steps are reasonable to protect trade secrets during these difficult work-from-home conditions. The insights provided here are not a statement of the law. They are tips for companies to consider to proactively safeguard trade secrets.