Labor/Employment,
Intellectual Property
Oct. 7, 2020

Bookmark

Remote workforces increase pressure on keeping trade secrets protected

With more workers accessing, disclosing, using and creating valuable company information from their homes, prudent company leaders must ensure that they have appropriate procedures, training and safeguards in place to protect company trade secrets.

ROBERT B. MILLIGAN
Partner, Seyfarth Shaw LLP

Email: rmilligan@seyfarth.com

UC Davis SOL King Hall; Davis CA

Robert is the co-chair of the Trade Secret, Computer Fraud and Non-Competes Practice Group and editor of the firm's Trading Secrets blog.

See more...

Shutterstock

TOP TRADES SECRETS 2020

While many companies employed a mobile workforce before the COVID-19 crisis, the magnitude of the pandemic and the incumbent stay-at-home orders have fundamentally changed how employees work. While experts debate the extent to which companies will return to their traditional work environment and practices once the pandemic subsides, many companies have had to cope unexpectedly with having the vast majority of their employees working at home. Company leadership, including legal, HR and IT resources, have scrambled to maintain continuity, including attempting to secure essential computer hardware and network infrastructure, as well as addressing how to employ appropriate policies and training to equip this new mobile workforce as part of our new

normal.

With more workers accessing, disclosing, using and creating valuable company information from their homes, prudent company leaders must ensure that they have appropriate procedures, training and safeguards in place to protect company trade secrets. Trade secret protection requires reasonable secrecy measures. Companies must ensure that they protect these valuable assets by maintaining the requisite secrecy standard as they navigate these unprecedented times. Below are some areas that leaders should assess and address as needed to protect company trade secrets.

Assessment of Existing Policies and Agreements and Making Necessary Updates

While some companies had remote work policies that addressed information security and trade secret protections prior to COVID-19, others did not or such policies had noticeable holes concerning security and trade secret protections. A prudent first step is to evaluate the company's existing policies and agreements to determine whether they provide sufficient protection in light of the company's current remote work environment.

Basic protections should include nondisclosure agreements and policies with clear identification of categories of information that the company deems confidential and proprietary. Companies should implement a remote work policy which makes clear that such nondisclosure obligations apply when working outside the office as well, including using social media. Policy requirements should address access to company systems and devices and the transfer of company files outside the company network, including addressing the company's expectations related to the transfer of company files to personal email accounts, USB and other file storage devices/accounts. Many companies prohibit such transfers, except with express company consent. Companies should also consider prohibiting or limiting the printing of sensitive company documents at home. Companies should also consider using clean desk policies with their remote workforce to help encourage good secrecy habits.

Employee Training and Education

As part of the implementation of a remote work policy, companies should provide practical training on the policies so that employees understand the dos and don'ts of working at home. Training should include making it clear that working at home does not abrogate employees' confidentiality obligations and that employees should try to work in a secure work environment, such as a home office. Employees should turn off home assistants such as Alexa and Google Home in the home office. Employees should avoid conducting important video or other conferences in the presence of their family or other third parties where there may be confidential information disclosed and when that is not possible or practical one should use appropriate headphones or earbuds. Companies should also provide training to employees on avoiding accessing malicious emails that may compromise network security.

Training should be clear on the company's expectations with respect to using a secured network or VPN to conduct work. Employees should avoid public Wi-Fi and be instructed to use a safe password protected internet connection. Companies should also remind employees to respect and abide by confidentiality designations. Employees leading video conferences should be encouraged to use secure platforms and requiring meeting identification numbers and passwords for access to meetings. Additionally, the company should clarify its expectations with respect to any prohibitions on storing company data on personal devices, accounts and storage.

The training should attempt to impart a strong company culture of confidentiality and mutual beneficial explanation of how strong confidentiality protections protect the company's intellectual property assets and contribute to company success. The training should also convey the company's expectations at the time of hire and upon termination so that employees realize that during their lifecycle with the company that they are not to rely on or improperly use others' intellectual property and that the company expects them to surrender its information at termination. Careful attention should be given to consistency of policy and practice amongst the workforce so that employees, even if they are in the C-suite, are held to certain company-wide minimum standards. Employees should receive periodic reminders regarding the company's expectations through recurring training or email reminders. HR managers should counsel employees who are found to deviate from company policy.

Assessment of High-Risk Business Segments (Sales/Engineers) and Scenarios

Company legal and HR leaders should conduct a risk assessment of their company's workforce who have access to the company's most valuable information assets. Oftentimes, these employees are in the C suite, sales force, engineering, or research development departments. Competitors may target these particular high-value asset employees. Further, disgruntled employees in these sectors constitute an acute risk because of their access and motivation, coupled with a remote work environment. Leaders should understand how these segments of the workforce are conducting their day to day business and what particular systems that they are accessing on a recurring basis. Any personal storage or transfer of such information should also be prohibited. Companies should consider employing tracking software for mission critical information assets that track user access and dissemination. Careful monitoring of key files and folders through the use of effective software can help minimize trade secret misappropriation events. Specialized training and access requirements, including multi-factor authentication, should be considered in these segments.

Onboarding and Departures

In our remote work environment, particularly with an increase in terminations and furloughs, special care should be given to onboarding and departure procedures. With respect to onboarding, companies must be vigilant with new hires to make sure that they understand not to use their former employer's information, through their agreements, policies and training. New hires that retain their former employer's information on personal devices or accounts must understand that they put their new employer at risk and compromise their employment by retaining and using such data. With respect to off boarding of employees, companies should ensure that their valuable information has been returned. Companies should consider using exit interviews and termination certifications to ensure that the departing employees understand their return of company material obligations and continuing non-disclosure obligations. As many employees have been working remotely, special care should be given in probing whether company information was stored on personal devices or accounts or otherwise retained. HR leaders, with the aid of competent forensic examiners as appropriate, should employ practical measures to

secure the return of company information.

Return to Work

While California has proceeded more slowly in allowing employees to return to the workplace, other states have moved more quickly. As part of companies' return to work plans and policies, which may consequently vary based upon state or county, careful consideration should be given to ensure that company information is properly stored on company servers and networks. To the extent that company information is stored on personal devices or accounts, companies need to have clear expectations for employees on how that data should be handled, e.g., saved to company servers and/or deleted from personal accounts or devices. Special care should be given to such information that may be covered under an existing litigation hold. Companies should also consider an amnesty program for employees who may have violated specific policies concerning the storage of company information on personal devices/accounts while working remotely as part of a return to work policy, particularly where there was no improper intent in such actions.

Company HR and IT leaders can formulate right size approaches to address such scenarios with the goal of ensuring that valuable company information is brought home. Additionally, in connection with a return to work policy, companies should consider questionnaires and certifications as part of obtaining the return of company information.

The unprecedented movement of a large segment of the workforce to a remote environment during COVID-19 has and will impact how trade secret cases look going forward. Courts will scrutinize whether companies have employed reasonable secrecy measures to protect their trade secrets. Companies that have employed strong confidentiality agreements and remote work policies, effective employee training, and sound information security measures, during this period will have an advantage in protecting their valuable trade secrets and avoiding costly trade secret suits. In sum, those companies that have employed thoughtful protection measures with their remote workforce to secure valuable company information will come out of the pandemic with their trade secrets intact.