Cooley

Protecting Trade Secrets in the Current Climate

April 7, 2020

As the COVID-19 pandemic has displaced workers across the country, companies need effective ways to protect intellectual property and confidential trade secrets. This article outlines pragmatic steps to contain risk and safeguard proprietary information in a workplace that features remote workers, furloughs and layoffs. Because many cases of trade secret misappropriation arise due to displaced or departing workers, these steps are especially critical now.

Know your trade secrets

A trade secret can be any information that derives financial value from being secret, provided the owner takes reasonable steps to protect the information. Under this broad definition, courts protect all forms of financial, business, scientific, technical, economic or engineering information. This often includes sales pipeline information, customer information, technical know-how, R&D and go-to-market strategies. Trade secret owners must take affirmative steps to safeguard their trade secrets.

Federal and state laws protect trade secrets. In 2016, Congress passed the Defend Trade Secrets Act, which federalized trade secret law and provided federal court jurisdiction over trade secret claims. The DTSA provides more uniform application of the law, increases the prominence of trade secret litigation and affords preliminary relief for trade secret claims.

Companies need not necessarily conduct trade secret audits or catalog their trade secrets – particularly because any written inventory could make it more difficult to enforce protections for other unlisted information. Still, legal and business units should have a sense of the company's valuable, proprietary information. Building and maintaining that awareness can help identify what steps to take to protect that information.

Protect trade secrets in a work-from-home environment

Even in this new environment, companies should still implement basic steps to protect trade secrets: (1) restrict access to specific information to those who need to know; (2) employ nondisclosure agreements (NDAs) with workers and business partners; (3) advise and train new hires that the company does not want and will not use third parties' confidential information; and (4) create a culture of compliance by monitoring and educating workers.

As the workforce becomes more remote, companies should also embrace the following steps to protect sensitive information when employees work from home.

- **Establish and recirculate policies**: Create remote-working policies that remind employees of the importance of protecting confidential company information, provide steps on protecting information at home and reiterate existing policies.
- **Require secure connections**: Require employees working from home to use secure internet connections and devices. If feasible, restrict access to trade secret information to company-issued devices and/or company-managed VPN networks. Also, remind employees to password protect their home Wi-Fi networks.
- **Provide secure electronic communication platforms**: Provide secure, protected means for workers to remain in verbal and electronic communication with their teams. For electronic communications, instruct workers to use only company email accounts, secure shared drives or secure file-transfer systems. Where feasible, remind workers not to use personal devices or accounts.
- **Provide secure vernal communication platforms and adjust Zoom settings**: For verbal communications, instruct employees to use protected Zoom or other password-protected conference lines. Within Zoom, companies can take additional steps to protect their communications.

    - **Implement** host-only sharing to prevent unwanted "Zoomboming" or sharing of offensive materials.
    - **Enable** automatic muting upon entrance to a Zoom meeting to prevent participants' microphones from picking up embarrassing or inadvertent commentary.
    - **Adjust** settings to notify hosts when a participant joins a meeting and to prevent removed participants from rejoining a meeting.
    - **Enable** account settings to disable file sharing to prevent malicious files from being sent. Instead, present materials through screen-sharing and presentation modes.
    - **Disable** far-end camera control to prevent participants from controlling a camera other than their own.
- **Limit printed materials**: Limit or password protect employees' ability to print confidential documents. If employees must bring home printed or physical materials, instruct them to keep that information securely stored when not in use.

Protect trade secrets with furloughed employees

Furloughed employees remain employees with access to company systems. Furloughing employees creates unique challenges in protecting trade secrets, particularly because working for another company typically violates the employee's confidentiality agreement. Accordingly, companies should take the following steps with furloughed employees.

- **Maintain and reinforce policies**: Remind furloughed employees that company policies protecting confidential information remain in effect for the duration of the furlough.
- **Require prior approval for alternative work:** Companies must balance the need to protect IP with helping furloughed employees get paid. The best compromise is to require company approval before a furloughed employee may begin alternative work.
  The company should give this approval liberally unless the employee proposes working for a competitor or would otherwise expose trade secrets. Implementing this oversight allows companies to serve both protect trade secrets and help furloughed employees.

Protect trade secrets with departing employees

Unfortunately, many companies have had to restructure their workforce in response to COVID-19. A departing employee who signed an NDA or trade secret agreement maintains a contractual obligation to protect the company's confidential information. Accordingly, companies should take practical steps to safeguard their trade secrets with departing employees.

- **Conduct an exit interview**: Companies should conduct exit interviews with departing employees, even if they must be done remotely. The company should be prepared to execute any termination benefits packages or certifications electronically. Exit interviews should convey at least the following points:
    - **Communicate** that any NDA, trade secret agreement or other restrictive covenants (e.g., noncompetition or nonsolicitation) remain in place.
    - **Advise** employees that they have an ongoing obligation not to use company trade secrets.
    - **Provide** a copy of any NDA, trade secret agreement or restrictive covenants.
    - **Instruct** the employee not to access company property, including electronics.
    - **Alert** the employee that forensics exist to track any downloading, uploading or printing of proprietary information.
    - **Require** the employee to return all electronics and company property, as described in detail below.
    - **Consider** making the receipt of any termination benefits contingent on an employee certification acknowledging his or her obligations.
- **Disable access**: After an exit interview, the company should immediately disable the departing employee's access to company networks, devices and physical facilities.
- **Retrieve company property**: The company should arrange logistics for the employee to return all company property via a delivery service. This may require sending prepackaged boxes, engaging a courier service or prepaying for delivery. The employee should return all company documents, notebooks, files, devices, cell phones, laptops, thumb drives, external hard drives or other company devices. Every departing employee must return all company property. Consider requiring the departing employee to certify that all company property has been returned.

- **Preserve the employee's returned company property**: Provide each departing employee's returned company property to IT. Suspend any automatic IT processes (e.g., back up or auto deletion). Consider preserving and imaging laptop hard drives before the device is touched, particularly for workers with prime access to valuable information and/or workers likely to join competitors. In sensitive cases, log external storage devices connected to company electronics and documents created, accessed, printed, copied or emailed in the recent past. Employees are most likely to take confidential material when they perceive a risk of being terminated. Consider retaining a snapshot of the employee's email or other accounts.
- **Monitor post-termination emails to the employee**: Forward any post-termination emails to the departed employee's email account to a central person who is responsible for reviewing them and logging any suspicious activity.
- **Monitor post-termination sales communications**: Particularly for departed customer-facing employees, monitor all post-termination communications from customers or potential customers to evaluate whether the departed employee has attempted to divert business from the company.
- **Engage counsel**: If the company suspects a terminated employee may have stolen or attempted to steal trade secrets, the company should escalate its suspicions to its in-house legal team or Cooley contact. The company should be prepared to send cease-and-desist letters promptly if there is evidence to support the suspicions. Contact counsel even if you suspect the violation may have been inadvertent, because a timely cease-and-desist letter can often mitigate harm.

Workforce restructurings can be painful for everyone. Many employers mistakenly believe that only employees choosing to leave their employment for a competitor pose a risk of trade secret theft. But employees, particularly those in customer-facing roles or with technical knowledge, often have access to trade secrets that could be exploited intentionally or incidentally to the company's detriment.

Implementing these practices now minimizes risk later.

Key Contacts

Tim Cook Boston	tcook@cooley.com +1 617 937 2433
Michael Sheetz Boston	msheetz@cooley.com +1 617 937 2330