Five Ways To Protect Your Company's Trade Secrets While Working From Home

Shelter-in-place orders and the temporary closure of non-essential businesses to stop the spread of the novel coronavirus have resulted in entire companies now working from home. While a necessary public health step, this significant work environment shift has the potential to wreak havoc on a company's ability to protect its trade secrets and confidential information. Companies are trying to balance the practical reality of employees performing their duties in new (usually less secure) environments with the necessity of maintaining reasonable practices to protect their proprietary information. Below are a few significant steps companies can take to make sure that their proprietary information remains protected during this unprecedented time.

Remind Employees Of Trade Secret Protection And Confidentiality Policies, And Enforce Those Policies.

Although many companies have adopted robust policies designed to protect their trade secrets and confidential information, they may not always take steps to remind employees of or routinely enforce those policies. As a matter of practice, and particularly in today's changed work environment, it is important to remind employees that these policies exist, highlight the key aspects of the policies, and emphasize that employees are not allowed to disseminate any trade secret or confidential information to any unauthorized recipients. Have employees acknowledge that they received and understand these policies. Although physical signatures are not always practical when working remotely, employee acknowledgments can be executed using tools like DocuSign or via email confirmation. Companies also should designate individuals responsible for communicating with employees about these policies, and advise employees to contact these individuals if they have any questions about the policies, or how best to ensure compliance while working from home. If an employee is furloughed or terminated, steps should be taken to disable the employee's access to confidential information and the employee should be required to certify that all company materials have been returned or destroyed. Employees should be encouraged to report any concerns about improper use or dissemination of confidential information, and companies should monitor employees' activities (to the extent possible) for signs of misconduct.

Develop Additional Best Practices For Working From Home.

Working from home brings new challenges that may not be addressed by current policies. As necessary, companies should quickly circulate policies to reflect these new scenarios. In the past, courts noted that allowing employees access to confidential documents outside the office could be used as evidence that the information at issue was not a trade secret. While today working at home is a common and even mandatory practice, companies should make it clear what the expectations are for employees working from home. If employees need to access trade secret or confidential information in order to perform their duties, the information should be maintained in a secure location, where third parties cannot access it. Phone calls and video meetings (e.g., via Zoom) should be conducted in a manner that reduces the possibility of other people hearing or interfering with them. If employees do not believe that they can keep information confidential in their current living situation, they should contact a designated person, who can help employees develop strategies for taking reasonable steps to protect the information. Printing documents should be prohibited or severely limited. Any hard copies of confidential documents should be kept securely and then brought back to the office when it reopens for proper disposal. Take the opportunity in any new policies to clarify existing policies and adopt best practices.

Five Ways To Protect Your Company's Trade Secrets While Working From Home

Remote Security.

Companies should have in place a multi-factor authentication feature that allows employees to log into the corporate network from home through a secured connection, such as a VPN. They should also instruct employees to always sign into the corporate network to access corporate documents and information and to contact IT staff if they experience any difficulties. Often courts find that remote access capability obviates the need to send documents to personal devices and accounts. Courts have also noted, however, that if a company has remote access capability, but it is common for employees to not use it, an employer may have a difficult time proving that it prohibited employees from working outside the network. Therefore, under no circumstances should employees be permitted to work outside of the corporate network. This includes the use of non-sanctioned apps for working with data.

Be Aware Of An Increase In Scamming.

The surge in employees now working remotely has resulted in a surge in hacking attempts against corporations. While employees should be instructed to sign into the corporate network, companies must take steps to make sure that hackers and other unauthorized third parties cannot exploit less secure personal networks as a gateway to the corporate network. Personal WiFi networks should be password protected, and access to them should be limited. IT departments should routinely advise employees about how to make their home networks more secure and make themselves readily available to consult and answer questions from employees.

Secure Data Sharing.

Many companies thrive through technology that enables spontaneous and continuous interactions between their employees. When working from home, these interactions are often more difficult or lost altogether, and employees may naturally try to recreate them. Employees should not, however, discuss trade secret or confidential information via text message, personal chats or emails, or other unsecure forms of communication. In the past, to negate allegations of theft, employees alleged that their employer allowed them to email documents to their personal devices because it was easier than using a secure method. Today this claim is most likely not sufficient because there are efficient tools for employees to work with documents outside of the office securely. On the flip side, it also means that employers must utilize these tools. Companies should develop secure ways for employees to communicate, such as regularly scheduled, password-protected video meetings. To the extent that trade secret or confidential information needs to be transmitted to a third party, transmittal should only be done through secured servers or drives, like a secure FTP site. Many such document-sharing tools include options for users to add security measures (e.g., HighTail allows users to password-protect and time-limit the accessibility of download links, and Box allows users to implement two-factor authentication for shared folders), which are simple ways to ensure information remains protected and only available to authorized users.

Communication is essential to successfully protecting trade secret and confidential information while employees work from home. Companies should regularly remind employees of existing policies, adopt new or modified policies to address new scenarios as they arise, and regularly publish and enforce those policies. They should also facilitate secure external and intra-company methods of communication, and designate IT and compliance personnel to assist employees who will inevitably have questions about working in a remote environment with new forms of technology.

Five Ways To Protect Your Company's Trade Secrets While Working From Home

For more information, please contact one of the following attorneys:

Mark Edgarton
Partner
617-248-5101 | medgarton@choate.com

Kevin C. Quigley
Principal
617-248-4737 | kquigley@choate.com

Caila Heyison
Senior Associate
617-248-4854 | cheyison@choate.com

Greta A. Fails
Principal
617-248-4039 | gfails@choate.com

Anita Spieth
Principal
617-248-4031 | aspieth@choate.com