Defending Against Employee Defection: The Intersectionality of Cybersecurity and Trade Secret Protections in the Digital Age

Corey A. Bauer

Corey A. Bauer is a Partner at the law firm of Houston Harbaugh, P.C. in Pittsburgh, Pennsylvania. He practices in the areas of intellectual property litigation, data privacy and cybersecurity litigation/investigations, and commercial litigation. Corey regularly counsels clients on issues relating to the protection of intellectual property and other digital information from cyber threats, as well as responding to cyberattacks and data breaches.

Cyber security and data protection often involve the protection of data and intellectual property ("IP"), such as trade secrets, from outside threats, but is your company prepared to defend against threats from the inside? The trending hybrid and remote work models in the wake of the COVID-19 pandemic have revealed that corporations have sub-par data protection and cybersecurity protections to defend their IP from inside the building (or their employees' living rooms). In fact, the cyber security company Code42 published its Annual Data Exposure Report for 2022, finding a 1 in 3 chance that a company will lose IP when an employee quits.

The tumultuous job market has only accelerated the effects of this. Companies need to be prepared with adequate legal protections to protect their trade secrets before an employee leaves the company voluntarily or otherwise. As this article will discuss, protecting trade secrets requires a proactive and conscious risk assessment approach anticipating the inappropriate acquisition, dissemination, or disclosure of trade secrets and other information, such as personally identifiable information (PII) of customers.

Cybersecurity Risks for Company Trade Secrets and How to Defend Against Them

Many factors may lead to an employee leaving a company with company data or IP, and it may not only be to assist a competitor. For example, employees sometimes feel ownership of the IP they helped to create and may leverage it to obtain a higher-paid position with a competitor. It is not unheard of for an employee to sell company IP or log-in credentials on a dark web retailer for financial gain or merely out of revenge. Crowdstrike, an international cybersecurity firm, recently published in their 2023 Global Threat Report that 2022 saw a 112% increase in data broker ads on the dark web. These brokers sell access information to company servers. Regardless of how it may occur, measures must be taken from a cybersecurity perspective to help protect company trade secrets. Ensuring that the company is protected and that employees understand company IP protection protocols is crucial, particularly when protecting trade secrets.

Code42's report revealed the most glaring corporate deficiencies in data and IP protection while an employee is working at the company. For example, the most commonly used means of data theft by employees is using USB devices and smartphones. The more portable data is, the more difficult it is for the company to control. Companies should forbid unauthorized USB devices, as they not only carry company information out of the building but also can carry potential malware into it. The rise of work-from-home policies has complicated this, considering that employees at home can insert a USB device into

their company device at will. This can be countered by data outflow tracking software.

According to Cloud42, the use of cloud-based storage services, such as Google Chrome and DropBox, accounts for over half of all data exposures outside of USB and other types of portable device disclosures. Crowdstrike's 2023 Global Threat Report that cloud-based storage exploitations rose 95% year over year. Unregulated access to these programs and the use of them with company materials should be forbidden. Additionally, properly managing and monitoring email accounts is extremely important. Former employees sometimes email themselves company trade secrets before a departure. Companies should work with their Information Technology departments to have email activity records dating back further than the default seven days of most email service providers and review employee emails, including deleted emails, after their departure. Some companies may utilize a keystroke or data outflow logger, as mentioned above, which can more closely trace employee behavior on company devices.

The more invasive protections may be more advisable for the employees chosen to have access to information the company believes is a trade secret. It is essential to consider that the protections a company can take must be balanced against the need to create a working environment where employees feel comfortable and productive. Having a clear policy for the personal use of company devices and a work-from-home policy can set expectations for employees while furthering the protection of confidential information.

One general and effective rule is restricting access and keeping current employees on a "need to know" policy concerning trade secret information. This does not mean a company should keep employees in the dark. For example, many employees may need to know that new software is being developed to enhance a business process, but not many need to know how that software is programmed. The critical consideration is ensuring that every employee has the information they need to work effectively without disclosing trade secret information unless disclosure is necessary for job function.

Even after an employee leaves, he or she can wreak havoc on their previous employer if the proper safeguards are not met. A surprisingly often overlooked measure companies must take is removing employee access to all company systems on the day of departure. The company may instead remove employee access to the most sensitive data when notice is given that the employee is leaving, which may be advisable under the circumstances.

An exit interview is another critically important step in protecting trade secrets. The exit interview should be conducted with the employee's supervisor and company legal staff or outside counsel. The supervisor can provide details of the protected information and lessen the risk that the company counsel will one day become a witness should the matter later go to trial. This should not be a cross-examination, but rather a conversation with three goals: First, remind the employee of confidentiality responsibilities and obtain an agreement to honor them. The company should identify examples of confidential information for the employee to avoid any doubt about what the company considers confidential. Second, obtain all confidential documents in the employee's possession. The method for doing so varies but often involves disclosing on- and off-premises materials. Third, the company needs to get information to assess whether its trade secrets are in jeopardy. Questions should be asked of the employee to determine their new employer and what they believe their role will be there.

It is important to acknowledge that not all information identified for trade secret protection requires the same forms of protection. And although this article focuses on digitally stored information and cybersecurity, various efforts can be utilized to protect said information and those protections can vary company-to-company. For example, a baking recipe stored in a digital file will be protected differently from computer code distributed within software.

Federal Trade Secret Law and its Protections

Federal and state laws can provide companies with a private cause of action to defend their trade secrets. Since 2016, the Defend Trade Secrets Act (DTSA) has provided a pathway for trade secret defense through the federal court system. Further, all but two states, New York and North Carolina, have adopted the Uniform Trade Secret Act (UTSA), although they have other laws designed to protect trade secrets at common law and elsewhere. Circuit Courts across the country have consistently held that the DTSA and state statutes aligned with the UTSA are substantially similar from a legal analysis standpoint. Thus, for this article, the focus will be on the DTSA.

A trade secret is defined in the DTSA as "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques,

processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing." However, the DTSA also requires that the purported trade secret derives "independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person" or company who can obtain economic value from the disclosure or use of the information (e.g., a competitor). 18 U.S.C. § 1839.

Critical to the article here, the DTSA additionally requires that the purported trade secret owner establish that it "t[ook] reasonable measures to keep such information secret." 18 U.S.C. § 1839(3)(b). Protective measures such as those discussed above, along with non-disclosure, non-compete, and non-solicitation agreements (should state law permit said agreements), are currently common ways to complete this necessary step to establishing trade secret protection under the law. However, the US National Labor Relations Board's general counsel issued guidance on May 30, 2023, announcing that noncompete provisions contained in many employment agreements violate the National Labor Relations Act unless narrowly tailored to special circumstances justifying the restrictions.

Importantly, courts have noted that "a company need not monitor its employees like a police state to garner trade secret protection for its confidential information." See, *Vendavo, Inc. v. Long*, 397 F. Supp. 3d 1115, 1136-37 (N.D. Ill. 2019). This is the trend across all Circuit Courts, as "reasonable measures" are all that are required under the DTSA. However, as the digital age evolves, so too does the definition of "reasonable," and one errant disclosure by a company without adequate protections can waive trade secret rights.

Conclusion

Vigilance against trade secret theft is an ongoing process that requires a company to have comprehensive monitoring and cybersecurity measures. As the digital age progresses, additional cybersecurity safeguards will be expected of trade secret holders. Although different secrets require different methods of protection, an IP protection program with policies that address the above concerns, among others, is the first step to protecting your digitally stored IP from disgruntled employees and ensuring you have remedies at law when your trade secrets are misappropriated. With the tools listed above, any company can be well on its way to establishing adequate protections for its trade secrets under the law.