The Six Stages of Trade Secret Misappropriation Protection

Article by David L. Cohen, Michael Kasdan & Donal O'Connell

Trade secret protection has become an increasingly important part of the arsenal of protections available for a company's intellectual assets. The reasons for this are many and include: (i) stronger federal protection under the Defend Trade Secrets Act ("DTSA"), (ii) the ability to protect a wide range of valuable information, including information that would not be eligible for protection under existing patent, trademark, or copyright law, (iii) the time, cost, and uncertainty inherent in the patent application process and a reluctance to disclose one's "secret sauce," and (iv) the ubiquity and transportability of data and increased importance of data and data-based analysis and technologies.

When considering how to protect their trade secrets, many companies typically begin and end their analysis with putting a valid non-disclosure agreement in place when communicating with third parties about their proprietary technologies. This approach, as we have **discussed** elsewhere, is necessary but not sufficient. Rather, proper trade secret protection of intellectual assets – one that will be able to most effectively guard against misappropriation and allow a company to pursue an enforceable remedy in instances of misappropriation – requires a proactive, holistic, and multi-pronged management approach.

This article examines considerations for an effective trade secret asset management through the prism of trade secret misappropriation, examining how to approach the question of what to protect as a trade secret and how and whether a company would safeguard and enforce its IP if there were a misappropriation.

There are six sequential stages of consideration: Recognition, Detectability, Provability, Specificity, Correlation, and Mitigation. (Any similarity to "The Six Stages of Grief" is purely coincidental. In fact, following these six stages is designed to avoid grief on the part of the trade secret holder when the time arises to pursue a claim of trade secret misappropriation.)

THE FIRST STAGE IS RECOGNITION.

In this first stage, the trade secret owner *recognizes* that they have a protectable trade secret and considers how to protect it. The first requirement in proving a trade secret misappropriation case is for the trade secret holder to establish that the information is protectable as a trade secret (i.e., that it is not generally known or ascertainable and has economic value) is that **"reasonable measures"** were taken to keep it secret. There is no "bright line" test under the DTSA for what constitutes reasonable measures; **what is "reasonable" depends on the circumstances**. Measures to maintain secrecy may include both legal and technological protections. For example, on the legal side, what is the company policy regarding who has access to the information? Is it marked Confidential or Highly Confidential and governed by non-disclosure obligations? On the technology side, how is limited access enforced and maintained? Factors that are considered in determining whether the measures a company put in place were sufficiently reasonable include the cost and effort in acquiring the information, the value of the information, the level of competition in the marketplace, and how easy it is to reverse-engineer.

An important part of recognition is to begin to consider valuation. For a secret to be a trade secret under the law it must derive some economic **value from being secret**. Thus, the trade secret owner must be able to show that the secret had or has value, and that its value was based – at least in part – on it being secret. While the absolute dollar threshold required to be considered a trade secret is relatively low, getting a sense of what the secret is worth will be very useful should the owner need to seek **damages**. **Sophisticated trade secret owners** will keep track not only of the value of their secrets but the costs associated with keeping them secret – both for internal controls and to assist in later valuation and potentially pursuit of damages in the event of a misappropriation. Recognizing the ranges of values of trade secrets can

CONTINUED

also help to prioritize allocation of resources and make decisions as to how to safeguard the most important assets.

THE SECOND STAGE IS DETECTABILITY.

Once a trade secret owner has put a trade secret protection regime in place, the owner needs to next consider what processes or tools it will put in place to monitor and determine whether the trade secret has been compromised or stolen. Examples of available tools for *detection* range from video cameras to software to detect when confidential files are downloaded to employee laptops or devices without pre-authorization. Some processes include daily physical inspection of the premises where trade secrets are located and monitoring competitor products for suspiciously similarities. One of the most troubling aspects of trade secret asset management is the recognition that most misappropriation comes from your trusted colleagues. While outside threats such as hackers are a serious issue, according to **one survey** of the reported cases, a whopping 82% of cases involve current (55%) or former (27%) employees, more often than not (59%) acting alone. While perhaps a sad commentary on employee loyalty, this fact of life should be viewed as an opportunity to employ common sense measures that both create disincentives to misappropriation such as surveillance (**which can deter and thus reduce theft**) as well as incentives for good behavior (**increased pay and employee satisfaction can reduce theft**).

THE THIRD STAGE IS PROVABILITY.

Once a trade secret owner has detected a misappropriation, the next concern is being able to *prove* in a legally sufficient way that there was in fact a misappropriation. While legal sufficiency will vary between legal jurisdictions, non-manipulatable proof of a misdeed is always preferred. This can include time-stamped and encrypted video logs, or notarized affidavits chronicling security protocols made prior to any particular suspicion of a theft arose. Indeed, simple technical protections also would do wonders to deter trade secrets – as the same **survey discussed above** showed 45% of all trade secret theft was of files or documents which employees accessed or handled improperly (e.g., saving the information to a USB drive, laptop, or sending it as an email attachment). Accordingly, keeping careful records of key electronic documents (who accessed, where saved, when, etc.) can be critical in building a trade secret case.

THE FOURTH STAGE IS SPECIFICITY.

Once a trade secret owner can prove that there was a misappropriation, they will need to tie that misappropriation to a particular bad actor. While it is always good to know that there was a security breach, being able to pinpoint *specific* entities or people that were involved in the breach will allow the trade secret owner to take maximal advantage of the various judicial remedies available. For example, being able to show that a particular user or IP address was used to access a company's server should be enough for the owner to convince a court to grant legal discovery of the user or IP address or *ex parte* collection of other evidence – and perhaps temporary injunctive relief.

THE FIFTH STAGE IS CORRELATION.

Once a trade secret owner can tie a misappropriation to a bad actor, the next step is to show that is more likely than not that the bad actor possesses the trade secret due to misappropriation and not due to their independent invention. It is not always the case that there was misappropriation when a competitor releases a markedly similar product to the trade secret owner's product. The ability of the trade secret owner to specifically establish when, where, who, and how the trade secret was misappropriated can be fatal to a defendant's defense of misappropriation claim by arguing independent invention – especially if they could reasonably have done so (e.g., they had similar R&D capacities as the trade secret owner). There is least one **US circuit court opinion** that held that where defendant can reasonably claim independent invention, the trade secret owner will ultimately still bear the burden of proof that defendant did not independently invent the trade secret.

Indeed, many times disgruntled employees will steal trade secrets from their employer and try to leverage possession of those secrets into jobs or money from their former employer's competitors. **One approach** that rights owners can use to protect themselves is to watermark –

CONTINUED

literally or figuratively – their trade secrets, or intentionally include "**Easter Eggs**" such that when an unauthorized third party uses them there will be evidence that their use is unauthorized. For example, there are many, many examples of competitors who used stolen source code and were unsophisticated enough to remove the original owners of the code comments.

THE SIXTH AND FINAL STAGE IS MITIGATION.

Once an owner's trade secrets have been misappropriated, what can be done to minimize the damage from its possession by bad actors? This does not refer to taking immediate action and not sleeping on one's rights. While that is also important, this stage addresses how to structure and share trade secrets in such a way that make it hard for a thief to fully exploit them. For example, only providing trade secrets on a "need to know basis" or to limited recipients; or only giving portions of a trade secret to any one recipient, such that the portion of the secret shared cannot be used to fully exploit the value of the entire secret. Another, in the **outsourced manufacturing context**, is structuring manufacturing processes so that the manufacturing process is conducted in stages, at different locations, with (possibly) different OEMs.

Depending on the circumstances, some of these stages are completed sequentially. Other times they are accomplished in parallel – typically in breaches of IT systems, where the same tools may allow the trade secret owner to determine who accessed the system to access which trade secrets, and correlate those trade secrets to a competitor using them to the owner's disadvantage.

We hope that reviewing trade secret misappropriation through the lens of these six stages helps to provide a framework that illuminates your potential vulnerabilities and reveals what steps should be taken to shore up your or your client's trade secret protections.

We believe that forewarned is forearmed and **that auditing your trade secrets asset management** with each of these stages in mind can both shore up existing trade secrets, while also providing an appreciation for intellectual assets you may not have even known you had.

About David Cohen, Michael Kasdan & Donal O'Connell:

David Cohen, Donal O'Connell and Michael Kasdan have been involved with this form of IP for several years.

David Cohen and Donal O'Connell have had over 50 papers published on various aspects of trade secrets and trade secret asset management. They have conducted intense trade secret workshops for a variety of companies and organizations. They have also developed a leading-edge trade secret asset management solution to help clients (operating companies, legal & IP firms, finance & tax firms, and IP insurance providers) manage such assets in a proper and professional manner.

Michael Kasdan is the head of Wiggin and Dana's **Trade Secret Practice Group**. He has **authored numerous articles on trade secrets** and regularly speaks to clients about trades secret asset management and trade secret misappropriation.

David Cohen has been practicing IP law for over 20 years. He is the former Chief Legal and IP Officer at Vringo (at the time a public tech and IP licensing company); Senior Counsel at Nokia; and was an IP lawyer first at Skadden Arps and then at Lerner David.

Donal O'Connell is ex VP of R&D and ex Director of IP at Nokia; Adjunct Professor of IP at Imperial College Business School and an IAM300 Top Global IP Strategist member for several years.

Michael Kasdan is an IP Partner at Wiggin and Dana LLP and an Adjunct Professor at NYU School of Law. He has been listed as one of the world's-leading IP Strategists in the 2017 – 2019 editions of *IAM Strategy 300 – The World's Leading IP Strategists*. He is the author of the chapter on Patent Licensing and Monetization in the *Oxford Handbook of Intellectual Property Law* (Oxford Press, 2017). He is also the author of the chapter entitled "Dealing in Intellectual Property: What You Need To Know To Get the Deal Done" in *A Practical Guide to Successful Intellectual Property Valuation and Transactions* (Wolters Kluwer Press, forthcoming 2020).