Bloomberg BNA

Privacy and Security Law Report®

Trade Secrets

Trade secret theft is a rapidly growing global problem that converges with cybersecurity. In-house counsel must provide legal advice and direction on how best to align and prioritize cybersecurity and trade secret protection practices with legal requirements for the preservation of trade secrets, the authors write.

Trade Secrets

The Convergence of Trade Secret Theft and Cybersecurity: An In-House Counsel's Primer on Mitigating Risks



BY CHRISTOPHER C. BURRIS, NICHOLAS A. OLDHAM AND HEATHER R. KANTER

In today's world, companies are consistently faced with business operations that have expanded across the globe, employees constantly moving from location to location, virtually all assets being digital and connected to the internet, and unscrupulous competitors, even countries, trying to take advantage to help enhance their business fortunes and economies. On top of these changes, the rapid growth of the digital economy and our ever expanding connectivity has created more ways to steal trade secrets that are now easily scanned, copied, downloaded or exfiltrated. As a result, trade secret theft has become a rapidly growing global problem. Indeed, estimates of trade secret theft range from one to three percent of the gross domestic product of the U.S. and other advanced industrial economies. Simply put, trade secret theft and cybersecurity have converged.

Chris Burris is a partner at King & Spalding LLP in Atlanta and represents clients in matters involving privacy, information security and related issues.

Nick Oldham is counsel at King & Spalding in Washington and is a member of the Data, Privacy & Security practice group.

Heather Kanter is an associate at King & Spalding in Atlanta.

The good news is that a thoughtful strategy tailored to the issues facing your company and industry can greatly mitigate the instances of theft and, correspondingly, the business impacts to your company. While an article such as this cannot cover all of the issues, our goal is to touch on the four core points below. These points are the foundation for launching an effective and efficient trade secret program.

First, the essential condition of a trade secret is secrecy, and effective cybersecurity is necessary to maintaining secrecy in today's hyper-connected environment.

Second, the well-known National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework) has been widely adapted and adopted across industries and organizations as part of cybersecurity programs. The process set forth in the NIST Framework can be adapted and adopted into your trade secret program that is holistic and tailored for your particular business. Doing so will not only mitigate the instances of, and harm from, trade secret theft, but will also allow for the efficient joining of cybersecurity and trade secret programs for effective governance.

Third, as with cybersecurity, strong incident response processes are critical to mitigate trade secret theft. Again, these processes must join with the cybersecurity incident response processes.

Fourth, the effective incorporation of company counsel into a company's trade secret program is essential to establishing and operating an effective trade secret program.

Defining Trade Secrets—How to Protect What's in the 'Secret Formula'

Taking a page from real life, while detailing an undercover operation relating to the theft of advanced computer chip technology by the film's villain in the film The Departed, Alec Baldwin's law enforcement character stated: ''[o]ur target is a major transaction of microprocessors. Yes, those. I don't know what they are, you don't know what they are, who [cares]? Cash. Lots of cash is gonna change hands . . . .'' In those short sentences Baldwin boiled down the nature of what is a trade secret and why they are at risk of theft: secrecy and value derived from that secrecy.

Trade secrets have historically been a creature of state law. Under the Uniform Trade Secrets Act (UTSA), which most states have adopted, a trade secret is information that (i) is not generally known or readily ascertainable by others; (ii) derives independent economic value from its secrecy; and (iii) is the subject of reasonable efforts to maintain secrecy. UTSA, § 1(4). Trade secrets can be almost any type of information, including a formula, pattern, compilation, program, device, method, technique, or process. Indeed, virtually every business plan, customer list, source or object code, or industrial process could qualify as a trade secret.

A thoughtful strategy tailored to the trade secret issues facing your company and industry can greatly mitigate the instances of theft and, correspondingly, the business impacts to your company.

It is not surprising that the premise of trade secret theft became a plotline in an Oscar-winning movie—the writers presumably realized the cutting edge nature of this issue. In the past decade, there have been numerous major cases where trade secret theft cost companies millions of dollars. In fact, in 2008, just two years after The Departed was released, a former Intel Corp. employee was charged with stealing $1 billion worth of trade secrets relating to the company's microprocessors.

The subject of trade secret theft is not just one of Hollywood and periodic prosecutions. In fact, because this is such a serious issue in today's global economy, Congress has enacted an update to the law on trade secrets. Earlier this year, President Obama signed into law the Defend Trade Secrets Act (DTSA), establishing a cause of action at the federal level for trade secret theft. The DTSA, aimed at increasing consistency through a uniform body of trade secret law, incorporates a definition of trade secrets that is substantively similar to that in the UTSA, but there are a few minor differences between the two.

It is important to understand that trade secrets can be a powerful form of intellectual property because the legal protection lasts forever.

Where the UTSA defines a trade secret as information that derives value from not being generally known, the DTSA defines a trade secret as ''all forms and types of financial, business, scientific, technical, economic, or engineering information'' that derives value from not being generally known. The DTSA also provides additional examples of the types of information that can be trade secrets, including plans, designs, prototypes, procedures, and codes. Finally, the UTSA states that the information must be the subject of reasonable efforts to maintain its secrecy, whereas the DTSA states that the owner must take reasonable measures to maintain the information's secrecy. UTSA, § 1(4); 18 U.S.C. § 1839(3) *as amended by* § 2(b)(1) of DTSA. Under both the

   ISSN 1538-3423

UTSA and the DTSA, trade secrets do not require any registration or formal filings.

With this backdrop, it is important to understand that trade secrets can be a powerful form of intellectual property because the legal protection lasts forever—specifically as long as the owner is able to maintain its secrecy. For example, the formula for the lubricant WD-40 has been protected for over 60 years. The original formula is locked in a bank vault and has only been taken out twice. In contrast, a patent covers more limited subject matter, has a shelf life of 20 years, and requires the owner to disclose how the invention works in exchange for the patent's monopoly.

But trade secret protection can be lost in the blink of an eye when ''reasonable efforts to maintain secrecy'' are not adopted and that secrecy is lost. For example, the improper disclosure to a third party without contractual protections, a former employee taking trade secrets to his new employer or inadequate physical or electronic safeguards could all potentially result in the loss of trade secret protection. Those risks, particularly with respect to electronic safeguards, are precisely where the convergence between trade secret theft and cybersecurity is occurring, as the term electronic safeguards is roughly synonymous with cybersecurity.

The NIST Framework—And Its Applicability to Trade Secret Theft Prevention

The NIST Framework is an overarching, risk-based approach to managing cybersecurity. Organizations use the NIST Framework to develop comprehensive cybersecurity policies and procedures, which then serve as a blueprint for operationalizing administrative, technical and physical safeguards to mitigate business and legal risks. The NIST Framework ''Core'' is composed of five high-level functions: *Identify, Protect, Detect, Respond and Recover*. These functions are subdivided into a series of categories and subcategories identifying specific practices along with references to supporting government and industry standards. For example, the ''Identify'' function includes a ''Risk Assessment'' category that, in turn, includes subcategories such as identifying asset vulnerabilities and identifying potential threats.

The Framework also provides implementation ''Tiers'' that describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Core, ranging from ad hoc approaches to extremely sophisticated practices. The Framework ''Profile'' consists of the Tiers at which specified practices align with the standards or guidelines in each category and subcategory of the Core. An organization's present practices may be referred to as its ''Current'' Profile, whereas it may aspire to improve its practices to achieve a ''Target'' Profile.

Comprehensive trade secret programs should address various topics, including, for example, identifying trade secrets and marking them, drafting appropriate employee and third-party agreements and other critical documents, conducting onboarding and exit interviews and training of employees and applying physical safeguards and electronic safeguards. Adapting and aligning a trade secret program with the NIST Framework would address all of these topics—from the high-level functions and key considerations in the subcategories, to the long-term planning and execution provided by the Tiers and Profiles.

In general, the high level functions for a trade secret program can be thought of along the following lines:

1. Identify. What assets need protection? A company should have a process in place to regularly evaluate the information in its possession to identify, catalog and value that information for trade secret, patent, or other legal protection. Relatedly, a company should have a process in place to identify risks to that information including cybersecurity risks.

2. Protect. What safeguards need to be developed and implemented? A good trade secret program will have technological, personnel and physical security components, such as company policies, employer/employee agreements and policies, training and education of company employees, agreements with third parties and cybersecurity controls and monitoring.

3. Detect. What techniques can identify incidents? A company should develop and implement the appropriate activities to identify the occurrence of trade secret theft, including through cybersecurity incidents.

4. Respond. What techniques can contain impacts of incidents? The first 48 hours after theft of a trade secret can be critical, and a company should have a plan that enables it to identify the nature and scope of the problem, secure necessary evidence and develop and implement a strategy for responding to the breach that is rooted in business realities.

5. Recover. What techniques can restore capabilities? A company should develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to the trade secret incident.

Incident Responses Processes

Like cybersecurity, having robust incident response processes is critical to (i) mitigating the instances of, and harm from, trade secret theft, including maintaining as much trade secret value as possible following a theft; and (ii) providing the baseline for enforcement and litigation as appropriate. Cybersecurity and incident response processes go hand in hand—protecting your company from losing valuable information should be seamless and companies should not unjustifiably compartmentalize various aspects of their program.

With that in mind, companies should also consider the importance of insider threat programs. Just as a cybersecurity program and the NIST Framework are critical to organizations in protecting misappropriation of their trade secrets, so too is a strong insider threat program. As just one example of the significance placed on such programs, companies look to the Defense Security Service's (DSS) National Industrial Security Program Operating Manual (NISPOM), which requires cleared industry contractors to submit their insider threat program plans to the DSS for approval. More than 5,500 insider threat programs have been approved by the DSS as of Oct. 2016.

If your company suffers a breach and trade secrets are stolen, you first need to preserve the trade secret as best as possible.

If your company suffers a breach and trade secrets are stolen, you first need to preserve the trade secret as best as possible to retain its value and contain the compromised system or application. In some instances of insider threat, simply demanding that a former employee return the information may resolve the matter. Negotiating or other efforts to work with a former employee's new employer may also yield satisfactory results. For instances of exfiltration, injunctions or temporary restraining orders may be sought under both state law (under the UTSA if you are in an UTSA jurisdiction) or federal law (under the DTSA). Containment and preservation are key during the first minutes, hours, and days following a breach—particularly in light of the core requirement that companies take ''reasonable efforts to maintain secrecy'' for trade secret protection to be apply.

As noted above, remedies for trade secret misappropriation are available under state and federal law. The UTSA allows for an action for misappropriation by showing that the trade secret was (i) acquired through improper means, (ii) disclosed or used by a party who knew it was acquired improperly or (iii) disclosed or used by a party who knew it was a trade secret and that it had been acquired by accident or mistake. The UTSA provides for several remedies for wrongs committed under the act: injunctive relief, damages and attorney's fees. Most states follow the UTSA, but there are variations in the law and its application from state to state.

The DTSA—explained above—created a new, private federal civil action for ''an owner of a trade secret that is misappropriated . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.'' The DTSA does not preempt state trade secret laws, but provides a clear route for trade secret owners to pursue an action in federal court for trade secret misappropriation. The DTSA provides for injunctive relief for the period of time it would have taken to independently develop the trade secret. Where injunctive relief would be inequitable, future use of the trade secret may be conditioned upon a reasonable royalty rate under the DTSA. The DTSA also provides for damages and attorney's fees under certain circumstances. Unlike the UTSA, the DTSA also provides for an ex parte seizure of property ''necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action'' in extraordinary circumstances.

Counsel should be involved in all stages of cybersecurity and trade secret protection program development and implementation.

In addition to these routes, other civil and criminal remedies may be pursued following theft of trade secrets. For example, under the Computer Fraud and Abuse Act (CFAA), it is a crime to access a computer without authorization or to exceed authorized access. 18 U.S.C. § 1030. The CFAA creates a variety of misdemeanor crimes depending on the nature of the access, and is one of the primary routes for prosecuting computer crime. Additionally, if an employee stole information, there could be claims for breach of contract, violation of an NDA (if one exists), or a violation of a fiduciary duty.

Companies should work to create a trade secret program and incident response processes with these potential remedies in mind. Knowing what potential remedies are available and which the company may wish to seek can impact everything from the information technology policies – i.e., how should the company restrict user access to take into account the prohibitions in the CFAA—to Human Resources procedures—i.e., does the company's NDA adequately restrict employees' behaviors?

For example, companies must be vigilant in their hiring processes to avoid the accusation that they hired an employee that is revealing its former company's trade secrets. This is because companies in most U.S. jurisdictions can be liable for trade secret misappropriation if the company received information from a new hire that it knew or had reason to know was the trade secret of the employee's former employer. For example, California Civil Code § 3426.1 prohibits ''[d]isclosure or use of a trade secret of another without express or implied consent by a person who ... [a]t the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade secret was ... [d]erived from or through a person who had utilized improper means to acquire it... .''

Furthermore, the steps that a company takes immediately following discovery of a theft can often impact what remedies are later available. The role of company counsel in incident response and in preparing the roadmap for incident response is therefore critical. Counsel should consider your incident response processes as a playbook—you need an established playbook that is clearly defined and understood, but which play you run will be based on real-time circumstances. Because if that playbook does not exists—or has not been practiced—when an incident occurs, the results can be severe.

Fundamental Role of In-House Counsel

As noted above, trade secret protection, like cybersecurity, is a team effort, with in-house counsel playing important positions on the team. As with cybersecurity, in-house counsel must provide legal advice and direction on how best to align and prioritize cybersecurity

   ISSN 1538-3423

and trade secret protection practices with legal requirements for the preservation of trade secrets and compliance with other legal areas. For example, the concept of ''reasonable efforts,'' like the elusive concept of ''reasonableness'' for adequate cybersecurity protection, is difficult to define and should be adopted only in conjunction with legal guidance. Any ''reasonable efforts'' must balance the existing case law, current best practices, and a host of other issues such as privacy, employment and human resources issues, and more.

Due to these concerns, counsel should be involved in all stages of program development and implementation. Specific examples of actions in which legal counsel should be involved include: identifying critical assets requiring protection, such as business methods, sales strategies and intellectual property; collaborating on best practices to guard against physical and electronic theft; drafting employment agreements, company policies and confidentiality and non-disclosure agreements for employees, customers, and third parties; implementing trade secret protection training programs for employees; and, coordinating trade secret protection plans and cybersecurity initiatives for compatibility and efficiency. Relatedly, counsel should be involved in responding to any incident of trade secret theft—for example, counsel should evaluate the applicability of legal privileges and manage the internal investigation, evaluate legal remedies and work with outside counsel, if necessary.