PROTECTING TRADE SECRETS WITH AN EFFECTIVE NEED-TO-KNOW POLICY

BY DAVID PRANGE AND ARI B. LUKOFF
CORPORATE COUNSEL
DECEMBER 16, 2016

Common to trade secret protection statutes is the requirement that companies make reasonable efforts under the circumstances to protect information considered a trade secret. The definition of a trade secret relied on by the recently enacted Defend Trade Secrets Act of 2016 (DTSA) is no different. Under the federal definition, information is a trade secret if "the owner thereof has taken reasonable efforts to keep such information secret." It should be expected that a defendant facing a claim of misappropriation of trade secrets may argue the steps a trade secret owner has taken to protect its trade secrets are not reasonable.

The DTSA should provide companies with an incentive to evaluate existing trade secret protection programs, or establish one if no program exists. Trade secret protection programs should use a variety of methods to segregate and prevent unfettered access to sensitive information. One option is to implement a compartmentalization, or need to know, policy for information of this type. Such a policy may reduce the risk of unauthorized access to sensitive information. An implemented policy may also support a claim in litigation that the asserted trade secret is a trade secret. This article discusses several considerations a company should address when implementing a need-to-know information protection policy.

REASONABLE MEASURES NEEDED TO KEEP INFORMATION SECRET

The DTSA (as well as the Uniform Trade Secrets Act and many state implementations) requires that a company should take "reasonable measures" to keep information secret (18 U.S.C. §§ 1839(3)). In litigation, parties defending trade secret misappropriation claims may argue that the trade secret holder did not take reasonable steps to protect the information. "Reasonable" protection measures will depend on individual circumstances and should be a question for the fact finder. Implementing any individual protection measure may improve on an argument that the efforts taken are reasonable.

Building the case that the trade secret owner employed reasonable protections for sensitive information means developing a record of the specific protective measures used by the owner. The type of protective measure and whether it is reasonably suited to keep information safe will depend on the information requiring protection. Protective measures may include ordinary physical security measures like fences and locked cabinets and commonly used electronic security measures like passwords. Another strategy, as referenced above, is compartmentalizing information so only those persons who have a need to know specific information have access to it. This compartmentalization strategy can be an inexpensive but effective way to restrict access and reduce unauthorized dissemination of company trade secrets.

THE NEED-TO-KNOW POLICY

An effective compartmentalization policy for protecting trade secrets may be easier to introduce than to implement. Generally, compartmentalization schemes restrict information access to only those individuals who need the information to perform their job duties. The most difficult decision may be distinguishing those individuals who have a need to know from those who do not, and then addressing potential issues with those who may not agree with

the decisions. Sometimes company managers feel they have a need to know solely by virtue of their position. Longtime engineers may believe they must know the company's technical trade secrets in order to contribute to technical projects.

Similarly, sales leaders may feel they need to know the technical details of a product for which they have responsibility. Making educated choices about what information should be accessible to each company employee may require substantial planning and an understanding of job duties and obligations. Gaining this understanding may require individual interviews or other survey efforts beyond just considering general job responsibilities.

In addition to identifying which employees should have access to trade secret information, a company should consider implementing protocols in order to control actual access to the information. Ideally, the protocol may be reduced to a written document where it may serve the purpose of informing employees of appropriate conduct. The document may also act as a useful exhibit at trial to support an argument that an asserted trade secret has been subjected to reasonable protections. A company should try to identify steps and protocols for recovering restricted information that may be leaked to employees who should not have access to it (or individuals who at one time may have had access to the now-restricted information). Since protection should account for human behavior, companies should consider employee education programs as a tool to implement policy goals. These education programs can also be useful evidence at trial.

As may be expected, identifying who should have access to information may be a difficult process. Here are three considerations to help guide decision-making.

1. CONSIDER EACH EMPLOYEE'S JOB DUTIES.

A foundational question for classifying employee access to information should be whether an individual's immediate job duties require the information. The decision necessarily depends on job type, industry and company culture. For example, engineers involved in product development likely need access to the immediate technological secrets in which they are involved. But engineers may not need to know financial information of the company, or potentially even engineering secrets unrelated to their immediate projects.

Employees tasked with the marketing and sale of company products and services may argue for broader access to sensitive product engineering information to allow for more detailed communication with customers. Caution should be exercised, however, because customer relations also present a greater risk for unintentional disclosure of information during discussions. A better approach to consider is reducing access to only some information, and allowing access by sales employees to a broader portion of information only after an appropriate non disclosure agreement is signed and cataloged for the company. This would help ensure that the salesperson understands the policy and boundaries of what may be disclosed. Thus, a policy can include a process to approve the disclosure of information both to individuals outside the company as well as to company employees.

2. CHOOSE CAREFULLY ON HOW MANY PEOPLE MAY KNOW INFORMATION.

In nearly all but the smallest companies, there should be few situations where a single individual needs to know all of the company's trade secrets. Business managers should be able to manage projects of their product lines without knowing the details of engineering trade secrets. Engineering managers should be able to manage their direct reports without knowing every detail of an engineering process. A company's sales force may not need to know engineering details of how a product is manufactured in order to sell the product.

A policy of compartmentalizing or decentralizing information can sometimes clash with a longstanding culture of allowing individuals to

participate in projects outside their core sphere of expertise. Allowing broad access may promote idea collaboration. While that kind of a policy can work in general, implementing additional restrictions should apply when trade secret information gets used or created. Simply put, a company should be cautious in allowing an overly permissive culture of access to develop. In the hands of a skilled defendant charged with trade secret misappropriation, broad access may also support an argument that the information is not subject to reasonable efforts to maintain secrecy—and may not be a trade secret at all.

Limiting availability of information also reduces the risk of trade secret theft by departing employees. Access to a trade secret based on seniority or experience alone should be avoided. More senior, more experienced employees may be the greatest risk to a company in terms of those who could oversee starting a competitive venture with company trade secrets. Fewer employees with access to all or substantially all company trade secrets translates to a lower possibility that enough secrets could be taken to build a competing enterprise or product.

Still, an access policy that is too restrictive may stifle innovation. The law requires reasonable efforts to maintain confidentiality, and companies should strive to implement a policy that balances a company's culture while still restricting dissemination.

3. RECOGNIZE THAT AN EMPLOYEE'S ACCESS TO THIRD-PARTY TRADE SECRETS COULD RESTRICT WORK ON FUTURE PROJECTS.

Beyond supporting an argument that a company took reasonable efforts to maintain the secrecy of information, a compartmentalization policy can also help to prevent commingling of third-party information with a company's own information. When a company has possession of a third party's trade secret (whether through a joint venture, a license, a negotiation or another circumstance), the company should recognize that it may not have permission to use the third party's trade secrets for the company's own, independent development. In such a circumstance, an employee who had previously accessed the third party's trade secrets may be precluded from working on future internal development projects because it could be impossible to distinguish the third party's trade secrets from the company's own information.

An effectively established need-to-know policy can help reduce these risks in two ways. First, companies should consider placing more restrictions on employees whose responsibilities include business development, partnerships and acquisitions. Individuals in these roles may have greater exposure to other companies' information when evaluating candidate partner companies. Reducing employees' exposure to internal trade secrets, particularly those relating to technology, can reduce the commingling risk. Second, companies can use a need to know employee list as a way to spot where a direct conflict may arise based on known company information and potential information originating from outside the company. It may also help a company allay concerns that commingling has occurred.

THE BOTTOM LINE

Information compartmentalization or need-to-know policies can be inexpensive but effect trade secret protection tools when correctly executed. They require foresight and regulation, however. If a need-to-know policy is not currently in place, companies should reassess the reasons why not, and consider when and how its use can help preserve the competitive advantage of a company's trade secret intellectual property.
