The current trade secret conundrum: the cart before the horse

By R. Mark Halligan, Esq., FisherBroyles, LLP

JULY 6, 2021

Recent studies show that over 80 percent of senior executives recognize that trade secrets are critical and essential to their businesses. Fifty percent of these senior executives say that trade secrets were more important than their patents and trademarks.

Even more (69%) say they foresee trade secret protection becoming more critical than safeguarding other types of intellectual property because of the rapid and furious pace of innovation. Over 60 percent of these senior executives say that protecting trade secret assets is a board-level issue. Nearly one-third of the respondents ranked the protection of trade secret assets a top-five concern.

So why is there a disconnect between the recognition of the importance of trade secret assets and the failure of companies to manage trade secret assets? The answer lies in understanding the various stages of trade secret asset management.

There are four stages of trade secret asset management: identification, classification, protection and valuation. The four stages cannot be juggled around. Identification precedes classification; identification and classification precede protection; identification, classification and protection precede valuation.

The problem lies in the starting point for trade secret asset management. Virtually everyone starts at the third stage — protection — with policies, practices, and procedures and a labyrinth of physical, contractual and technical requirements for "protecting" trade secret assets before the identification and classification of specific trade secrets. Without the identification and classification of trade secret assets before security measures are implemented, the protection measures are doomed to fail—you cannot protect "IT" if you do not know what "IT" is.

A recent study by the Economist Intelligence Unit (EIU) which is the research arm of The Economist Group, publisher of the Economist, illustrates the trade secret conundrum. The EIU surveyed 314 senior corporate executives based in six countries: China, France, Germany, Singapore, the United Kingdom and the United States from six sectors of the economy: Consumer Goods and Retail; Finance; Energy and Natural Resources; Life Sciences; Manufacturing and Technology; Technology, Media and Telecommunications. The interviews were conducted in January and February 2021.

Top threats to trade secrets were ranked by senior corporate executives: weaknesses in cybersecurity (49%); employee leaks (48%) competitive intelligence (27%); third-party service provider risks (26%); corporate espionage (24%).

The senior executives were then asked which of these practices would be most effective in preventing potential threats to trade secrets: installing computer safeguarding and cybersecurity software (53%); confidentiality agreements and policies (46%); restricting digital and physical access to documents (42%); introducing a culture with incentives for trade secret protection (31%); avoiding cloud storage of important trade secrets (27%).

These security protocols have been available for years, but these practices put the cart before the horse. This is the current trade secret conundrum. Companies keep adding more security measures to the organization, but economic espionage and trade secret theft continue to increase unabated.

Companies recognize the importance of trade secret assets, but companies do not focus on trade secret identification and classification of trade secrets assets before implementation of security measures not reasonably tailored to protect the specific trade secrets. There is no audit trail, no ownership, no documentation.

In the EIU study, 13% of the senior corporate executives identified the failure of the organization to categorize intangible assets as a significant threat to the security of the organization's trade secrets.

In addition, 22% of the senior executives responded that one of the biggest obstacles to safeguarding trade secrets is "difficulty in defining trade secrets" and 28% that identified a "lack of in-house experience or awareness about trade secrets" as a major impediment to protecting trade secrets.

These are alarming findings especially when one considers the damages caused by trade secret misappropriation. The senior executives identified these consequences of trade secret theft to the organization: loss of business (52%); loss of competitive advantage (51%); reputational damage (42%); disruption to operations (37%); legal costs (33%); decreased incentives to innovate (22%).

What should be the next step? The organization should focus on the identification and classification of trade secret assets before security measures not tethered to specific trade secrets. There should be

an internal Trade Secrets Committee and/or a trade secret czar responsible for the identification and classification of trade secret assets.

Trade secret assets must be identified and classified. All trade secrets are not created the same. The economic value and security risks vary. The basic "go/no-go" test requires proof that: the information is not generally known in the trade; it is not readily ascertainable by proper means; reasonable measures have been taken to protect the information; and the trade secret owner derives independent economic value from the secrecy of the information.

Courts (and juries) examine the six common law factors derived from Section 757 of the Restatement (First) of Torts to adjudicate whether a piece of information qualifies as a trade secret.

The six factors are:

> Factor 1: The extent to which information is known outside the company (the more extensively the information is known outside the company, the less likely that it is a protectable trade secret).
>
> Factor 2: The extent to which the information is known by employees and others involved in the company (the greater the number of employees who know the information, the less likely that it is a protectable trade secret).
>
> Factor 3: The extent of measures taken by the company to guard the secrecy of the information (the greater the security measures, the more likely that it is a protectable trade secret).
>
> Factor 4: The value of the information to the company and competitors (the greater the value of the information to the company and its competitors, the more likely that it is a protectable trade secret).
>
> Factor 5: The amount of time, effort and money expended by the company in developing the information (the more time, effort and money expended in developing the information, the more likely that it is a protectable trade secret).
>
> Factor 6: The ease of difficulty with which the information could be properly acquired or duplicated by others (the easier it is to duplicate the information, the less likely that it is a protectable trade secret).

The six-factor test has stood the test of time approaching 200 years since the American Law Institute identified the six factors in 1939 (based on a review of case law going back to 1837).

Today, the six-factor test has become the litmus test for state and federal courts to assess whether an alleged piece of information qualifies as a statutory trade secret asset.

The six-factor test is now a standard jury instruction in trade secret misappropriation cases. Appellate courts have reversed trial courts that adjudicate trade secret cases without applying the six-factor litmus test to evaluate the evidence.

Trade secrets are intangible intellectual property assets that impart substantial economic value because they provide a proprietary competitive advantage derived from the secrecy of the information.

There is no public registration system for trade secret assets so an organization must develop an internal trade secret asset management system to identify and classify trade secret assets. Embarking on efforts to implement security or "cybersecurity" measures before trade secret assets are identified and classified are doomed to fail because you cannot protect "it" if you do not know what "it" is that is being protected.

Using the six-factor test to pre-identify and pre-classify trade secret assets before litigation is the key to successful trade secret asset management. Reasonable measures to protect trade secret assets can now be successfully tailored to protect specific trade secret assets and ensure success in trade secret litigation.

About the author

R. Mark Halligan is a partner at **FisherBroyles, LLP** and is based in Chicago. He focuses his practice on intellectual property litigation and is recognized as a leading practitioner in the development of automated trade secret asset management blockchain systems. He has taught Advanced Trade Secrets Law in the LLM program at UIC John Marshall Law School for the past 26 years and is the lead author of the "Defend Trade Secrets Act Handbook," 3rd Edition, just published by Wolters Kluwer. He can be reached at rmark.halligan@fisherbroyles.com.

This article was first published on Reuters Legal News and Westlaw Today on July 6, 2021.