Trade Secrets 101

FOCUS ON: ENGINEERING MANAGEMENT

There are advantages to protecting intellectual property by keeping it under wraps. But there are some things you just can't keep from getting out.

by Kirk Teska

Probably nothing in the law breeds as many myths as trade secrets. One positive aspect of trade secrets is that they can protect things patents cannot, since the general definition of a trade secret is any information that is in some way valuable, provided that reasonable efforts are used to maintain the secret.

There is no requirement that the secret be inventive or unobvious as there is for patents. And, a compilation of data, an equation, or customer list, which are not eligible for either copyright or patent protection, could indeed be the subject of a trade secret.

Trade secret protection can also last indefinitely. Patents, by contrast, expire 20 years after they are filed. Examples of secrets that, had they been patented, would have entered the public domain years ago include the recipe for Coke, the spices in the recipe for Kentucky Fried Chicken, and the formulation of WD-40. Trade secrets also work great for testing and inspection devices and procedures and know-how used in-house.

The problem with trade secrets begins when engineering managers rely on trade secrets without understanding their limits or use trade secrets as a fall-back business decision (for example, because patents are so expensive).

As a thought exercise, suppose you invent a lightsaber (à la Star Wars) and begin selling them in numerous quantities. A competitor buys one of your products, gains an understanding of its overall function, tears into it in order to reverse-engineer the circuitry involved, and begins selling competing lightsabers. You have no patent. Unfortunately, there is no trade secret violation in this scenario because the moment the product was sold, its status as a trade secret ended. No less an authority than the U.S. Supreme Court stated that it is perfectly lawful to "steal" a company's trade secrets by reverse engineering.

You say your secrets are buried deep within the circuitry or computer code of the product? When market share is at issue, businesses will sometimes go to great extremes to learn a competitor's secrets.

The dark side of secrets: Suppose you invent a better lightsaber; any trade secrets inside are open to anyone who can reverse-engineer them.

Consider the case of Nintendo versus Atari. One of Nintendo's early video game players would accept only Nintendo's game cartridges because of a coded message key sent by a chip in the cartridge to the player to "unlock" it. Engineers at Atari (which sought to sell game cartridges that would play on Nintendo's players) chemically peeled the

layers of Nintendo's chip sets to allow microscopic examination of the object code in an effort to figure out the key. And, over the years, it seems that every technological advancement that helps protect chips, integrated circuitry, or software against reverse engineering has been met with a new defeat, tampering scheme, or piracy technology.

Besides ensuring that a secret cannot be defeated by reverse engineering, you also have to take steps to maintain and protect the secret. If the proper steps are not taken, the results can be disastrous. In one case, a company by the name of ConFold designed a reusable shipping container for Polaris's snowmobiles. Polaris and ConFold even signed a non-disclosure agreement, but a court found that it failed to address the design of the shipping container. Since the design was not a trade secret and since it wasn't covered by the agreement, Polaris was free to have someone else manufacture shipping containers according to ConFold's design.

The case of Incase Inc. versus Timex just last year is similar. Incase, a designer of injection molded packaging products, designed a retail display package for Timex's watches. At first, Timex purchased the Incase watch holders, but later Timex started ordering the watch holders from an overseas vendor. Incase sued Timex for misappropriation of trade secrets, but to no avail because Incase failed to take "reasonable steps" to preserve the secrecy of the watch holders: No documents were marked "confidential" or "secret," there were no security precautions or confidentiality agreements, and Incase didn't tell Timex the design was a secret.

"The fact that Incase kept its work for Timex private from the world is not sufficient," the court said. "Discretion is a normal feature of a business relationship. Instead, there must be affirmative steps to preserve the secrecy of the information as against the party against whom the misappropriation claim is made."

STEPS TO TAKE

How, then, does an engineering manager increase the odds that his company's trade secrets will be adequately protected?

Establish a trade secret program. There should be policies and procedures handed down from upper management concerning confidential and sensitive information. Employees should be made to sign employment agreements wherein they acknowledge the company's trade secret policies. When an employee leaves your employment, an "exit interview" is a good idea to remind the ex-employee about the company's trade secret and non-competition policies and agreements. Also, visitors to a company facility should be required to check in and out, and be escorted while on company property.

Finding the key: Atari engineers decoded a chip so their company could make games that would play on Nintendo's game system. It was perfectly legal.

Important information should be handled in a way similar to military or government secrets. The secrets should be documented and locked away. Only key employees with a "need to know" should have access to the secrets. Computer access to key information should also be controlled.

Non-employees to whom any secrets are revealed should be required to sign confidentiality agreements. Even then, limit who is made privy to sensitive information.

Confidential markings should be used when appropriate. If drawings, procedures, specifications, or even PowerPoint presentations contain confidential information, they should include "secret" or "proprietary" legends.

Conduct regular trade secret audits, a mechanism where a trade secret specialist gains an understanding of a company's secrets, ensures that they are sufficiently defined, and that they are adequately protected.

In the end, though, the real key is understanding both the benefits and limitations associated with trade secrets. Rarely do trade secrets work to protect ideas or functions associated with products placed on the open market.

Here is an exam question my law school students regularly get wrong. Suppose, many years ago, Computer Co. invented a software function where text in one document can be highlighted and copied and pasted into another document. Why isn't that a trade secret?

The correct answer is because the minute Computer Co. sells a word processing program with that functionality, it is known to the world. In fact, Computer Co. would likely advertise the copy and paste function. Things that you advertise cannot be trade secrets because, well, they are not secret anymore.

KNOWING THE LIMITS

But, don't go too far and start to think trade secrets have no value. As stated at the outset, trade secrets can protect things patents and copyrights cannot. And, at least one scholar, Karl Jorda of the Franklin Pierce Law Center, deems trade secrets and patents "complementary" and "synergistic."

Finally, understand the limits with trade secrets insofar as employees are concerned. The ability to force employees to sign non-competition agreements is a function of how much a company desires a given prospect. What an employee knows and when he knew it is a factor.

In one famous case, an employee was hired by a company precisely because of his experience with a given technology. When the employee left to begin working at a competitor, the company sued. In the end, a court found that what the employee knew before his employment with the company did not become the company's trade secrets just because he worked there. As for what the employee learned at the company, it is a "well settled rule," said the court, "that an employee upon terminating his employment may carry away and use the general skills or knowledge acquired during the course of employment."

Consider the following hypothetical as a way to summarize trade secret protection contrasted with other forms of intellectual property protection: A company has a new, soon-to-be-released microprocessor-based product. Its functionality is defined in a functional specification, its design is captured in engineering drawings, and the marketing ideas and pricing strategies for the product are explained in a business plan. Before the product is released, everything about it can be protected as trade secrets, including the business plan.

After the product is released, its high-level functionality (what it does) is no longer a trade secret, but could be protected via a patent. Marketing literature and data sheets are also no longer trade secrets because they are usually made public. The engineering drawings can still be considered a secret, but don't forget about the legality of reverse engineering. Finally, both copyright and trade secrets can protect the source code for the software running on the microprocessor.

Kirk Teska is an adjunct professor of law at Suffolk University Law School in Boston, and is the managing partner of Iandiorio Teska & Coleman, an intellectual property law firm in Waltham, Mass. His book, Patent Savvy for Managers, is now available online and at most major bookstores.