

# Trade Secrets: An information security priority

By Steve Luebke

**Theft of intellectual property – trade secrets, patents, copyrights, and trademarks – costs US businesses approximately \$250 billion per year and more than half a million jobs in the US.**

How secure are your company's trade secrets? Theft of intellectual property – trade secrets, patents, copyrights, and trademarks – costs US businesses approximately \$250 billion per year and more than half a million jobs in the US<sup>1</sup>. This means that every day, your organization's competitive edge – your trade secrets – are at risk. As security professionals, it is our duty to inform company leadership on how to identify and protect trade secret materials, processes and information.

Nearly 80 percent of all confidential data loss occurs from employees or insiders<sup>2</sup>. Additionally, a survey conducted by ASIS International and PricewaterhouseCoopers, of Fortune 1000 companies, reported that current and former employees posed a considerable threat to the security of company trade secrets<sup>3</sup>. These internal threats reinforce the need for developing tighter security standards, beginning with the people within your company. Taking proactive steps now to protect your trade secrets can mean the difference between surviving a security breach and closing your doors forever.

## What is a trade secret?

A trade secret is defined as “a formula, process, device or other business information that is kept confidential to maintain an advantage over competitors”<sup>4</sup>. More specifically, the following four elements further characterize a trade secret as: 1) information 2) that derives economic value from the fact that it is a secret, 3) is not generally known to the public, industry competitors, or others that recognize its economic value from its disclosure or use, and 4) is treated as a secret with reasonable efforts taken to protect and maintain its secrecy. More than 40 states have adopted legislation that relies on this or a similar description of a trade secret<sup>5</sup>.

How does a trade secret differ from a patent, trademark or copyright? The most obvious difference is that a trade secret is just that – a secret – and loses its trade secret status once the information is made public. Conversely, patents, copyrights and trademarks are typically public information, whether it is recorded in a government

---

**A trade secret is defined as “a formula, process, device or other business information that is kept confidential to maintain an advantage over competitors.”**

---

office or used as a company's logo. A patent is a registered document that grants an exclusive right to make, use or sell an invention for a specified period of time. A trademark (or service mark) is a mark or name that distinguishes a company's trade product from its competitors. A copyright provides the author of an original work the right to prevent others from using the work without permission.

Although it may not seem advantageous to treat something as a trade secret, there are considerable benefits to doing so. Let's use an example of a recipe, which could either be patented or treated as a trade secret. There are compelling reasons to treat the recipe as a trade secret rather than patent it. Filing a patent application is expensive. Often, companies must obtain patents in multiple countries. Some of these countries are not proactive in protecting the owner's rights, and excessive legal fees may arise in the enforcement of the patent protection. Additionally, patents expire after 14 or 20 years, and every detail of the process then falls into the public domain. In contrast, trade secrets never expire and are not public record. Therefore, a company would benefit by treating the aforementioned recipe as a trade secret rather than filing for patent protection.

1 [http://www.commerce.gov/opa/press/Secretary\\_Gutierrez/2005\\_Releases/September/09-21-05%20IPR%20initiatives.htm](http://www.commerce.gov/opa/press/Secretary_Gutierrez/2005_Releases/September/09-21-05%20IPR%20initiatives.htm)

2 <http://library.findlaw.com/2004/Apr/19/133389.html>

3 <http://www.wcsr.com/default.asp?id=114&objId=43>

4 *Black's Law Dictionary, Second Pocket Edition, 2001*

5 Uniform Trade Secrets Act, 18 U.S.C. § 1(4)

## How to protect your trade secrets

It can be difficult to determine how to label your intellectual property. Therefore, in dealing with intellectual property, assembling a team from various areas of the organization can provide much-needed assistance and expertise. The trade secret team should include the corporate leadership, the corporate attorney, Human Resources and the Chief Security Officer. Together the team identifies intellectual property that belongs to the company and determines how to effectively protect that information by implementing a security policy based on people, process and technology.

Once the trade secret team is established and has identified the company trade secrets or confidential information, the team must then define and implement necessary security policies and procedures. Security policies and procedures can include access controls, marking

---

**A company that employs best practices to protect trade secrets has a greater chance of proving that a piece of information is a trade secret and maintaining trade secret protection.**

---

and labeling confidential information, non-disclosure/non-compete agreements, and exit interviews upon termination of employment. The policies and procedures must be documented, and every employee must read, understand and adhere to the policy. An employee awareness and training program on what the company considers a trade secret will establish a trade secret protection plan. Properly written confidentiality, non-disclosure and non-compete agreements can be the difference between winning a case and losing your trade secret protection.

Upon creating the policies and procedures that will be used to protect trade secrets, the trade secret team can implement and exercise best practices by conducting daily audits of the digital media containing trade secrets as well as spot checks of employees to verify their understanding and observance of the procedures. It is also beneficial to keep a journal of your findings to use as evidence should you have to testify in court. A company that employs best practices to protect trade secrets has a greater chance of proving that a piece of information is a trade secret and maintaining trade secret protection.

For example, Lockheed Martin recently filed a lawsuit against three former employees and a competitor alleging that they took confidential and proprietary business information without Lockheed's authorization. In the suit, Lockheed alleges the three employees conspired with the competitor to win a \$1 billion US Air Force contract. According to Lockheed, the information taken was marked as proprietary, a claim that one defendant disputes. The defendants argue that Lockheed did not have a clear practice for identifying information as proprietary or as a trade secret. The defendants also claim Lockheed failed to set up the appropriate procedures to prevent disclosures of supposed trade secrets by current or departing workers. Although the case is still pending, it has provided companies with a valuable lesson: Clearly identify trade secrets and establish strong security policies and procedures.

In addition to internal audits, an external audit by a legal firm with expertise in intellectual property protection can further support best

practices and the goals of the trade secret team. According to Attorney Paul M. DeCicco, there are six compelling reasons to identify and protect vital information through an audit:

1. An audit provides a current snapshot of your trade secret assets
2. An audit verifies that security policies and procedures are in place and adhered to so as to prevent losing your trade secret protection
3. An audit provides additional legal protections against former employees or competitors that attempt to exploit your trade secrets
4. An audit can be used as evidence of best practices when seeking legal protection of trade secrets
5. A trade secret audit helps avoid misunderstandings and costly litigation by reiterating to current and former employees what information they can and cannot use
6. A trade secret audit can save you money through consistent examination and review of your information assets<sup>6</sup>

In addition to external audits, having a third party conduct regular penetration tests on your computer systems can further prove best practices and potentially avoid internal and external theft of your trade secrets.

## My trade secrets were stolen – now what?

In the event your trade secret is compromised, it is imperative to know the legal protections afforded your company. An aggrieved company can seek an injunction, restitution and punitive damages. However, to successfully obtain an injunction or win in court, three different elements must be documented and proven, or the action to protect the trade secret will fail. You must prove 1) the information was treated as a trade secret; 2) the information is not readily available or generally known to others; and 3) the information has economic value to the owner. Once you have met that burden you must then prove the defendant stole the information. In addition to civil charges, the government may bring criminal charges against the defendant under the Economic Espionage Act and must prove:

1. The information was a trade secret
2. The injured party owned the information
3. The offender stole, or without authorization of the owner, obtained, destroyed or conveyed the information
4. The offender knew the disclosure of the information would injure the owner
5. The offender intended for someone other than the owner to benefit economically
6. The trade secret was related to or was part of a product that was either produced or placed in commerce<sup>7</sup>

Additionally, understanding how to successfully prosecute a trade secret theft is crucial to executing an effective trade secret protection plan. For example, a process controls engineer for Wright Industries, Inc., a Tennessee designer of fabrication equipment, was hired by Gillette to help develop a new shaving system. This new shaving sys-

<sup>6</sup> [http://www.pmdlaw.com/trade\\_secrets\\_primer.htm](http://www.pmdlaw.com/trade_secrets_primer.htm)

<sup>7</sup> Uniform Trade Secrets Act, 18 U.S.C. § 1832

---

## It is our duty to inform company leadership of the risks of failing to properly recognize, label and protect trade secrets.

---

tem project was extremely confidential and treated as such by both Gillette and Wright Industries. The employee, angry with his supervisor and fearful of losing his job, took the project's technical drawings and released them to Gillette's competitors in the razor market, Warner-Lambert Co., BIC, and American Safety Razor Co. These disclosures were made by fax and email. The employee pled guilty and was sentenced to two years and three months in prison for five counts of Theft of Trade Secrets under the Economic Espionage Act of 1996. He was also ordered to pay more than \$1 million in restitution to Gillette and Wright Industries to compensate for the losses incurred<sup>8</sup>.

In a similar case, a defendant was sued for releasing price lists and customer information upon accepting employment with a competitor. The former employer argued that the information was a trade secret and that the defendant violated the agreement not to compete or disclose customer information or price lists by accepting employment with the competitor and releasing the information. However, the defendant argued that the information was not treated as a trade secret and that the non-compete agreement did not apply because he

was not terminated for "just cause" as was required per the agreement. The court held that the defendant did not violate terms of the non-compete agreements because the former employer did not terminate the defendant for just cause; therefore the defendant was not bound by the non-compete agreement. Additionally, the court held the information was not a trade secret because the company failed to treat the information as a trade secret and take reasonable measures to secure the information<sup>9</sup>. Like the Lockheed Martin case, this case reiterates the need for properly written employee agreements and a strong security policy.

### Parting thoughts

As security professionals, it is our duty to inform company leadership of the risks of failing to properly recognize, label and protect trade secrets. Creating a trade secret team, developing thorough policies and procedures, conducting regular assessments of your company's security practices, and understanding your legal rights will ensure that your company is following best practices to protect your trade secrets. By being proactive, you can be the catalyst for positive change and elevate your company's chance of success.

### About the Author

*Steve Luebke is CEO of Senteras, which provides businesses and organizations with information security solutions. He can be reached at [steve.luebke@senteras.com](mailto:luebke@senteras.com).*

<sup>8</sup> *United States v. Davis*, Crim. No. 97-CR-124 (M.D. Tenn. 1997)

<sup>9</sup> *Square D Co. v. Van Handel*, 2005 U.S. Dist. LEXIS 21480 (E.D. Wisc. 2005)