

As Seen in the March 1999 Issue of *Security Management Magazine*

Trade Secret Safeguards

A single federal law now addresses trade secrets, replacing a hodgepodge of state laws. But companies must first implement the right measures to benefit from the law's provisions.

It is often said that we don't appreciate the value of what we have until it's gone. The same could be said of businesses and their trade secrets. To avoid awaking one day to the frightening realization that the business has lost its competitive edge, management must carefully identify, quantify, and protect company trade secrets. Fortunately, the legal framework on which companies can build a case for legal recourse against would-be information thieves has been strengthened in recent years. But to gain the maximum protection from the law, management must understand how the law defines a trade secret and what triggers various provisions.

Intellectual property such as patents, copyrights, and trademarks have long been protected under federal law. But trade secrets were protected only under state laws until Congress passed the Economic Espionage Act (EEA) in 1996. Now, businesses are successfully using a combination of state, federal, and even international laws to fight trade secret theft.

The following overview looks at the four basic steps in trade secret protection: identifying the assets, valuing them, assessing risk, and providing security.

Identification. Before a company can identify its trade secrets, it must understand how they are defined by the law. As defined by the EEA, a trade secret is any form of "financial, business, scientific, technical, economic, or engineering information" that the owner has taken reasonable measures to keep secret. The information must also have eco-

nommic value, either actual or potential, that would be jeopardized were the information to be disclosed. The definition includes all types of information including patterns, compilations, formulas, prototypes, methods, techniques, and procedures, as well as programs and codes. These types of information are protected whether they are stored physically or electronically as graphics, photographs, or text.

Under this definition, information intended for a future promotion can be protected as a trade secret until it is released. Other proprietary information such as a doctor's status report on the president of a company, while confidential, is not considered a trade secret because it has no commercial value.

Most businesses do not realize the importance of determining what proprietary information qualifies as a trade secret. Doing so is a critical first step toward preventing disclosure or, in the event of a theft, readily proving that the company had protections in place.

Companies must also be aware that the identification of trade secrets is a dynamic process and that a company's portfolio of trade secrets changes constantly. Some trade secrets become obsolete, new ones must be added, and others need amending.

Life cycle. The life cycle of a trade secret may be finite or perpetual. If the trade secret is already a product, its trade secret status will last as long as it is not discoverable through reverse engineering—the process of working backwards from

a completed product to the secrets behind it. In *Bonito Boats v. Thunder Craft Boats, Inc.* (United States Supreme Court, 1989) the Court found that a business cannot prevent the reverse engineering of a non-patented product that is sold publicly.

Not all products can be reverse engineered, however. For example, Coca Cola's most important trade secret—a unique combination of ingredients—is unlikely to be discovered through reverse engineering.

Valuation. The EEA requires that a business establish the actual or potential value of trade secret information if it wants to successfully charge someone with the theft of

Before a company can identify its trade secrets, it must understand how they are defined by the law.

those secrets. There are three accepted ways to assign value to a trade secret: the market approach, the cost approach, and the income approach.

The market approach compares the sales price of similar assets to the assets being valued. It can be difficult to use this approach for trade secrets.

The cost approach uses the concept of replacement cost as an indicator of value. It is more well suited to trade secret valuations than the market approach is.

The income approach measures the value of anticipated future economic benefits to be derived from

Court Considerations

Before the EEA, a business could only prosecute trade secret cases at the state level. Remedies were available through the Uniform Trade Secrets Act, which authorized states to pass specific trade secret legislation. Since the EEA has become law, businesses can, for the first time, take civil or criminal action at the federal level.

If a company chooses not to pursue a civil case, it can turn the issue over to the Department of Justice. The government will then criminally prosecute the trade secret theft, resulting in lower costs for the company. However, if the government brings suit, only a limited number of individuals can be included as defendants—unlike in civil cases where the number of defendants is unlimited—reducing the likelihood that the company will recover its losses. And, though judges in criminal cases can fine defendants, the primary purpose of a criminal case is to exact punishment, not recover damages.

Despite these drawbacks, seeking government assistance can be helpful in complex cases. For example, in a recent case, Eastman Kodak enlisted the government's help to catch a retired manager suspected of trafficking in stolen trade secrets.

First, an executive from Kodak and one of the company's security consultants, posing as employees of a phony Chinese company eager to break into the modern film manufacturing business, met with the retired manager and attempted to obtain the proprietary information. The meeting was secretly videotaped. Kodak then took its information to the FBI, and the former manager's home was subsequently searched. The search uncovered a "recipe book" containing all of Kodak's secret formulas for film manufacturing. The suspect was apprehended and later pled guilty to lesser charges as the result of a plea bargain arrangement.

Whether a company takes the civil or criminal legal option, preserving

the confidentiality of trade secrets during court proceedings is easier than it was before the EEA. The EEA states that a federal court shall "...enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets..." in an effort to lessen the threat of disclosure for potential plaintiffs.

In a civil trade secret case, the EEA provides that the court can issue a protective order limiting access to documents and information both at the state and federal level. It can also order certain parts of the record to be sealed, and it can conduct hearings dealing with sensitive issues outside the public courtroom.

The EEA is not specific with regard to criminal proceedings, other than allowing for an immediate appeal by the plaintiffs should the district court direct the disclosure of a trade secret, as occurred in *USA v. Kai-Lo Hsu and Chester S. Ho* (United States Court of Appeals for the Third Circuit, 1998). In that case, three Taiwanese citizens were accused of attempting to illegally obtain the secret recipe for taxol, an anticancer drug. Taxol, which is derived from the Pacific yew tree and is used to treat ovarian and other cancers, had generated sales of \$941 million in 1997.

Ironically, a federal district judge ordered prosecutors to turn over to the defendants' lawyers the very documents the defendants were accused of trying to steal, since the defendants had claimed that these were needed to prepare their defense. Bristol-Myers appealed the decision. The appellate court ruled that Bristol-Myers was not required to turn over the documents.

The three-judge panel agreed that the contents of the documents were irrelevant. Even if the materials contained no confidential information, ruled the court, the defendants were charged with attempting to steal what they thought was proprietary data.

the use of the assets. The cost and income methods are the most common means of valuing trade secrets.

Risk assessment. After valuing each trade secret, the company must determine its vulnerability to theft and anticipate the types of threats that might be encountered. Those in the best position to steal trade secrets include current employees, former employees, vendors and contractors, and joint venture partners. Other groups presenting enormous risks to trade secrets are information brokers, computer hackers, and agents of foreign intelligence services—all of whom are capable of using sophisticated methods to penetrate a company's security measures.

Security. Once the trade secrets have been identified and valued and the risks have been assessed, the company must ensure that adequate safeguards are put in place. Implementation of these security measures may involve training personnel to recognize the importance of trade secrets and the consequences of disclosing that information.

Procedures should also be in place to allow for an ongoing review of policies and procedures. Any significant changes in the risk environment may signify the need to update or modify controls. This step is critical, because inadequate security can make it difficult for the company to prove in court that it took reasonable measures to protect the confidentiality of proprietary information.

In addition to physical measures, the company should ask all parties with access to trade secrets to sign job-specific confidentiality and nondisclosure agreements. (The company should, of course, consult an attorney to ensure that these documents are drafted so as to have the force of law.)

The case of *IDS Life Insurance Company v. SunAmerica, Inc.* (U.S. District Court for the Northern District of Illinois, Eastern Division, 1997) illustrates how these documents can help a company protect its trade secrets. In this instance, the plaintiff, an insurance company, claimed that its sales agents were being induced to quit and join SunAmerica. Agents were also urged, said IDS, to sell SunAmerica products to the same customers they had serviced while at IDS. Furthermore, IDS claimed that this action

had destroyed thousands of its long-term customer relationships and caused sales agents to misuse IDS's its confidential and trade secret information, resulting in the loss of millions of dollars.

IDS claimed that it had spent millions of dollars developing confidential customer information and that the company had taken reasonable measures to preserve the confidentiality of the data by requiring their agents sign noncompete contracts. The contracts included the covenant prohibiting their agents from soliciting or selling insurance or securities products in the territories in which they had worked for one year after leaving IDS.

The plaintiff told the court that it had further attempted to ensure its trade secret confidentiality by including a clause in its nondisclosure contracts requiring that employees maintain the confidentiality of such information and return that information upon leaving the company.

The court ruled that these contracts were valid and that the one-year limitation on sales to former clients and the restrictions placed on the use of confidential and trade secret information did not unduly restrict former employees from earning a living.

IDS successfully argued that it was entitled to receive trade secrets protection for the customer lists. The defendants were directed to turn over all trade secret information, including the customer lists, obtained in violation of the noncompete agreement.

Conversely, the lack of proper policies caused the prosecuting company

to lose in *Hoffman-LaRoche, Inc. v Frank W. Yoder* (Southern District of Ohio, 1997). During the early 1980s, Yoder, a clinical investigator for the pharmaceutical company Hoffman-La Roche, obtained 550 pages of documents pertaining to Acutane, a medication being used for the treatment of acne and related skin disorders. This information consisted of protocols for clinical trials, investigative drug brochures, and correspondence between Hoffman-La Roche and Yoder.

The company alleged that Yoder later tried to sell this information, advertising a minimum bid of \$9.5 million. In February 1996, Hoffman-La Roche filed suit against Yoder seeking an injunction to prevent him from selling or disseminating what it termed "highly proprietary, confidential, and trade secret information" that he had received while serving as a clinical investigator for Hoffman-La Roche.

The court ruled against the company, finding that it had not taken the proper measures to protect its alleged trade secret information. For instance, the company had not insisted that Yoder sign a written confidentiality agreement. Of the 550 pages of data, only three were marked confidential. Also, the information contained in these documents had been given to nineteen research centers nationwide that were involved with Acutane trial testing.

The court ultimately determined that Hoffman-La Roche did not have a formal policy for retrieving the testing information. It was also discovered

that the company lacked adequate internal and external document controls and that the documents in question had not been locked away for safekeeping.

Whatever a company's stock in trade, its competitive advantage is sure to rest at least in part on trade secrets. By identifying, valuing, and properly protecting these information assets, management can go a long way toward securing both their confidentiality and the company's legal recourse if the intellectual goods get into the wrong hands. ■

Dr. Edwin Fraumann is senior manager of New York City-based Deloitte & Touche's forensic and corporate investigative services group. Prior to joining Deloitte & Touche, he served twenty-seven years with the FBI. Fraumann currently specializes in forensic and corporate investigations and intellectual property. He has also taught criminal justice and public management graduate courses at the John Jay College of Criminal Justice in New York City. Dr. Joseph Koletar is director of Deloitte & Touche's forensic and corporate investigative services group. He served twenty-five years with the FBI prior to joining the firm. He has also taught graduate courses at the John Jay College of Criminal Justice.

Deloitte & Touche LLP

DISPUTE AND LITIGATION CONSULTING SERVICES

Two World Financial Center
New York, NY 10281-1414
Telephone: (212) 436-3046
Facsimile: (212) 436-5989

For more information contact:

Ted Fraumann

efraumann@dtus.com