IEEE ENGINEERING MANAGEMENT REVIEW

Volume 36 • Number 3
Third Quarter 2008

Competitive Intelligence

Editor: Wade H. Shaw
College of Engineering
Florida Institute of Technology

RECEIVED
SEP 11 2008
HETERICK MEMORIAL LIBRARY
OHIO NORTHERN UNIVERSITY

301 092008 22152694 0007005
OHIO NORTHERN UNIV 0059
OHIO NORTHERN UNIVERSITY
HETERICK MEMORIAL LIBRARY
525 S MAIN ST UNIT 1
ADA OH 45810-1541 002503

IEEE

IEEE Technology Management Council

TMC publishes the *IEEE Engineering Management Review*, and the *IEEE Transactions on Engineering Management*. *The Review*, published since 1973, reprints from other publications significant articles and selected original materials related to professional practice. The *Transactions*, published since 1954, documents the original contributions that are being made to advance the theory and practice of engineering management. These publications, are provided to all TMC subscribers without additional charge. TMC also underwrites and sponsors conferences, educational products, books, and chapter activities of interest to its members.

Board of Governors

Gerard H. Gaynor
President
g.gaynor@ieee.org

TBA
President-Elect

Irving Engelson
VP, Operations
i.engelson@ieee.org

Louis A. Luceri
Treasurer
l.a.luceri@ieee.org

Tarriq S. Durrani
Past-President
tdurrani@ieee.org

Leslie Martinich
VP, Publications
lmartinich@ieee.org

Charles P. Rubenstein
VP, Conferences
c.rubenstien@ieee.org

Mary Reidy
Secretary
mary.reidy@us.ngrid.com

Governors at Large

Ram Gupta—Aerospace and Electronic Systems Society • **William Hayes**—Broadcast Technology Society

Tuna B. Tarim—Circuits & Systems Society • **Celia Desmond**—Communications Society

Chris Schober —Computer Society • **Jeffrey J. Welser**—Electron Devices Society

Michael W. Condry—Industrial Electronics Society • **Milton Chang** —Lasers and Electro-Optics Society

Luke Maki—Professional Communications Society • **Sam Keene**—Reliability Society

Jennifer Q. Telewicz—Signal Processing Society • **Rakesh Kumar**—Solid State Circuits Society

Wil A. H. Thissen—Systems Man and Cybernetics Society • **Dennis Bodson**—Vehicular Technology Society

Honorary Life Members

M. W. Buckley • **V. A . Carr** • **G. H. Gaynor** • **A. Goldsmith**

T.H. Grim • **C. P. Rubenstein** • **W. H. Shaw**

Ex-Officio

I. Engelson —Division VI Director • **M. Ward-Callan**—Managing Director Technical Activities

G. F. Farris—Editor Transactions on Engineering Management • **W. H. Shaw**—Editor Engineering Management Review

Editors

George F. Farris
Editor—*Transactions on Engineering Management*
ieeetem@business.rutgers.edu

Wade H. Shaw
Editor—*Engineering Management Review*
w.shaw@ieee.org

Subscriptions? **Membership?** **Problems?**

U.S. and Canada: +1 800 678 4333 Elsewhere: +1 732 981 0060

Email: member.services@ieee.org

Address Changes: +1 732 981 9667 (fax), address.change@ieee.org (e-mail)

This material may be protected by Copyright law (Title 17 U.S. Code)

Trade Secrets: A Legal Update

—KURT KAPPES
Seyfarth Shaw LLP

—MICHAEL WEXLER
Seyfarth Shaw LLP

COMPETITIVE INTELLIGENCE MAGAZINE by Kurt Kappes, Michael Wexler, Seyfarth Shaw. Copyright 2008 by Society of Competitive Intelligence Professionals. Reproduced with permission of Society of Competitive Intelligence Professionals in the format Magazine via Copyright Clearance Center.

COMPETITIVE intelligence is a necessary business function for any competitive business. It involves gathering and analyzing information about competitors through legitimate and ethical means. The need to protect and respect proprietary information that has risen to the level of a trade secret has become increasingly important.

This article describes factors that determine the existence of a trade secret. It also offers guidance in protecting trade secrets, detecting culprits, and discussing possible remedies if your trade secrets become misappropriated. Most important, this article provides instructions on how to avoid misappropriating trade secrets and emphasizes that whenever questions arise regarding proprietary information, you should refer them to your legal counsel.

WHAT IS A TRADE SECRET?

In 2003, the Seventh Circuit Court of Appeals declared that a trade secret "is one of the most elusive and difficult concepts in the law to define." (See *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714 (7th Cir. 2003).) Nevertheless, 45 states have adopted at least some version of the Uniform Trade Secrets Act, which gives substance to the term. The Act describes a trade secret as information, including a formula, pattern, compilation, program, device, method, technique, or process that meets the following criteria:

- It derives independent economic value, actual or potential.
- It is not generally known to and not readily ascertainable by proper means.
- Others can obtain economic value from its disclosure or use.
- It is the subject of efforts that are reasonable under the circumstances to maintain its secrecy (see, e.g., Cal. Civ. Code § 3426.1).

HOW DO I KNOW IF INFORMATION IS A TRADE SECRET?

The existence of a trade secret depends on several factors, including the following:

- The extent to which the information is known outside the company's business.
- The extent to which it is known to employees and others involved in the company's business.
- The extent of the measures taken by the company to guard the secrecy of the information.
- The value of the information to the company and to its competitors.
- The amount of effort or money expended by the company to develop the information.
- The ease or difficulty others would have to properly acquire or duplicate the information.

PROTECTING TRADE SECRETS: WHO?

Once you have identified a trade secret, the next step is to sufficiently protect it. The main concern is the possibility

that former employees, foreign competitors, on-site contractors, and domestic competitors will leak your trade secrets. Secondary concerns for leaks include computer hackers, vendors, suppliers, and current employees.

You often disclose trade secrets in a business setting. Trade secrets, however, are also exposed through the course of mundane activities such as in a dinner conversation, during an airplane trip, or simply through an overheard cell phone conversation.

How Are Trade Secrets Misappropriated?

A starting point to guarding proprietary information is identifying individuals and the means by which they could misappropriate trade secrets. Additionally, you need to know what information they generally seek. These individuals often target customer lists and related data, strategic plans and road maps, financial data, and research and development information. They often obtain secrets by copying documents, downloading information from computers, gathering e-mail information, and memorizing information. Pay attention to these cues and have a system to report suspicious activities to your human resources department, your supervisors, or other appropriate personnel.

Four Steps to Protect Trade Secrets and Confidential Information

Competitive intelligence practitioners need to be aware of the problem of trade secret misappropriation. As discussed above, by identifying your trade secrets, the individuals who are likely to seek them, and their strategies, you are already headed in the right direction. You should also be alert to indicators of suspicious activities such as the ones listed above.

Educate your employees about trade secret protection and provide instructions on how to report possible trade secret violation. Finally, implement a four-step program:

- Draft contracts that identify your trade secrets and that plainly state that you intend to enforce your rights.
- Develop and disseminate personnel policies and procedures.
- Conduct periodic trade secret and confidential information audits for employees at all levels.
- Enforce your rights to enjoin others from using your trade secrets, and provide appropriate remedies for misappropriation.

By following these steps, you can maintain a level of comfort that your proprietary information will remain respected and protected. Any uncertainties with respect to protecting trade secrets and confidential information should be directed to your counsel.

Competitive Intelligence Concerns

Your proprietary information concerns as a competitive intelligence (CI) practitioner are twofold. On one hand, you want to ensure that your proprietary information is protected as your competitors implement and execute their own competitive intelligence process. On the other hand, you want to be careful not to misappropriate your competitors' proprietary information as you execute your own competitive intelligence process.

The first step in the intelligence process is gathering facts on common competitors from many sources. Primary sources include industry observers such as journalists and industry and stock analysts, and industry participants such as suppliers, customers, and consultants.

The first step in the intelligence process is gathering facts on common competitors from many sources.

Trade shows are also a primary source for fact gathering. There, common competitors and employees provide an ideal and open opportunity to gain insight into competitor strategies, plans, intentions, and changes. From information obtained at these venues, you can begin analyzing intelligence to determine the competitive situation, make predictions about common competitors, determine how the competitors are similar or dissimilar to your business, and provide recommendations to surpass the competition.

Avoiding Misappropriation Claims: The Pepsi-Coke Story

On July 4, 2006, the Federal Bureau of Investigation (FBI) arrested a Coca-Cola employee and two codefendants for conspiring to steal and solicit Coca-Cola's trade secrets. The defendants wrote a letter to Pepsi agreeing to provide Pepsi with information regarding Coca-Cola's new product and product packaging in exchange for more than a million dollars. After receiving the offer, Pepsi notified the FBI, which led to the

arrest and later the conviction of the conspirators. The Pepsi-Coke story demonstrates the proper ethical standard to follow regarding misappropriated trade secrets.

The Pepsi-Coke story provides us with a clear example of how trade secrets can become misappropriated, but the line between competitive intelligence and corporate espionage and fraud is not always so bright. Therefore, refer to counsel whenever there is any doubt if uncovered intelligence has risen to the level of a trade secret and could potentially be wrongfully misappropriated. Many companies have also adopted codes of conduct that provide useful guidance. guidance of this nature should perform the following functions:

- Outline the company's trade secret information and the steps that will be taken to protect it.
- Instruct employees not to use or share trade secrets obtained from others.

Avoiding Misappropriation Claims: Hiring Policies and Procedures

Competitors' former employees can be a source of competitive intelligence. When your company hires new employees at any level, make sure that they know they should honor their former employers' trade secret disclosure agreements. Your employment agreements should require employees to represent that they do not have any trade secrets or confidential information from their previous employer. It should also remind them that they are expected to honor their former employers' disclosure agreements, as well as those of your company. The agreement should provide that the company will discipline an employee who fails to abide by such agreements, including termination as appropriate.

If there is any uncertainty over proper disclosure agreements, again consult counsel promptly. You may wish to work with counsel beforehand to identify trade secrets and ways to avoid misappropriation. The more guidelines and examples you have available, the less you will need to confer with counsel. You can then consult counsel for the more extraordinary situations. Employees should be trained not to ask during the interview process for trade secrets.

Remedies When Your Information Is Misappropriated

If you discover that your trade secrets or confidential information have been misappropriated, civil and criminal actions are possible. These remedies are available under a wide array of laws, including the Uniform Trade Secrets Act, the Computer Fraud and Abuse Act, the Economic Espionage Act, and state criminal laws such as the larceny statutes. (See for example Computer Fraud and Abuse Act, 18 U.S.C. §1030.)

Congress passed the Computer Fraud and Abuse Act in 1984 and expanded it in 1996. Any person who intentionally accesses a computer without authorization or exceeds his or her authorized access on a protected computer violates this act. The act allows for a right of action in federal court and does not limit claims to trade secrets.

Additionally, in 1996, Congress passed the Economic Espionage Act. The act criminalizes an attempt or conspiracy to steal trade secrets. The act protects trade secrets if the owner has taken reasonable measures to keep them secret. It also requires that the information have independent economic value and that the information not be generally known. Penalties for violating the act include imprisonment for up to 15 years and a fine up to $500,000. Moreover, corporations can be fined up to $10 million under the act.

The Economic Espionage Act can affect a company in two ways. The act can be used as a weapon to protect trade secrets, with the penalties as an effective deterrent. However, the act can expose a company to new liabilities through the actions of its employees. Therefore, as competitive intelligence practitioners, you should familiarize your employees with the act and stress that the company seeks to comply with both the legal restrictions of the Economic Espionage Act as well as the ethical considerations involved.

Enforce! Enforce! Enforce!

Protecting your trade secrets and avoiding misappropriation claims are a vital component to your success as a competitive business practitioner. Be sure to identify and consult regularly with your corporate security personnel. Familiarize your company and employees with guidance on how to detect a trade secret, how to protect it, and which ethical implications to consider when provided with a competitor's proprietary intelligence. You can refer to legal counsel whenever there is any uncertainty, but having basic policies in place is key.

[Author's note: Courtney Vasquez provided valuable assistance in preparing this article.]

REFERENCES

Cal. Civ. Code § 3426.1
Computer Fraud and Abuse Act, 18 U.S.C. §1030
Learning Curve Toys, Inc. v. PlayWood Toys, Inc., 342 F.3d 714 (7th Cir. 2003)

Kurt A. Kappes is a partner in the Seyfarth Shaw LLP Sacramento office, and has extensive trial and pretrial experiences in a variety of commercial litigation matters, including trade secrets, Sarbanes-Oxley Act proceedings, and unfair competition litigation. He has a BA from Butler University and a JD from Northwestern University School of Law. Kurt can be reached at kkappes@seyfarth.com.

Michael D. Wexler is a partner in the Seyfarth Shaw LLP Chicago office and is national chair of the firm's corporate espionage, trade secrets, and unfair competition group. A former state prosecutor, he focuses on trial work and counseling in the areas of trade secrets and restrictive covenants, corporate espionage, and intellectual property infringement in both federal and state courts. Michael has a BA from the University of Illinois and a JD from IIT Chicago Kent College of Law. He can be reached at mwexler@seyfarth.com.