



Book Review

TRADE SECRET ASSET MANAGEMENT

BY KARL F. JORDA

A GEM OF A BOOK SAW THE LIGHT OF DAY RECENTLY. It is titled *Trade Secret Asset Management—An Executive's Guide to Information Asset Management, Including Sarbanes-Oxley Accounting Requirements for Trade Secrets*. It was published by Aspatore Books and was authored by R. Mark Halligan and Richard F. Weyand. Mr. Weyand is the President of the Trade Secret Office, which is developing management methods and software for the automated discovery, inventory and valuation of trade secrets. Mr. Halligan, a partner in the Chicago office of Lovells LLP, teaches "Advanced Trade Secret Law" as well as "Trade Secret Litigation" at John Marshall Law School, has a data base of over 700 trade secret decisions and is recognized as the country's leading expert in trade secret law, the Economic Espionage Act of 1996 (EEA) as well as the application of the Sarbanes-Oxley Act of 2002 to trade secrets.

The book's small size of 8-1/2 by 5-1/2 inches and only 150 pages of text belies its importance for the management of corporate trade secrets. As the subtitle indicates it is a guide for executives. As such it is refreshingly hands-on and non-legalistic without authorities or citations and without footnotes or endnotes. And it uses plain and straightforward language with an executive summary at the beginning and a summation at the end of each chapter.

After breezing through the basics of trade secret law in Chapter 1 through 4 on what trade secrets are and how they are defended and lost, the authors focus in great detail on the "all-important" security and accounting issues in the remaining chapters, Chapters 5 through 15. These discussions are impactful and trailblazing.

The book then concludes with 92 pages of useful appendices, consisting of

- the Uniform Trade Secrets Act, the Economic Espionage Act, the Computer Fraud and Abuse Act and excerpts from the Sarbanes-Oxley Act;
- four important exemplary trade secret cases, in one of which Judge Posner extols the importance of trade secrets to the economy;
- a checklist of potential trade secrets; and
- samples of a non-disclosure and confidentiality agreement and an employee trade secret exit interview form.

In Chapter 2, which deals with the nature and importance of trade secrets, the authors state that

"the vast bulk of the value of (a corporation's) intangible assets is comprised of the company's trade secrets, not of its goodwill, branding, or other intangible assets. Trade secrets are what allowed Goggle to come out of nowhere to dominate the search engine business over competitive search technologies from companies with established goodwill and branding like Yahoo!, AOL, and Microsoft. It is the trade secrets that drove their success, which in turn drove their goodwill and branding, not the other way round."

In this chapter, they also quote FBI Director, Robert S. Mueller III as claiming in a speech in 2003 that "as much as \$200 billion is annually lost to economic espionage." What's more, in Chapter 14 on "Trade Secrets Sarbanes-Oxley," they relate that the 2004 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage reported that

"individuals from both the private and public sectors of almost 100 foreign countries engaged in efforts to obtain unauthorized access to trade secret assets in the United

See EDITOR, page 2

■ EDITOR, from page 1

States in fiscal year 2004. It is currently estimated that trade secret losses exceed \$300 billion per year.”

The authors then conclude that the “company’s trade secrets are at risk of theft, this risk is large and growing, and most companies are insufficiently aware of or prepared to deal with this risk.” Given the dominance of trade secrets and the prevalence of trade secret theft, it is deplorable that most companies have no trade secret policies in place, when “trade secret protection (should) be front and center of every company’s risk management program.” Hence, their extraordinary emphasis in the six ensuing chapters on security measures, which of course are requisite as a matter of law anyway for safeguarding the trade secret status of all proprietary information and know-how.

Thus, the heart of this trade secret book is the detailed discussion in six chapters of security; namely, security against outsiders, security against insiders, inbound security and establishment and monitoring of a trade secret culture. According to the authors, the importance of security measures to maintain “the company’s trade secret property rights in its information cannot be overemphasized.” Security lapses, that is, failures to take reasonable measures to maintain secrecy, are the most common stumbling blocks in trade secret litigation. Besides, such failures can result in the loss of trade secrets, “even if the actual access to the information was proper and not due to any lapse in security measures.”

In Chapter 6 on security against outsiders, the authors discuss first of all outside access by proper means and warn against:

- careless, inadvertent and unprotected disclosures in trade shows, conference speeches, sales calls, customer visits, employment or media interviews, etc.;
- discussion of proprietary information in public places—“loose lips sink ships”;
- errors in transmission—“Proprietary & Confidential” legends should be prominent; and
- careless disposal of materials containing proprietary information—“waste paper

archeology” being a favorite technique for going after trade secrets.

Next, under the heading “Outsider Access by Improper Means,” access by fraud, trespass, theft, hacking and through inducement of breach, are gone over and the suggestions are made to:

- chaperone outsiders by an employee at all times,
- break up sensitive information and store it in different places;
- screen employees carefully when hiring or promoting;
- limiting the use of paper documents and encrypting sensitive files on computers and;
- above all, establish a zero tolerance policy and employ a so-called “red team attack” by “retaining outside competitive intelligence specialists to see if they can penetrate the company’s security systems “by discovering and exploiting the company’s weakest links.”

Chapter 7 then deals with “Security Against Insiders.” The authors note that insider theft is the most common source of information loss, due to high employee turnover. It can be lessened through compartmentalization of information and access controls (need to know) as well as careful management of employee agreements and creation of a trade secret culture. Such precautions cause a major dilemma for a company: it must disclose trade secrets to employees but strict policing can be construed as distrust of employees with undesirable consequences on employee morale and loyalty. Practice tips are also made regarding the entrance and exit interviews and the employment agreement. This agreement should be given to a prospective employee prior to offering a position, the employment agreement should be renewed annually—a completely novel suggestion—and the exit interview should include a trade secret segment, in which a statement is signed by the employee affirming his/her abiding trade secret obligations. Contractors, consultants, suppliers and customers rate similar attention.

And Chapter 8 covers “Inbound Security.” A company can be found vicariously liable for trade secret misappropriation, if for example, a new employee, hired from a competitor, discloses competitor’s trade

secrets to the new employer, who uses them without consent. Guarding against importation of trade secrets from others, hence, is also critically important. An “ostrich defense” will not shield a company from liability. Independent development of such trade secrets is then no longer possible.

In Chapter 9, the authors point out that it is “important to proactively monitor the company’s business environment to detect theft of proprietary information so corrective measures can be taken to address the situation before it gets worse.” And the last chapter on “Security,” Chapter 10, contains an exposition on establishing a trade secret culture as more economical and self-sustaining and reinforcing than “stand alone employee training sessions.” This involves unambiguous top-down and effective bottom-up communications.

The next five chapters deal with “Accounting,” including inventorying, classifying, valuating and reporting trade secrets as well as with the topic of “Sarbanes-Oxley and Trade Secrets” and the need for a trade secret holding company. Because there is less awareness of, and attention to, such accounting issues in corporate trade secret policies and practices, these chapters are even more critical and pivotal. Even though inventorying trade secrets is difficult, because a trade secret portfolio is “amorphous, intangible and inchoate,” it is an indispensable first step to classification, valuation and reporting of trade secrets.

Anent classification, I question the authors’ distinctions between “Confidential,” “Secret,” and “Top Secret” secrets, and their call for a “structured regime of security measures and rules of distribution, disclosure, transportation, and access control and tracking that are tailored to the sensitivity of trade secrets of that classification.” In all the decades I have been professionally interested in trade secret law and practice, I have never heard of such a categorization or hierarchization, except in government circles. On the contrary, I have become convinced that when it comes to trade secrets there are no grades or shades of confidentiality and secrecy. It is an either/or matter for trade secrets, just like with

See **EDITOR, page 3**

■ EDITOR, from page 2

pregnancy, and that industry must give their trade secrets and proprietary data the highest classification in order not to jeopardize their legal status. Besides it would be an impossible administrative burden even for big corporations to periodically upgrade or downgrade trade secrets to “remain appropriate to the sensitivity of the trade secret information” throughout the “life cycle” of a trade secret (“from creation, through development, patent election, application, and potential licensing, to obsolescence”). This is suggested and discussed by the authors in their Chapter 13, titled “Life Cycle Management of Trade Secrets.”

In these chapters on “Accounting” the authors also discuss the importance and difficulty of valuation of trade secret assets. Assetization of trade secrets is a critical step for realizing and reporting the full value of a trade secret inventory. Once assetized, trade secrets can be insured against loss and are available as collateral for loans as well as for sale or license to other companies, with the valuation via the discounted cash flow method giving valuable guidance in setting the royalty rates or sale prices.

As regards “Reporting,” the authors suggest that a reporting structure be employed that provides granularity of reporting that will be of value to shareholders and investors without being of value to competitors by reporting them “in large enough aggregate categories and with general enough descriptive labels to obscure the nature of the information.”

Chapter 14 on “Sarbanes-Oxley and Trade Secrets” is truly an eye-opening must-read for management. Mark Halligan has lectured and written extensively and convincingly on the Sarbanes-Oxley Act of 2002 (SOX) (“Public Company Accounting Reform and Investor Protection Act of 2002”) and its impact on corporate trade secret practice. While SOX does not specifically mention trade secret assets nor for that matter any IP assets nor even intangible property, the requirements of SOX transcend any specific asset class and relate to the financial condition of the corporation as a whole. SOX requires adequate internal financial controls, certification by company executives

of the accuracy of financial reports, attestation by the company’s auditors and imposition of criminal penalties to knowing or willful certification of untrue financial reports. Since every company has trade secrets and trade secrets are financial assets, providing by definition economic value and competitive advantage, the value of trade secrets must be reported.

In the final chapter, Chapter 15, under the topic of “Accounting,” they boldly propose separate trade secret holding companies, structured as subsidiaries and profit centers with resources for the effective management of companies’ trade secret portfolios, including the licensing and collateralization and the many requirements of FASB rules and the Sarbanes-Oxley Act.

It is the opinion of the authors that a holding company is even more desirable for trade secret assets, which are less well defined but far more important, than for patents, trademarks and copyrights, for which holding companies have already been used. But because of the close relationship between trade secrets and patents (“every patent begins life as a trade secret”), such holding companies should manage both patents and trade secrets. But given the pervasive general antipathy toward and neglect of trade secrets, I cannot see corporations rush to establish trade secret holding companies or even IP holding companies for patents and trade secrets, especially since IP holding companies have come under IRS scrutiny.

Finally, as mentioned at the outset, the authors include as a relevant appendix the text of the Computer Fraud and Abuse Act of 1984 (CFAA) and in Chapter 6 (Security Against Outsiders) ever so briefly refer to it by stating this:

“Access to the company’s computers by hacking is a criminal violation of the federal Computer Fraud and Abuse Act and often a criminal violation of the federal Economic Espionage Act, and the resulting access to proprietary information is an actionable misappropriation.”

However, at the Annual Meeting in October 2007 of the American Intellectual Property Law Association (AIPLA), Mark

Halligan elaborated in quite some detail on the relevance of the CFAA. In fact, he presented the CFAA as a potentially very effective new club against trade secret misappropriation involving computers, which nowadays is more likely to be the rule rather the exception. And he did this twice: in a plenary meeting in which he reviewed recent trade secret decisions as well as in a meeting of the AIPLA’s Trade Secret Committee, which he chairs.

Indeed, the CFAA appears to be gaining unprecedented cognizance, as corroborated by a Luncheon and CLE Program of the New York Intellectual Property Law Association, held on December 12, 2007 in New York City. The topic fielded expertly by Peter Toren of Kasowitz, Benson, Torres & Friedman, was “Theft of Trade Secrets and the Federal Computer Fraud & Abuse Act.” In addition to covering such issues as civil liability, criminal prosecution, examples of offensive computer uses, jurisdictional requirements, damages and remedies, etc., he also discussed the recent International Airport Centers v. Citrin decision by Judge Posner, which he called a “leading case.”

In this decision Judge Posner ruled that Citrin’s putting the deletion program on his computer constituted a “transmission” of trade secrets and that this transmission destroyed files which Citrin, as a departing employee, had no authorization to delete. Therefore, he was guilty of violating the CFAA. *(A more detailed discussion of this decision will be presented in a future blog at <http://blogs.piercelaw.edu/trade-secrets/>.)*

It is likely that in the future the CFAA will be invoked more often than the EEA. ■

Karl F. Jorda, David Rines Professor of Intellectual Property Law & Industrial Innovation, Director, Kenneth J. Germeshausen Center for the Law of Innovation & Entrepreneurship, Franklin Pierce Law Center, Concord, NH.

