TRADE SECRETS AND CORPORATE GOVERNANCE: BEST PRACTICES

James Pooley
Milbank, Tweed, Hadley & McCloy LLP
3000 El Camino Real, 5 Palo Alto Square
Palo Alto, CA 94306
email: jpooley@milbank.com
(650) 739-7045 tel.
(650) 739-7100 fax

TRADE SECRETS AND CORPORATE GOVERNANCE: BEST PRACTICES

by James Pooley and Katherine Nolan-Stevaux*

INTRODUCTION

No one seriously disputes that information is the primary corporate asset of the twenty-first century. But few seem to recognize that it goes by a legal name, "trade secrets," and that corporate officers and directors face increasingly serious responsibilities to identify and care for it.

If you were to ask an accountant to define a company's intangible property, you might get a vague answer like "goodwill," referring loosely to the difference between a company's hard assets and its value in the marketplace. Pressing further, you might hear a reference to intellectual property, by which the accountant will likely mean patents, copyrights or trademarks. All of these come with government certificates, making their inventory easy and their valuation more or less straightforward.

But the fact is that these federally-defined forms of IP are the distant runners-up in the corporate contest. Survey evidence shows that the vast majority of information assets are protected exclusively by trade secret law, by choice of the companies which own the property.[1] It's not hard to understand why. Trade secrets extend far beyond the coverage of patents, protecting virtually any competitively sensitive data.[2] And securing the legal right is relatively cheap, requires no registration, and is potentially permanent.

Corporations, through their boards and management, are duty bound to take informed action to protect the company's assets; but individual directors and officers can also be liable for

---

 Mr. Pooley is a partner in the Palo Alto office of Milbank, Tweed, Hadley & McCloy LLP, and Dr. Nolan-Stevaux is a third year student at Boalt Hall School of Law. Mr. Pooley's treatise, *Trade Secrets*, is available from Law Journal Press.

[1] Cohen, W.M., R.R. Nelson, and J.P. Walsh, "Protecting Their Intellectual Assets; Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not)", NBER Working Paper 7552 (2000).

[2] See Pooley, *Trade Secrets* (Law Journal Press, updated) §§ 1.01 and 4.02 (hereafter "Trade Secrets").

failing to monitor the company's activities to ensure compliance with the law.[3] Where trade secrets are concerned, it helps to think of management's duty as having two fundamental aspects. First, consider the classical need to conserve the corporation's property from loss through theft or dissipation. We might refer to this as **outbound** protection, since it focuses on control of information leaving the organization. This involves all the traditional security techniques of document classification, visitor access control, network security and the like. Outbound protection is directed at keeping close track of the company's secrets.

The second sort of protection is **inbound**, directed at information belonging to outsiders, information that can infect a company just as a virus infects a person. Here the focus is on hiring employees and consultants (who carry – at least in their heads – valuable information of their former employers) and on external business relationships such as potential licensors or business partners. Inbound controls make sure that others' secrets come into the company only by agreement and in a carefully managed way.

Modern corporate governance is increasingly concerned with addressing both forms of protection. Shareholders rightly want to know what management is doing to expand and exploit the company's information assets, especially in industries where the value of those assets is volatile. But they also want to be sure that management is keeping the company out of trouble, since improper handling of someone else's secrets can lead to lawsuits or even criminal prosecution.[4]

These concerns are not mere abstractions. The last several years have seen profound changes in the regulations applicable to corporations and their management. The most well-

---

[3] See *In re Caremark Int'l Inc. Derivative Litigation*, 698 A.2d 959, 969-970 (Del. Ch. 1996).

[4] Consider Boeing, which lost over a billion dollars in government contracts as a result of theft of information from Lockheed. Criminal exposure comes mainly from the Economic Espionage Act, 18 U.S.C. §§ 1831-1839, which empowers local United States Attorneys to indict corporations and individuals involved in trade secret misappropriation. See *Trade Secrets*, § 13.03.

known (or notorious) of these new requirements is the certification process mandated by the Sarbanes-Oxley Act, which one study estimates has cost U.S. businesses $1.4 trillion.[5] But lurking inside this accounting burden is a significant new obligation to identify and value a company's trade secrets and to institute processes designed to keep it out of trouble for misusing trade secrets of others. This growing imposition on management started in 2001 with the issuance of a new accounting standard, FASB 142, directed at revaluing "intangibles"; Sarbanes-Oxley put a sharper point on the issue in 2002 with the certification requirement; and with the 2004 amendments to the Federal Sentencing Guidelines corporate boards and officers have been told what they need to do to stay out of jail for information theft.

This article describes these new corporate standards and suggests what is likely to be the resulting set of "best practices" that companies will be expected to follow regarding protection of trade secrets (their own and others'). Of course, complying with these new standards will take time and cost money. But the good news is that, properly implemented, a robust protection plan will not only keep you in compliance but should provide substantial returns in efficiency and productive exploitation of the company's intangible assets.

FASB 142: THE NEW REQUIREMENT TO VALUE "INTANGIBLES"

In 2002 the Financial Accounting Standards Board issued a new standard, FASB 142:

> "While goodwill is an intangible asset, the term *intangible assets* is used in this Statement to refer to an intangible asset other than goodwill." (para. 4)
>
> "[A]ll intangible assets shall be aggregated and presented as a separate line item in the statement of financial position." (para. 42)
>
> "An entity shall evaluate the remaining useful life of an intangible asset that is being amortized each reporting period." (para. 14)

[5] Ivy Xiying Zhang, *Economic Consequences of the Sarbanes-Oxley Act of 2002*, cited in *The Economist*, May 21, 2005, p. 71.

FASB 142 reflected a broad consensus among business and accounting professionals that intangible assets are "an increasingly important economic resource."[6] The Board believed that requiring companies to re-evaluate their intangible property annually would lead to financial reporting that better reflects the underlying economics of the organization, including how the value of intangible assets might change in the future. Separating out specific classes of intangibles from the all-inclusive "goodwill" for this annual assessment marks an important change in information management. Appendix A to FASB 142 provides a guide for implementation and lists several forms of intellectual property as examples of intangible assets, including trade secrets.

The bottom line is this: in order to comply with accounting standards, companies must now understand and place a value on their information assets. Operationally, management should implement processes for an inventory and review, sometimes referred to as a "trade secret audit." (See section below on "Compliance Plans")

SARBANES-OXLEY

Legislative reaction to the scandals at Enron and Worldcom led to the Sarbanes-Oxley Act of 2002. Section 906 requires that CEOs and CFOs of public companies personally certify their financial statements, with stiff criminal sanctions for noncompliance. Section 302 directed the SEC to issue rules governing certifications, and pursuant to that authority, the SEC requires that a company's statement address procedures ensuring that the necessary information is collected and communicated to management. Pursuant to § 404, the SEC has issued rules on internal controls and procedures ensuring compliance. Thus, Sarbanes-Oxley as implemented requires that corporations, at the highest level of management, understand and value their intellectual property and report it in an understandable fashion.

[6] Financial Accounting Standards Board, Summary of Statement No. 142, June 2001.

SEARCHING FOR A STANDARD: THE REGULATORS

In addition to the congressionally-mandated regulations issued by the SEC, other rules have been proposed by NASDAQ and the NYSE to improve transparency of the markets and to establish a baseline of ethical behavior. All of these rules require companies to establish a code of ethics, although they differ as to the details of the codes. Nonetheless, these promulgations suggest a minimum standard for behavior – a set of "best practices" in other words – that would comply with Sarbanes-Oxley and FASB 142.

Section 406 of Sarbanes-Oxley directed the SEC to issue a rule requiring companies to adopt a code of ethics for senior financial officers. Under § 406, such rules should set forth standards "reasonably necessary" to promote honest and ethical conduct, including the handling of actual and apparent conflicts of interest, "full, fair, accurate, timely, and understandable disclosure" in the reports required to be filed, and compliance with governmental rules and regulations.

In implementing the rule governing codes of ethics as mandated by § 406, the SEC supplemented the requirements addressed by the code of ethics, which apply for fiscal years ending on or after July 15, 2004.[7] First, the code of ethics applies not only to the senior financial officers but also to the chief executive officer. Second, in addition to promoting proper conduct, the code of ethics must be designed to deter wrongdoing. Toward that goal, the code must designate a person to whom any breaches must be promptly reported. It must also establish accountability for adherence to the code. In order to improve transparency, the code of ethics must be publicly available as an exhibit to the annual report, on the corporation's website, or available free upon request.

[7] 21 C.F.R. § 229.406.

NASD regulations build on the requirements of the ethical code contained in § 406 of Sarbanes-Oxley. Rule 4350(n), effective May 4, 2004, was intended to bolster investor confidence by demonstrating that NASDAQ implemented a system to ensure that companies discover and promptly address any questionable behavior. Under NASD 4350(n), the code of ethics described in § 406 applies to all directors, officers, and employees, and is required to include an enforcement mechanism. However, the rule does not provide examples of what that mechanism might be.

The NYSE code of conduct and ethics, applicable to all companies listed on the exchange, imposes broader responsibilities than either § 406 or the NASD codes of ethics. NYSE 303.A10, effective October 31, 2004, aims "to provide guidance to personnel to help them recognize and deal with ethical issues, provide mechanisms to report unethical conduct, and help to foster a culture of honesty and accountability." Thus, the code of ethics and conduct applies to directors, officers, and all employees, and any waivers of the code must be disclosed. Codes adopted by NYSE-listed companies must address:

- conflicts of interest,
- corporate opportunities,
- confidentiality,
- fair dealing,
- protection and proper use of company assets,
- compliance standards to facilitate the operation of the code, and
- mechanisms to report illegal and unethical behavior.

Rule 303.A10 defines as confidential as "all non-public information that might be of use to competitors, or harmful to the company or its customers, if disclosed." Although this

provision may have been aimed at minimizing insider trading, it also encompasses management's obligations to protect the company's trade secrets ("outbound" protection). Thus, the provision seeks to ensure that opportunities to exploit trade secrets are not wasted. As a result, NYSE-listed companies are now required to take reasonable steps both to protect confidential information and to exploit it for the benefit of the corporation. In this way, the NYSE standards bring corporate governance more deeply and obviously into the realm of intellectual property protection than might be required merely by FASB 142, or by the provisions of Sarbanes-Oxley.

Thus, the securities regulators, as part of their effort to ensure transparency of markets and the integrity of financial reporting, have begun to publish minimum ethical standards for corporate management. These standards recognize that the protection of confidential company property – i.e., trade secrets – should receive specific attention. Codes of conduct and compliance plans satisfying these regulations should help to ensure that companies also comply with the requirements of Sarbanes-Oxley and FASB 142.

FEDERAL SENTENCING GUIDELINES

As noted earlier, management's duty of care extends to inbound information, that is, protecting the corporation against infection by trade secrets belonging to others. This is not merely an issue of avoiding civil lawsuits, although the expense and disruption of trade secret litigation are reasons enough to act. But since the enactment of the Economic Espionage Act of 1996 – and particularly since 2001, when local U.S. Attorneys acquired the power to file cases without approval from the Department of Justice – companies and their management have been exposed to federal criminal liability for trade secret misappropriation. The EEA is very broad, defining trade secrets as sweepingly as the civil law (that is, with no restriction to technical or scientific information), and basing liability on possession with intent to convert a secret, intent

which of course can be established by circumstantial evidence. In effect, many civil trade secret cases could qualify in the abstract as a federal crime, assuming that one can find an interested federal prosecutor.

But why be concerned with the Federal Sentencing Guidelines, which were issued to help federal judges determine a sentence following criminal conviction? The reason is that the Guidelines include a fairly specific set of attributes – best practices, if you will – that characterize a company's plan to prevent and deal with criminal conduct. Although the existence of a qualifying compliance plan will result in a reduction of sentence, in practice this can be a critical factor in a prosecutor's decision whether to charge a crime in the first place. So establishing a compliance plan will help to avoid criminal exposure. But it also is very helpful in satisfying the corporate obligations of officers and directors. As the Delaware Chancery Court has explained, in approving settlement of a derivative suit against a company's board members:

> "The [Federal Sentencing] Guidelines offer powerful incentives for corporations today to have in place compliance programs to detect violations of law, promptly to report violations to appropriate public officials when discovered, and to take prompt, voluntary remedial efforts. [] Any rational person attempting in good faith to meet an organizational governance responsibility would be bound to take into account this development and the enhanced penalties and the opportunities for reduced sanctions that it offers."[8]

Largely in response to Sarbanes-Oxley, the Federal Sentencing Guidelines have been toughened and made more specific regarding the expected content of Compliance Plans. The new Guidelines, effective November 1, 2004, reflect a significant shift in emphasis. Instead of a comment, the criteria for an "effective compliance program" have been elevated to the status of a guideline. Seven criteria are designed to reflect "an organizational culture that encourages ethical conduct and a commitment to compliance with the law." New features are highlighted in bold below:

---

[8] *In re Caremark Int'l Derivative Litigation*, 698 A.2d at 969-970.

1. The company must establish "standards and procedures to prevent and detect criminal conduct," including "**internal controls** that are reasonably capable of reducing the likelihood of criminal conduct."

2. Importantly, the **Board of Directors and senior management** must be knowledgeable about and **oversee** the compliance program. Although responsibility for operation may be delegated, the person in charge must have **"direct access" to the Board**, which must provide **adequate resources** and receive reports at least annually.

3. Individuals involved in management of the program should be free of any relevant record of criminal behavior.

4. The Board of Directors and senior management must receive compliance and ethics training.

5. The plan must include **auditing and monitoring systems** and must guarantee the right of individuals to come forward without fear of retribution.

6. The program must provide both **incentives** for individual compliance and disciplinary measures for non-compliance.

7. Once criminal conduct has been detected, the company must take reasonable steps to respond to it and to prevent further similar conduct.

In addition to these seven basic features, the guidelines require that a company "**periodically assess the risk** of criminal conduct" and take steps to modify its program to reduce that risk.

COMPLIANCE PLANS

As we have seen, the SEC and securities exchanges have provided substantial guidance on responsibility for the identification and valuation of outbound secrets. And the Federal Sentencing Guidelines' approach to avoiding liability for inbound secrets is fairly

comprehensive. (For a comparison of the various regulations, see Appendix A.) With this background, we can suggest the basic elements of an overall Compliance Plan that should meet management's obligations with respect to this important form of intellectual property.

First, the outbound issues should be addressed through a **trade secrets review**, also known as an "audit."[9] The process involves establishing a team (usually including company counsel, security, human resources, and information services) that collects relevant data from key individuals in each department or business unit. This effort focuses first on identifying the information – the "intangible assets" – that need protection. Open-ended questions are used to define what gives that business unit its competitive edge, how the information is developed, exploited, stored and protected, and what value might be placed on it. Once a baseline inventory is established, all key stakeholders participate in evaluating the risks and opportunities associated with various categories of data, as well as measures appropriate to ensure its proper treatment. From that point, a process of regular reviews will examine whether the protection system continues to be adequate, focusing on issues such as employee education, restrictive contracts, document and information systems control, facilities security, and publications. Reporting the results to upper management regularly should satisfy a company's obligations for informed attention to its own trade secrets.

Second, companies should establish a plan that satisfies the requirements of the Federal Sentencing Guidelines. Here, focus on certain key principles. The Compliance Plan is a **custom** document, designed to meet the particular risks of infection for that business, based on factors such as the nature of the technology, growth in hiring, use of consultants and temporary workers, outsourcing (or other collaborative ventures), foreign operations and government contracts. The

[9] For a more comprehensive treatment of trade secret inventory and audit processes, see *Trade Secrets* § 9.03[3].

plan must establish **standards of conduct and discipline**, and as noted above, must provide incentives for compliance and confidentiality for internal reporting. Critically for Sarbanes-Oxley compliance, the plan must establish **board and senior management** responsibility in terms of access, reporting and monitoring. Finally, the plan has to be adequately funded and well-communicated to the rank and file.

CONCLUSION

Unquestionably, the intersection of trade secrets, criminal law, and corporate compliance has marked a new and serious challenge for management. At the same time, following these newly strengthened requirements will provide value to the enterprise, by raising the visibility of its intangible (but increasingly valuable) assets, and by making theft or contamination of those assets less likely. Company counsel have an opportunity to present these compelling issues in that positive context.

APPENDIX A

	SECURITIES REGULATORS' APPROACH			CRIMINAL APPROACH
	SOX § 406(c)	NYSE 303A.10	NASD 4350(n)	Federal Sentencing Guidelines Chap. 8
Applies to	Senior Financial Officers, including principal financial or accounting officer, comptroller	Directors, Officers, and All Employees	Directors, Officers, and All Employees	Organizations sentenced for felony & class misdemeanors. Directors and Officers must exercise oversight with regards to implementing the program
Promote ethical behavior	Yes	Yes	Yes	Yes
Address conflicts of interest	Yes	Yes	Yes	No
Address Corporate Opportunities	No	Yes	No	No
Address Fair Dealing	No	Yes	No	No
Address Confidentiality	No	Yes	No	No
Require Disclosure Outside Organization	Yes, in periodic reports	Yes, must be listed on corporation's website	Yes	No
Require Compliance Plan	No	Yes	No	Yes must publicize plan within organization
Require Enforcement Mechanism	No	No	Yes	Yes
Encourage or Require Reporting of Illegal or Unethical Behavior	No	Encourage	No	Must take "reasonable steps"