

## Duty to identify, protect trade secrets has arisen Sarbanes-Oxley requires internal controls over how they are valued.

By R. Mark Halligan

SPECIAL TO THE NATIONAL LAW JOURNAL

INTANGIBLE PROPERTY, intellectual asset management and information security are now critical flash points in the Sarbanes-Oxley Act of 2002 and a myriad of other federal and state statutes. At the heart of these developments are trade secrets that comprise the largest asset class of most U.S. corporations. Companies now have a fiduciary duty to identify and protect trade secret assets. These assets encompass any information that derives economic value, actual or potential, from the secrecy of such information. See Uniform Trade Secrets Act With 1985 Amendments, [www.law.upenn.edu/bll/ulc/fnact99/1980s/utsa85.pdf](http://www.law.upenn.edu/bll/ulc/fnact99/1980s/utsa85.pdf).

Trade secrets no longer can be viewed as an amorphous intellectual property right. Trade secrets define an asset class. Asset valuations have shifted in the United States from physical property assets to intellectual property assets. Trade secrets are estimated to comprise 80% of the assets in New Economy companies. Ideas are now the core of value creation. Corporate growth is being driven by idea creations. The Financial Accounting Services Board (in FASB statements 141 and 142) and the Internal Revenue Service (in its § 482 regulations) are beginning to develop rules and procedures for capturing the economic value of this new asset class.

Trade secret assets often are created and stored electronically. As a result, computers and the Internet have resulted in a merger of information security protocols and trade secret protection measures. Protection of trade secrets is now inextricably intertwined with the same security management practices and computer hardware, software and network secu-

**TRADE SECRETS**

*R. Mark Halligan is a partner at Chicago's Welsh & Katz. He focuses on trade secrets law. He also serves on the adjunct faculty at The John Marshall Law School in Chicago, where he teaches advanced trade secrets law and trade secrets litigation.*



rity practices relating to the identification and protection of other types of information assets.

Until Sarbanes-Oxley, intellectual asset management was not viewed as an oversight issue for the boards of directors of U.S. companies. Management was given carte blanche authority over intellectual property matters. The board of directors became involved, if at all, only when the company was engaged in a major intellectual property lawsuit.

### Duty to defend assets

Sarbanes-Oxley has changed the rules of the game. It now is clear that the directors and top managers must become actively involved with intellectual asset management and information security, to avoid both civil and criminal liability under Sarbanes-Oxley and shareholder derivative suits for the breach of the fiduciary duty to adequately protect intellectual property assets. This represents a sea change in the law.

In the past, most companies neglected trade secret assets, and many companies still lack adequate systems for the identification, protection and economic evaluation of their trade secrets. Tens of billions of dollars in trade secret assets are lost each year by U.S. companies due

to the failure to take reasonable steps to protect them. See, for example, the 2004 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, at [www.nacic.gov/publications/reports\\_speeches/reports/fecie\\_all/fecie\\_2004/FecieAnnual%20report\\_2004\\_NoCoverPages.pdf](http://www.nacic.gov/publications/reports_speeches/reports/fecie_all/fecie_2004/FecieAnnual%20report_2004_NoCoverPages.pdf). The greatest losses to U.S. companies involve research and development and manufacturing trade secret assets. Losses have averaged almost \$50 million per incident.

Sarbanes-Oxley imposes new duties of disclosure and corporate governance. Section 302 of the act requires the chief executive officer and chief financial officer of public companies to certify that their annual and quarterly reports contain no untrue or misleading statements of material fact or material omissions, and to certify that the financial information in the report fairly presents the financial condition of the company. Section 404 requires companies to

document and certify the scope, adequacy and effectiveness of the internal control structure and procedures for financial reporting and controls. Section 906 imposes civil and criminal penalties for violations of the Sarbanes-Oxley Act.

Since trade secrets are financial assets, Sarbanes-Oxley requires adequate internal controls over the procedures by which they are valued and their value reported publicly. At a minimum, U.S. companies must now have a trade secret asset-control committee or a specific corporate officer charged with the responsibility to identify, protect and value trade secret assets on a day-to-day basis. These functions will extend to third-party relationships and outsourcing in foreign countries. In addition, trade secrets sold or acquired in mergers and acquisitions will have to be tracked and monitored by the corporation.

The identification of trade secret assets requires a systematic procedure involving the six-factor test from the Restatement (First) of

**Secrets are considered financial assets.**

Torts (§ 757, comment b). Efforts are now underway to develop computer software to facilitate the identification of trade secret assets in both large and small corporations. See, for example, The Trade Secret Office Inc., at [www.thetso.com](http://www.thetso.com).

Identification of trade secret assets also requires a classification scheme because these are information assets, and such information can span a continuum from notes on a blackboard to a secret formula locked in a safe. Seminars are now being held in the United States to develop best practices for company information classification systems and inventory procedures. Recently, the International Organization for Standardization (ISO) has promulgated a standard, ISO17799, for the management, protection and classification of a company's proprietary information.

In addition to the immediate requirement for the institution of trade secret identification and classification systems, U.S. companies must implement adequate security systems to protect their trade secret assets. This is the fundamental legal requirement to protect their trade secret assets in a trade secret theft action. The trade secret owner must demonstrate that reasonable measures have been taken to protect the trade secret assets. In turn, security procedures implicate access controls and a wide array of other computer security issues because most trade secret assets today are created, stored and disseminated in an electronic environment.

Access systems limit trade secret assets to disclosure or use on a need-to-know basis. This is the most effective way to protect trade secret assets. Password-protection and other security techniques must be used to define different levels of access to trade secrets. However, limiting access to trade secrets is just the first step. There must also be tracking systems in place to control and monitor the distribution of trade secret assets after initial access. See, for example, SealedMedia Inc., [www.sealedmedia.com](http://www.sealedmedia.com).

These tracking systems must ensure that nondisclosure agreements are executed by third parties before the trade secret assets are made available to them. The law requires that the third-party recipient, having been placed on notice, agrees to receive the trade secret asset in confidence. Failure to obtain executed nondisclosure agreements from third-party recipients before disclosure of the trade secret assets will result in forfeiture and loss of those assets as a matter of law.

Once there are systems in place for the identification, classification and security of trade secret assets, economic valuation issues must be addressed. A recent study concluded that the appropriate economic valuation model for trade

secret assets is the net present value of expected future cash flows to be derived from the competitive advantages conferred by the asset. See *Fundamentals of Intellectual Property Valuation*, ABA Section of Intellectual Property Law (2005), Chapter 9. This economic valuation model, in turn, is a function both of the content of the trade secret information and the stewardship and protection of the trade secret asset. Once again, unless reasonable measures are taken to protect the asset, the trade secret rights in the asset will be forfeited and the economic value of the asset will be zero.

The identification, classification, security and economic valuation of trade secret assets still are not enough effort to ensure compliance with Sarbanes-Oxley. Adequate internal controls must exist to assure the timely reporting of material changes or losses relating to trade secrets. There must be management alerts to assure notice of material changes to trade secret assets for accurate financial reporting. The board of directors, in turn, must have oversight functions in place to make sure that the board receives timely reports from management relating to trade secret assets.

### Defense against espionage

This is a tall order for U.S. companies, and some might suggest that this takes Sarbanes-Oxley too far. Not so. The aggressive application of the Sarbanes-Oxley Act will surely be one of the government's primary tools to protect U.S. companies from economic espionage and the theft of trade secret assets. We have already seen evidence of these developments. For example, the Securities and Exchange Commission went on record last year to say that the Sarbanes-Oxley Act and the related SEC rules will strengthen the internal controls in U.S. companies for the identification and protection of trade secret assets that, in turn, will improve the ability of companies to track the costs of economic espionage and trade secret theft.

Corporate governance is changing rapidly. The focus of attention is now on the board of directors to ensure that management protects shareholder value. This trend started with the Caremark International shareholder derivative action in 1996. See *In re Caremark Int'l Inc. Derivative Litig.*, 608 A.2d 959 (Del. 1996).

In 1994, Caremark International Inc. was charged with multiple felonies relating to violations of federal and state health care statutes. At issue was the scope of the fiduciary duty owed by the board of directors to the shareholders. Although much of the decision was dicta, *Caremark* now stands for the proposition that the board of directors bears a fiduciary duty to ensure that it remains reasonably informed about the

corporation's activities and to exercise good faith to ensure that adequate systems are in place to deliver accurate and timely information so the board can intervene to protect the interests of the shareholders and the corporation.

### Sentencing guidelines

The principles of *Caremark* and Sarbanes-Oxley show up again in the revised version of the Federal Sentencing Guidelines that took effect on Nov. 1, 2004. See U.S. Sentencing Commission Guidelines Manual, [www.uscc.gov/2004guid/gl2004.pdf](http://www.uscc.gov/2004guid/gl2004.pdf), § 8b2. The original 1991 guidelines did not specifically address directors. However, the new guidelines require boards of directors and executives to assume responsibility for the oversight and management of compliance and ethics programs. Trade secret assets and trade secret thefts fell squarely within the Federal Sentencing Guidelines with the passage of the Economic Espionage Act of 1996. Compliance with Sarbanes-Oxley also falls within the ambit of the Federal Sentencing Guidelines. The Federal Sentencing Guidelines have become the universal de facto standard for all corporate compliance programs.

These changes in corporate governance relating to the identification and protection of trade secret assets also were manifested in the New York Stock Exchange's corporate governance rules, effective on Oct. 31, 2004. See NYSE's Listed Company Manual Section 303A.10 (Nov. 4, 2003), [www.nyse.com/pdfs/finalcorpgovrules.pdf](http://www.nyse.com/pdfs/finalcorpgovrules.pdf). The NYSE now mandates that reasonable measures be taken to protect trade secret assets and third-party proprietary and customer information together with compliance programs similar to the requirements of the new Federal Sentencing Guidelines.

This is a wake-up call to corporate America. Trade secret assets can no longer be swept under the rug and ignored by management and the board of directors until a key executive leaves the company and a lawsuit is filed. The failure to implement the systems outlined in this article for the identification, classification, protection, valuation and oversight of trade secret assets will no longer be tolerated. Continued failure to act will result in serious Sarbanes-Oxley violations, a rash of shareholder derivative suits and the continued staggering losses of trade secret assets to competitors in the United States and abroad. **NLJ**

This article is reprinted with permission from the August 29, 2005 edition of The National Law Journal. © 2005 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact American Lawyer Media, Reprint Department at 800-888-8300 x6111. #005-09-05-0007