

TRADE SECRETS: POLICY FRAMEWORK AND BEST PRACTICES*

Every business would like to know its competitors' secrets of success, including any proprietary information of commercial value. As confidential information and knowledge increasingly drives business success, companies are honing their policies and practices to safeguard confidential information of commercial value against accidental, inadvertent or willful misappropriation, misuse, sabotage, loss or theft. Competitive intelligence, industrial espionage and sabotage are facts of life that cannot be glossed over, so secret information or data needs proper protection and management if it is to be leveraged for competitive advantage. Once confidential information is disclosed to competitors, its value is lost forever.

Only with due effort to keep information confidential or secret does such an intellectual asset become property that may be licensed as a trade secret or used to obtain protection for another type of marketable intellectual property asset. Inventions (protected by utility model or patent registration), trademarks, industrial designs, artistic or literary works (the latter protected by copyright and related rights), where they have not yet been made public, are kept as trade secrets until used or published as such, or during the process of registration or grant of the relevant intellectual property rights.

* This article is a follow up to the article on Protecting Trade Secrets in the April issue of the WIPO Magazine.

An enterprise-wide information security and protection program is essential for the protection of trade secrets. Such a program should have a wider scope, going beyond trade secrecy, to protect other types of secret information without commercial value, such as medical records of employees, attorney-client communications, etc. It should also deal with issues of business continuity and disaster planning for the secure and uninterrupted delivery of information during natural or man-made disasters. This step involves adopting a formal information security and protection policy. As many legal and technical considerations might bear on an information security and protection policy, companies should consult with legal and technical specialists to develop one that best suits their needs.

A basic step in developing and implementing such a policy and program is to identify and prioritize business secrets based on their value and sensitivity. This exercise should be carried out periodically to review and update the findings, given the fact that the value of information changes with time. Regular trade secret audits have emerged as an effective means of identifying, protecting and managing trade secrets, as they provide a basis for timely adaptation of the information security and protection system to the constantly evolving business environment.

Means of Protection

A common way of protecting trade secrets is through confidentiality or non-disclosure and non-compete clauses in an employment contract. In addition, a company should have similar rules and requirements for the protection of confidential information from contractors, consultants, vendors, customers, prospective or temporary staff, interns, visitors, non-employees working on site, etc.

There is no government registration process in any country of the world that forces enterprises to reveal their confidential business information to the authorities in order to obtain trade secret rights. So the cost of protecting trade secrets is largely the cost of putting in place an information security and protection policy and program in the company and the cost of monitoring, surveillance, audit and legal measures against insiders or outsiders who breach or try to breach the security system.

So long as a company has made systematic efforts that are considered reasonable under the circumstances to preserve confidentiality or secrecy, it may take legal measures to redress the misappropriation of almost any kind of information of competitive value. It is ille-

>>>

>>>

gal to acquire another's trade secret if one knows or has reason to know that the trade secret was acquired by improper means. Improper means include theft, bribery, misrepresentation, breach or induced breach of a duty to maintain secrecy, or espionage by electronic or other means. Reverse engineering or independent derivation alone are not considered improper means. Thus, a trade secret suit will not succeed if an aspect of a product's design or construction has been obtained by examination of an item purchased in the marketplace. Nor will a suit be useful against those who independently discover a secret process or make a compilation of commercially valuable information.

Employee Relationships

Employee education is an important component of a corporate trade secrets program. A good in-house information protection program informs employees of a company's policies regarding non-disclosure and educates and trains all employees on the practical aspects of information protection by providing clear, consistent definitions of confidential information, illustrated with specific examples from the work environment. It also includes a system for monitoring compliance and a process for audit, evaluation and continuous improvement.

Such a program also specifies that, when hiring, the company should exercise caution to avoid allegations that a new employee has misappropriated trade secrets from a former employer. Newly hired employees receive a copy of the information security and protection policy along with a briefing on the subject, and they agree to abide by the policy by signing an acknowledgement to that effect. Periodical reminders of the policy and proper training in its implementation are necessary throughout the period of employment. Employees leaving the company are reminded of their continuing responsibilities in that regard and of the need to return any information or document that may contain trade secrets. They also sign a separation report attesting to the return of all confidential information and trade secrets.

"Following the recent departure of employees from our asset-backed and mortgage-backed business, we discovered that intellectual property and other proprietary business information belonging to the Bank had been wrongfully taken," said the spokesman of a Major U.S. bank involved in a trade secret dispute.

(National Post Online - April 18, 2002)

Controls on Physical Access

A good policy provides that physical access to a trade secret document repository or to a manufacturing or research and development facility requires a security pass. A well defined and clear system consistently marks and controls the distribution of documentation containing confidential or secret information. Access to such information is limited to key personnel and is disclosed only after a written confidentiality or non-disclosure agreement has been signed. A good confidentiality agreement is detailed and direct, and limits post-employment restrictions, if at all, in time and geographical scope.

Security in the Electronic Environment

What is relatively easy in the physical world is much more complex when a company relies on computers, e-mails, instant messaging and websites for sharing information and engaging in e-commerce. A company must know its information and information systems in order to protect them, and understands all the types of information available anywhere on the company's various computer systems.



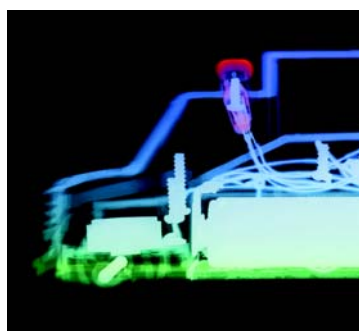
Courtesy: Osram GmbH



Top management should have a working knowledge of the different kinds of information that enter the system, what the system does with the information, how it is stored and when it leaves the system. Which employees have access to what kinds of information? How are employees prevented from accessing information without authorization? Are the internal barriers protecting different kinds of information secure? How are electronic archives created, accessed and protected? All employees are to be regularly reminded that online communications should receive the same care as written communications, and that a trade secret requires the same protection whether online, or in written or oral communication.

Electronic communications are more likely to leave a trail of inadvertent copies that can be seen with special software tools or during maintenance of computer systems. Every company should therefore have a system for encrypting and/or monitoring communication, and employees should know that this is being done. A company should monitor only enough to obtain legitimately needed information, and should stop once it has obtained sufficient information to establish employee behavior that violates its information security and protection policy.

In a computerized workplace, consideration is given to the kinds of information needed for specific job functions and to conforming the information system's internal barriers to ensure that employees have access to only the information needed for their own jobs. A centralized service assigns each authorized user a unique password,



to be protected and kept confidential by that individual, that is difficult to crack and is changed on a regular basis and deleted when no longer authorized. A good in-house policy clearly states that all employees are strictly forbidden to access another employee's e-mail or voice mail, and that violating this policy leads to severe disciplinary action.

Electronic storage media containing secret information/data, such as diskettes, compact discs and DVDs, should be physically segregated and secured in the same way as confidential or secret paper documents. Documents on such media, on hard drives of computers, and on secure central or network servers should contain a

legend that appears when the user tries to open the document stating that the document sought contains confidential or secret information or data of commercial value. Technical measures, software and encryption techniques may be employed to restrict access to classified information on secure networks, and to prevent or track unauthorized access to confidential information.

E-Commerce Concerns

Of the various concerns in e-commerce, protection of trade secrets is an important one. The main source of trade secret information created by a website is the web server, which systematically registers every visitor to the website, along with other information that may be useful for developing business strategy and marketing plans. This becomes a real issue when a company uses an external website hosting company. In this situation, such a company's directory on the web server often contains other information, data and programs that can constitute trade secrets, such as customized software. Therefore, every business should ensure that its external website host is contractually bound to ensure that the data stored on its site is adequately protected.

>>>

Take All Cases of Abuse Seriously

Companies frequently overlook the problem of loss of trade secrets by acts of omission or commission on the part of employees with computer access. This may have serious repercussions, as the employees of today may be tomorrow's competitors. Companies must therefore take steps to protect themselves against abuse of company information by errant employees. A coherent approach to controlling information may even provide a company with a better set of legal defenses and affirmative claims against employees who misuse confidential information.

A farsighted employer treats every known abuse of its secret information seriously. If the facts establish that an employee has accessed company information without authorization, then such an employer never fails to take the appropriate disciplinary action, as failing to apply appropriate disciplinary measures to one employee is simply putting arguable evidence of discrimination into the hands of another. Moreover, the wrongful nature of the employee's conduct could provide an extremely potent defense for the employer should the employee ever sue him. So disgruntled current employees are not at liberty to surf the company's computer system looking for evidence to use against the employer in future or current discrimination litigation.

Trade Secret Policy Underpins Intellectual Property Policy

As enterprises rely increasingly on intangible or knowledge-based assets for creating and maintaining their competitiveness in the marketplace rather than on tangible or physical assets, their ability to create, deploy and strategically manage such proprietary assets is becoming a crucial factor of business success. Adequate and effective creation, protection, use and management of trade secrets is the starting point on the road to successfully developing and managing intellectual property strategy and integrating it in the business strategy of an enterprise.

For more information on various practical aspects of the IP system of interest to business and industry, please visit the website of the SMEs Division at www.wipo.int/sme.

The next article in IP and Business will be on "Patents and Development of New Products".

Three months after taking a job at a US communication company, an employee allegedly made a late-night visit to the office, downloaded some files on to a laptop, and walked out the door. A few weeks later, he was named vice-president of one of the company's biggest competitors. The "suspicious" career move has since ballooned into a hostile battle over corporate loyalties and heavily guarded trade secrets – a battle that recently made its way into Canadian courts.

(National Post Online - February 23, 2002 - Michael Friscolanti)