International Journal of Economics and Management Sciences
Vol. 1, No. 9, 2012, pp. 77-82
Publication Date: May 17, 2012

MANAGEMENT JOURNALS
managementjournals.org

ECOMMERCE PROTECTION THROUGH INTERNET

PhD Jae-Sung, Lee
visiting professor in New Jersey City University, USA
E-mail: jslee797@yahoo.co.kr

ABSTRACT

Protection and enforcement of trade secrets outside the USA have been minimal and undeveloped and of particular concern when using the Internet. Substantive and procedural laws vary from country to country. In recent years there has been a move toward harmonization under the North American Free Trade Association (NAFTA) and the Trade Related Aspects of Intellectual Property Rights (TRIPS) agreement under the General Agreement on Tariffs and Trade (GATT) 1994. However, the provisions of TRIPS allow for varying periods for member countries to come into compliance. In the meantime international protection of trade secrets is uncertain, thus necessitating the development and implementation of strategies for preserving trade secrets in the international business environment. This paper discusses those strategies, beginning with defining and identifying a company's trade secrets and the formulation of various policy measures to be taken to protect trade secrets, with emphasis on the risks inherent in the loss of trade secrets when using the Internet and how to eliminate or reduce that risk.

Keywords: *Trade, Ecommerce, Legislation, Strategy, International business.*

1.INTRODUCTION

Trade secret protection outside the USA is minimal, undeveloped but improving. Substantive and procedural laws vary from country to country, with theories of recovery for wrongful disclosure or misuse ranging from breach of contract to violation of confidentiality laws. Many countries have enacted trade secrets protection laws but enforcement is lacking (MacLaren, 1993).

Trade secret law is well developed in the USA, the UK and in most jurisdictions that have the common law system. In civil law jurisdictions, as in most of continental Europe, there are reasonably comprehensive rules governing confidential information. In Asia, since the latter part of the 1980s, international pressure has brought major changes in the enactment of trade secret protection laws. However, enforcement has been ineffective. Developing countries have viewed intellectual property laws as a means of continued economic domination by industrialized nations with resistance to enact and enforce meaningful intellectual property laws. In general, foreign investment in many cases was discouraged due to a fear of losing valuable technology because the foreign jurisdiction did not provide reliable trade secret protections or because compulsory licensing laws and limited terms of protection resulted in the trade secrets technology being lost to disclosure.

2. NORTH AMERICAN FREE TRADE ASSOCIATION - NAFTA

With varying degrees of protection and enforcement of trade secrets globally there is a need for harmonization. The first major move toward international harmonization of trade secrets rights and protection occurred under NAFTA. The treaty addresses protection against misappropriation and defines trade secrets in virtually identical terms as provided under the Uniform Trade Secrets Act (UTSA), which has been adopted by most states in the USA.

The UTSA defines a trade secret as information, including a formula, pattern, compilation, program, device, method, technique or process that:

- derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use; and
- is subject of efforts that are reasonable under the circumstances to maintain its secrecy (therefore matters of public knowledge or general knowledge in an industry cannot be appropriated by one as his secret).

The NAFTA countries are required to provide legal protection of trade secrets information as against "unauthorized acquisition, disclosure or use in a manner contrary to honest commercial parties" which means that a "party know or be grossly negligent in failing to know that the information was misused", while under US law the standard is "known or should have known" the information was misused. This appears to be a less restrictive criterion. NAFTA does allow Mexico to require that secrets to be protected must be reflected in a document, e.g. "know-how" not embodied in a document would apparently be unprotected under NAFTA. The treaty also provides for perpetual protection and prohibits discriminatory or excessive restrictions on the right to license trade secrets. Further, the treaty protects confidentiality of trade secrets when necessary to disclose to the Government unless disclosure is "necessary to protect the public." Enforcement includes injunctive relief to prevent violation of intellectual property rights.

3. TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS(TRIPS)

Part of the Uruguay Round of General Agreement on Tariffs and Trade (GATT) 1994 establishing the World Trade Organization, was the TRIPS agreement. Since many countries are signatories of the treaty and many others want to become members, the terms of the TRIPS agreement is the most significant attempt to harmonize intellectual property rights globally. The treaty's provisions and coverage regarding trade secrets are similar to those provided under NAFTA and the UTSA. However, there is a question whether TRIPS includes secret information that has potential or future commercial value, as does NAFTA and under US laws. The treaty does provide extensive provisions for judicial enforcement with considerations of due process. Implementation of the TRIPS provisions allow varying periods (five to ten years) for member countries to come into compliance, depending on its stage of development (TRIPS, 1994).

4.STRATEGIES FOR PROTECTING TRADE SECRETS

Given that international protection of trade secrets is presently uncertain due to many countries being in various stages of enacting and enforcing trade secret laws in their effort to comply with TRIPS, it is still necessary to develop strategies to ensure protection of trade secret information in international commerce and especially when using the Internet. The issue of trade secret protection and use can occur in many contexts, e.g. in distribution and sales representation agreements, joint ventures, subsidiaries, employment, and is especially problematic in licensing confidential information and technology. Some countries require compulsory licensing to a business partnership or joint venture established there and in which there will be some form of local participation. Also nondisclosure provisions of a license agreement may be limited as to time, after which the trade secret information can be used and disclosed without compensation. Further, many countries regulate technology licenses if they contain territory or use restrictions that have anti-competitive effect.

5. INITIAL CONSIDERATIONS

The first step in creating an effective strategy in protecting trade secrets is to identify and inventory what materials and information the firm considers and qualifies as a trade secret. From the definition cited above a trade secret must meet three elements:

5-1.the information must not be generally known in the industry;
5-2.the information would be valuable to competitors; and
5-3.reasonable efforts must be made to keep the information confidential.

Specific examples of trade secrets include computer software and related data bases, hardware, customer lists, customer product use and preferences, formulas, profit margins, internal cost information, production processes

and strategies, supplier information and know-how. Just about anything that gives a company a competitive advantage can be considered as a trade secret (Lott, 1997).

In identifying what qualifies as a trade secret, each company should consider the following checklist:
What gives your company its competitive advantage and what would your competitors most like to know about your business operation?

How would you state and define your most important secrets and how do they differ from your competitors?

Can you assess the value of the secret to the company and to your competitors and how difficult would it be for someone to lawfully discover or recreate the secret? For example, a trade secret can be lost through reverse engineering.

How is the secret stored, communicated and who has access? Are there any threats to the security of the secret? Confidentiality and non-disclosure agreements should be examined.

Who within the company would most likely have answers to the above questions? Consider talking to people in marketing, sales, research and development, finance, production and computer programmers and MIS managers. Once the firm has identified its important secrets it can then implement protective measures. Traditional efforts to preserve secrecy include marking documents as confidential and limiting access to a "need to know" basis. The company should create a confidentiality policy communicated to all employees, who would then acknowledge receipt of the policy. Employees, vendors, licensees and anyone to whom secret information will be disclosed should sign confidentiality agreements and records should be kept of persons to whom the secrets were made available, when they were released and returned and what information was contained in them. A security system should be created for the business premises with check in and out procedures, badge requirements, restriction of access to visitors, use of passwords, and sensitive information should be kept under lock and key. Further, it would be advisable to schedule exit interviews to remind terminated employees of their obligation not to disclose or use the company's trade secrets and to inventory all secret items prior to his or her departure.

6.INTERNATIONAL CONSIDERATION

In the international context, additional measures must be taken to protect trade secrets. Initially, it is important to review the trade secret laws and procedures of the country in which the trade secret is intended to be utilized and avoid those jurisdictions in which enforcement of confidentiality obligations is lacking. Also it is important to choose overseas employees and licensees carefully by doing extensive background checks and having them sign confidentiality and non-disclosure agreements. This is important because some countries will be more willing to enforce contract provisions than to recognize an implied obligation of confidentiality. Monitoring compliance with the terms of such agreements should be done on a routine basis.

The owner of the trade secret information should only provide and disclose the kind of information necessary to accomplish the purpose of the transaction or relationship. It should be made clear in the contract to whom trade secret information may be disclosed and for what purpose and what security measures must be taken. For example, all sensitive documents should be marked "confidential". Discussions of such information should not be made by telephone or by e-mail, unless some encryption system is in place. Further, there should be a provision for resolution of disputes. Consideration should be given for the use of mediation and/or arbitration and also designation of choice of law and forum in which the dispute will be resolved. Finally, it is advisable to take into account whether to impose monetary penalties in the event of wrongful disclosure or misuse of trade secret information.

7. TRADE SECRETS AND THE INTERNET

With millions of users worldwide, the Internet can be especially problematic for preserving trade secrets. Once a trade secret has been exposed to the Internet a "cached" version of the text containing a secret may remain in

search engines for months and on users' hard drives indefinitely, even if the secret is removed from the Web site. Therefore proper use of the Internet is necessary to ensure that secrets are viewed only by intended recipients.

Trade secrets can get on the Internet in a number of ways. They may be posted intentionally with no understanding of the consequences. This can happen with Web sites listing new products plans, strategies for the future, revealing proprietary software, satisfied customers etc. The secret may have been posted negligently, for example, by not obtaining proper clearances from management. Secrets may be e-mailed to third parties for legitimate purposes without taking adequate precautions against retransmissions. This can result in the third party thereafter retransmitting, accidentally or intentionally, the information to countless others via e-mail or public postings with chat rooms and discussion groups. Also disgruntled employees and others may post secrets to sabotage the company. Hackers may gain entrance to internal computer systems and access and copy the company's stored secrets. Other means to access secrets may be developed by cyberspies.
So how does the trade secret owner preserve secrecy in the digital environment? There are three areas of concern regarding trade secret protection in cyberspace: Web sites, e-mail transmissions and chat room and discussion groups. Each one has its own special problems, discussed in the following subsections.

8. WEB SITES

How does the company ensure that information on their Web site does not include trade secrets? Since the company has control over what appears on the Web site, reasonable precautions must be taken to protect the secret, keeping in mind that competitors may view the site as well as potential customers. The company should not list satisfied customers on its Web site if it considers its customer list to be a trade secret. Also the listed customers may consider their source of supply as secret. Therefore it is important for personnel familiar with the firm's trade secrets to review proposed Web postings, and consider some form of digital lock or password protection plan or some form of click through confidentiality agreement for sensitive information that is deemed necessary to be placed on the Web (*Hot Mail Corp.* v. *Van Money Pie, inc.*[1]). A click through agreement would appear as a Web page or computer screen and requires the user to click e.g. "I accept" before moving onto the next page. Finally, in the event that a third party is involved in developing the Web site, the company should obtain ownership of all relevant software and require the developer to sign confidentiality and transfer agreements.

9. E-MAIL COMMUNICATIONS

The company should adopt a confidentiality plan that is communicated to employees so that they are informed of the significance of providing confidential information to others. Employees should be made aware that any e-mail that passes through the company computer is company property and may be monitored. Also company policy should prohibit forwarding of any documents to an outside e-mail without prior approval of the appropriate supervisor.

In the event of an e-mail transmission being sent to the wrong party, there should be a legend stating that the misdirected or received e-mail be destroyed and deleted. It is unlikely that an e-mail will be intercepted since the precise route traveled over the Internet varies from message to message. Even if it were intercepted it would be unlawful in the USA under the Electronic Communications Privacy Act. Whether it would be unlawful elsewhere depends on national law.

A major risk in transmitting digitized information via e-mail is that it can be easily retransmitted by the recipient to an unlimited number of unauthorized persons, e.g. a vendor can e-mail a customer's pricing information to the customer's competitors or an unhappy employee can e-mail sensitive information to discussion groups that will in turn retransmit and exchange this information with many other discussion groups worldwide.

To reduce this risk a number of measures can be taken. Employees and others should be counseled to use caution in selecting what they will transmit over the Internet and who the recipients will be, based on a need to know. These recipients should be deemed reliable and be informed that the information is confidential. Further, the company should make sure that e-mail is sent to the intended party and implement protective measures such

as passwords or encryption that will make it more difficult to retransmit the information to third parties. Periodic testing and review should be done to determine if these measures are being followed or need to be enhanced.

With regard to stored e-mail, the firm should use a password to protect highly sensitive e-mail so that it cannot be easily accessed once received. Sensitive information transmitted internally should include the construction of an "intranet" with secure firewalls that would prevent potential retransmissions over the external Internet. Other methods to prevent excessive or inappropriate use of e-mail include the use of monitoring software to track what happens to particular information, whether it was forwarded to third parties, downloaded, copied or e-mailed.

10. CHAT ROOMS AND DISCUSSION GROUPS

Chat rooms and discussion groups have many of the same problems as e-mail. There is no reason for employees to be posting confidential information in these places other than for some improper reason. Discussion groups, and chat rooms are places that pose the greatest risk of losing trade secrets. Many discussion groups automatically exchange posted information with other groups which leads to a total loss of control over the information discussed. A practical problem is identifying who posted the information. Anyone with access to trade secrets should be counseled not to post any secrets on public Internet discussion groups. If an individual wrongfully posts such information, this can result in a suit for misappropriation and possible criminal prosecution. A related question deals with what, if anything, can be done to prevent an innocent recipient from using or disclosing the confidential information to others since the information is no longer secret? In general there is not much that the owner of the disclosed secret can do. However, it should be noted that under USA case law it has been held that in determining whether a trade secret has been lost, the mere fact that the secret was disclosed on the Internet is not controlling. As discussed above, trade secret status requires that the information not be "generally known." The US courts have held that the general public is not the relevant population for determining if the alleged trade secret is generally known. In the case of *Religious Technology Center* v. *Netcom On-Line Communications Services, Inc.*[2], the US court held that the relevant population is potential competitors. In addition, the court will review all the circumstances surrounding the posting and consider the interests of the owner and policies favoring competition.

Therefore the trade secret owner must attempt to delete any misappropriated secret from the Internet as thoroughly and as quickly as possible. This includes re-registering with search engine services that may not update their caches frequently. Getting the word out that the public is not free to use the secret information can be accomplished by removing the secret from the places it has been posted and replacing the original posting with a statement that the prior posting has been removed because it was posted without the owners permission and may contain information that was misappropriated from the owner, and informing site viewers that use or retransmission of the information contained in that prior posting constitutes misappropriation. Of course this does not guarantee that trade secret status has been preserved, but as damage control it will minimize the risk of loss and show an attempt to use reasonable efforts to maintain secrecy (Burke, 2001).

11. CONCLUSION

Harmonization of the laws for the protection of trade secrets has begun with the enactment of NAFTA and the TRIPS agreement, but until their provisions are fully implemented by the member states, global protection of trade secrets is still problematic. This requires careful planning in the utilization of trade secrets abroad by first identifying the firm's trade secrets and then implementing protective measures to preserve their secrecy. Review of trade secret laws of the country in which the information is intended to be utilized is essential as well as evaluating to whom the information is to be disclosed, with their contractual obligations to maintain confidentiality.

Particular attention must be given when using the Internet to ensure secrets are viewed only by intended recipients. With regard to Web sites, it is important for the firm to review proposed Web postings with some form of password protection plan to be put into effect for sensitive information. When a third party is involved in Web site development, the firm should retain ownership of all relevant software and require the developer to sign confidentiality and transfer agreements.

Employees should be informed of the significance of providing confidential information to others via e-mail. These messages should include a legend stating that misdirected or unauthorized receipt of an e-mail be destroyed or deleted. Caution must be taken in selecting what will be transmitted and to whom, as well as implementing protective measures to reduce the risk of e-mail retransmissions to unauthorized third parties.

All parties with access to trade secrets should be counseled not to post trade secrets on public Internet discussion groups. If a third party does receive secret information via an unauthorized posting, the firm must attempt to delete such information as quickly as possible.

By being sensitive to the risks inherent with trade secrets and their utilization, the firm can take the appropriate steps to minimize misappropriation or unauthorized disclosure of such information. This will then preclude the loss of trade secrets by showing that reasonable efforts were taken to maintain secrecy.

REFERENCES

Burke, F.J. Jr (2001), "The challenge of protecting trade secrets in cyperspace", *Fifth Annual Internet Law Institute*, Practicing Law Institute, Vol. 1 pp.737-57.

Dratler, J. Jr (1993), "Trade secrets", *Intellectual Property Law: Commercial, Creative and Industrial Property*, Law Journal Seminars Press, pp.4-111 to 4-114.

Lott, L.J. (1997), "Taking stock of an intellectual property inventory", *Protecting Your Intellectual Property*, Practicing Law Institute Handbook, pp.221-32.

MacLaren, T. (1993), *Worldwide Trade Secrets Law*, Clark Boardman Callaghan, .

Pooley, J.H. (1995), "Trade secret audits", *Conducting Intellectual Property Audits*, Practicing Law Institute Handbook, pp.293-311.

Trade-Related Aspects of Intellectual Property Rights (TRIPS), Annex to the GATT of April 15, 1994, Articles 39 to 50, .

Electronic Communications Privacy Act, 25U.S.C.A. Section 2510 et seq, .

North American Free Trade Agreement, Article 1711 et seq, .