MODULE

04

Trade Secrets

MODULE 04. Trade Secrets

OUTLINE

LEARNING POINT 1: Basics of trade secrets

1. Definition of a trade secret

2. Type of information that could be a trade secret

LEARNING POINT 2: Trade secret management program

1. The 10 steps to build up a trade secret management program

LEARNING POINT 3: Misappropriation of trade secrets

1. Definition

2. How trade secret gets stolen

3. Protection of trade secrets

LEARNING POINT 4: Violation of trade secrets

1. How to establish violation of trade secrets

2. Remedies

LEARNING POINT 5: A trade secret audit

1. How to conduct a trade secret audit

INTRODUCTION

In a highly competitive business environment, responding to the new and evolving needs and wants of current and potential customers requires the creation of new or improved goods and services. For an existing or new business to survive, grow and thrive in this environment, it must be able to create itself or get the needed useful information to create and provide the new or improved goods or services in the marketplace. Such useful information is a “trade secret.” Often, competitors get access to such information rather easily, for example, by winning over or merely hiring away your key employees who created or have access to such useful, confidential information that gives your business a competitive edge. To prevent the erosion or loss of its competitive edge provided by such information, a successful company has to safeguard its proprietary or confidential information.

LEARNING OBJECTIVES

1. You understand the nature of trade secrets, the reasons for protecting them and the practical challenges in identifying and protecting them.

2. You know how to develop an effective trade secret management program.

3. You understand what is meant by misappropriation of a trade secret and how to prevent such misappropriation.

4. You know how to take various types of suitable actions to prevent violation of trade secrets.

5. You understand why and how to conduct a trade secret audit.

LEARNING POINT 1: Basics of trade secrets

1. Definition of trade secret

A trade secret is defined as any information that is:

(1) not generally known to the relevant business circles or to the public;

(2) confers some sort of economic benefit on its owner. This benefit must derive specifically from the fact that it is not generally known, and not just from the value of the information itself; and

(3) the subject of reasonable efforts to maintain its secrecy.

A trade secret continues for as long as the information is maintained as a trade secret.

Anything that is easily and completely disclosed by the mere inspection of a product put on the market cannot be a trade secret.

Learn more: The reason for protecting trade secrets

1. Trade secret law seeks to maintain and promote standards of commercial ethics and fair dealing.
2. A key objective of trade secret law is to provide an incentive for businesses to innovate by safeguarding the substantial time and capital invested to develop competitively advantageous innovations, both technical and commercial, and especially those that are not patentable or do not merit the cost of patenting.
3. If not protected by trade secret law, then competitors could use these innovations without having to shoulder the burden of costs or risks faced in developing the innovations.

More Reference 1-1: The formula of Coca-Cola

Perhaps the "best-kept trade secrets in the world".
The procedures for protecting the formula for Coca-Cola (a.k.a. "Merchandise

7X"), according to an affidavit given by a senior vice-president and general counsel for Coca-Cola in a court case, are as follows:
The written version of the secret formula is kept in a security vault at the Trust Company Bank in Atlanta, and that vault can only be opened by a resolution from the Company's Board of Directors. It is the Company's policy that only two persons in the Company shall know the formula at any one time, and that only those persons may oversee the actual preparation of Merchandise 7X.

The Company refuses to allow the identity of those persons to be disclosed or to allow those persons to fly on the same airplane at the same time. The same precautions are taken regarding the secret formulae of the company's other cola drinks- diet Coke, caffeine-free diet Coke, TAB, caffeine-free TAB and caffeine-free Coca-Cola.

2. Type of information that could be a trade secret

Virtually any type of information may qualify as a trade secret

(1) A trade secret may consist of information relating to a formula, pattern, device or other compilation of information that is used for a considerable period of time in a business.

(2) Often, a trade secret is technical information used in the manufacturing process for production of goods.

(3) A trade secret may relate to marketing, export or sales strategies, or a method of bookkeeping or other business management routines or procedures, including software used for various business purposes.

Other examples of potential trade secrets may include technical, scientific or financial information, such as business plans, business processes, list of key customers, list of reliable or special suppliers, product specifications, product characteristics, purchase prices of key raw materials, test data, technical drawing or sketches, engineering specifications, proprietary recipes, formulas,

content of laboratory note books, salary structure of a company, product pricing and advertising rates, source code, object code, databases and electronic data compilations, agreements containing details of marketing tie-ups, promotional or marketing material under development.

More Reference 1-2: Challenges and limitations of trade secret protection

A trade secret cannot be protected against being discovered by fair and honest means, such as by independent invention or reverse engineering.

If a person not having legal access to the trade secret information, deciphers the information without taking recourse to any illegal means, such as by reverse engineering or as by independent invention, then such a person cannot be stopped from using the information so discovered. Under these types of circumstances, the owner of a trade secret cannot take any legal action against the other person.

Advantages of trade secret protection

1. Trade secrets involve no registration costs;
2. Trade secret protection does not require disclosure or registration;
3. Trade secret protection is not limited in time;
4. Trade secrets have immediate effect.

In the case of inventions that may be patentable the disadvantages of protecting such inventions as trade secrets.

1. The secret embodied in an innovative product may be discovered through “reverse engineering” and be legitimately used.
2. Trade secret protection only protects you against improper acquisition, use or disclosure of the confidential information.
3. A trade secret is difficult to enforce, as the level of protection is considerably weaker than for patents.
4. Another person may patent someone’s trade secret if he has developed the same invention by legitimate means.

LEARNING POINT 2: Trade secret management program

1. The 10 steps to build up a trade secret management program

(1) Put in place a system for identifying trade secrets

Identifying and categorizing the trade secrets is a prerequisite for starting a trade secret protection program. The steps taken to protect your trade secrets should be dictated by the nature of the secrets themselves.

a. The basic questions to ask

- What information would hurt my business if my competitors get it?
- And how much will it hurt?

b. A related question to ask

- Do you have staff specifically assigned to record keeping, data security, or for preservation of trade secrets?

Make a written list of the information to be protected and organize it into the different types of information, depending on its value to the business and the type of protection measures that would be needed to protect it.

(2) Develop an information security policy that includes a trade secret protection policy

The information security policy encompasses systems and procedures designed to protect the information assets from disclosure to any person or entity not authorized to have access to that information, especially information that is considered sensitive, proprietary, confidential, or classified (as in national defense).

a. It is important to have a written information security or trade secret protection policy. A written policy provides clarity on all aspects that

need to be addressed.

- It should explain the why and how of doing so.
- It should prescribe how to reveal or share such information in-house or with outsiders.
- It should articulate and demonstrate the commitment of the business to protect its trade secrets as this would eventually play an important role in any unavoidable litigation.

b. Information security can be implemented at various levels such as the following:
   - Physical controls
   - Administrative controls
   - Technical controls.

(3) Educate all employees on issues related to information security

a. Always hire an employee on the basis of his competence knowledge and skills and not because of his access to trade secrets of a former employer.

b. All employees should acknowledge that they have understood the policy and that they agree to abide by it. Periodically, reiterate the policy.

c. Avoid hiring a person bound by a non-compete agreement. If unavoidable then do so only after taking advice from an independent and competent lawyer.

d. Indemnifying a new employee, who is bound by a non-compete agreement to a previous employer, should be avoided, as doing so raises suspicion of wrong doing and may result in a financial obligation if wrong doing is proved in a court case.

e. Remind your employees not to disclose trade secrets to unauthorized individuals or entities and to follow the security procedures; do so by way of notices, memos, network e-mails, newsletters, etc.

f. Hiring away more than one employee from a competitor would raise suspicion of wrong doing, and, therefore, it should be avoided as far as possible.

(4) Importance of exercising care in hiring an employee of a competitor

a. Educate and train employees on information security policy.

b. Transform every employee into a potential security officer.

c. Every employee must contribute to create a secure environment.

d. Prevent inadvertent disclosure that may take place due to ignorance.

e. The employees should be trained to recognize and properly protect trade secrets.

<Departing employees>

Make departing employees aware of their obligations towards former employer. Do so by conducting exit interviews that should also focus on issues related to confidentiality, trade secrets, etc.

If necessary or desired, they should be made to sign a new or updated confidentiality agreement. You may write a letter to new employer informing him about the relevant aspects of your trade secret concerns so that the departing employee is not put by the new employer on projects or activities where inevitable disclosure of your trade secrets would occur or is most likely to happen.

(5) Include reasonable restrictions in writing, in all contracts

Signing a good confidentiality or non-disclosure agreements with employees,

suppliers, contractors, business associates is of immense value in keeping information away from competitors.

a. Non-analysis clauses

Include non-analysis clauses in agreements for licensing trade secrets so that the other party agrees not to analyze or have analyzed any material or sample supplied under the agreement to determine its composition, qualities, characteristics, or specifications, unless authorized in writing by a duly authorized representative of your business.

b. No-raiding, non-recruitment or non-solicitation clause

A no-raiding, non-recruitment or non-solicitation clause in an employment agreement prohibits a departing employee from soliciting co-workers to leave with him to join another business or set up a new rival business.

(6) Restrict access to paper records

To prevent unauthorized access to records classified as confidential, sensitive, or secret, limit access to only those employees who are duly approved, or cleared, to see them on a need to know basis.

This may be done more easily by proper labeling of records (e.g., with a stamp such as confidential or secret) or using special colored folders (e.g., red or orange), and by keeping such marked records physically isolated or segregated in a secure area or in locked filing cabinets.

Depending on the size and nature of the trade secret, the location of the separated information can vary from a locked file cabinet, to a security

patrolled warehouse or storage facility. There has to be proper access control through appropriate authorization and accountability and tracking system for employees provided access to classified information.

(7) Mark documents

There are various types of useful ways for marking confidential or trade secret information. Look at the following examples:

a. MAKE NO COPIES

b. THIRD PARTY CONFIDENTIAL

c. DISTRIBUTION LIMITED TO ____

d. COVERED BY A NON-ANALYSIS AGREEMENT

The CRITICAL, MAXIMUM, MEDIUM, and MINIMUM labels are examples of information classifications

In general, the labels should provide brief but clear direction to the user on how to handle the information.

(8) Office management and keeping confidentiality

a. Mobile or cellular phones discussing sensitive topics over a cellular phone is a dangerous practice. Confidential information may be “lost” if there is unrestricted use of mobile or cellular telephones.

b. Fax machines

Often, the fax machine is located in a common area with unrestricted access and it is typically unattended. The second problem with fax transmissions is that they utilize phone lines, which can be tapped quite easily.

c. Photocopying

It is not unusual for an employee to make copies of a secret or confidential document, pick up the copies and walk away, leaving the original in the copier for the next user to find. Extra care should be taken to remember to retrieve those original secret or confidential records when the copying is finished.

d. Shredding

A better method for disposition of all paper records, of course, is shredding them. Shredding is a major element in most information security programs. With a wide variety of machines on the market, businesses may implement shredding in several ways.

e. Telephones

Callers posing as researchers, industry analysts, consultants, or students ask for information about the organization and its employees–and many times get it.

f. Internal literature

Newsletters, magazines, and other in-house publications often contain information useful to snoops, including new product announcements, results of market testing, and names of employees in sensitive areas (who are potential contacts).

g. Waste bins

It is not safe to put them into a nearby office waste paper or trash bin, as anyone with access to the trash might make use of those records for gathering competitive intelligence.

h. The compulsive talker and loose talk

Employees are deluding themselves if they think their lunchtime or coffee break conversations and any discussion of company business on

the metro, subway, bus stop, train station, or a restaurant is wholly private. It is not at all unusual for people nearby to hear clearly these conversations.

(9) Maintain computer secrecy

For most computer systems at least two security measures are built into them:

a. Use of passwords for a user to access the system

b. Automated audit trails to enable system security personnel to trace any additions or changes back to whoever initiated them, and to indicate where and when the change was carried out.

<Access Control and Security Labels>

Access control is a means of enforcing authorizations. There are a variety of access control methods that are based on different types of policies and rely on different security mechanisms.

a. Rule based access control is based on policies that can be algorithmically expressed.

b. Identity based access control is based on a policy which applies explicitly to an individual person or host entity, or to a defined group of such entities. Once identity has been authenticated, if the identity is verified to be on the access list, then access is granted.

(10) Guarding secrets that are shared in partnerships

a. While employees can be the single biggest threat to secrecy, it is also important to guard secrets in joint ventures, with consultants and even with customers.

b. For many software companies, the most dangerous exposure is the sale of a system because the software is then susceptible to reverse engineering. In software and many other high-tech industries, licensing of your company's product is a secure way to guard against loss.

More Reference 2-1: Locked waster paper bins

1. Advantages of locked waste paper bins

   (1) Paper is secure from point of generation through point of destruction.

   (2) It can be visually and systematically demonstrated to customers/clients that an infrastructure exists to protect information.

   (3) Avoids the need to shred at point of generation.

2. Disadvantages of locked waste paper bins

   (1) Additional cost of purchasing locked bins.

   (2) Additional labor to collect paper from locked bins.

   (3) Additional space may be required to stage locked bins during collection.

   (4) Finding and keeping track of keys for bins; need to decide if all bins should be keyed alike, or have multiple keys or multiple locks.

   (5) May reduce staff compliance if use of the locked bins is not easy or they are not as accessible as unlocked bins.

LEARNING POINT 3: Misappropriation of trade secrets

1. Definition

(1) Unfair acquisition that is, acquiring a trade secret by theft, fraud, coercion, or other unlawful or dishonest acts.

More Reference 2-2: Basic rules in using computer passwords

1. Never share a password with anyone.
   Even if shared with a trusted person, the possibility of its falling into hostile hands exists.

2. Make a password at least six characters long.
   Password-guessing computer programs can guess three-character passwords in as little as fifteen minutes, while a six-character password will normally take two years to "crack."
3. Do not create passwords that others can guess. (e.g., family names, birthdays).

4. Change passwords regularly (e.g., once per month).
   This practice reduces the chance of someone guessing a password.

5. Keeping a written copy of the password in the office.
   If you do that, especially near the computer (all-too-common a practice) the purpose of the password is defeated.

6. Treat dial-in phone numbers as carefully as passwords.

7. Never leave their computer terminal unattended while logged on.
   This practice eliminates the need for an intruder's guessing a password and simply allows anyone quick access to data stored in the computer.

(2) Acquiring a trade secret with knowledge of its prior unlawful acquisition, or acquiring such trade secret without actual knowledge of its unfair acquisition but being grossly negligent in failing to know of the earlier unfair acquisition and, in either case, using or disclosing a trade secret so acquired.

(3) Although innocently acquiring a trade secret, using it or disclosing it after learning of its earlier unfair acquisition by another person.

(4) Using or disclosing the trade secret in breach of a contractual obligation to maintain the trade secret.

a. Acquiring a trade secret that was disclosed in the circumstances set forth in (4) above, either knowingly or with gross negligence in failing to know of the breach of the contractual obligation, and using or disclosing such trade secret

b. Subsequent to the innocent acquisition of a trade secret that had been disclosed under the circumstance set forth in (4) above, using or disclosing it after learning of the earlier breach of contractual obligation or being grossly negligent in failing to learn of such earlier breach.

2. How trade secrets get stolen

(1) Industrial espionage

Intense competition in domestic and export markets has also lead to an alarming increase in theft by outsiders, known as industrial espionage. Such activities are on the rise due to increasing global competition, shorter product cycles, thinning profit margins, and declining employee loyalty.

a. External threats

External threats include corporate spying with professional criminals targeting specific technology, initiating network attacks (hacks), laptop computer thefts:

- accessing source code, product designs, marketing plans, customer lists
- approaching employees to reveal company information etc.

Businesses strive to protect their trade secrets by enacting corporate security measures and confidentiality clauses in employment, technology licensing, distributorship and joint venture agreement.

b. Internal theft

Internal theft by disgruntled workers or former employees is also intentional. Some of these people allow themselves to be exploited by competitive intelligence operatives, either for money or merely for spite.

Example

A fired or retrenched employee might go directly to a competitor and offer, for seeking revenge or for a fee, to disclose your trade secrets, marketing strategies, or new product plans–often despite signed nondisclosure or confidentiality agreements.

Sometimes, competitive intelligence operatives may tap phone lines, or regularly sift through a company's garbage, break into computer systems. They may include seemingly innocent persons such as research analysts, business analysts, information specialists, and potential employees or customers, who gain employees' trust for obtaining proprietary information by inducements, gifts or blackmail.

3. Protection of trade secrets

Generally, most countries do not have a specific law for trade secrets

The owner of trade secrets has to rely on relevant provisions of the national law against unfair competition and/or by court action under the law of torts and by appropriate clauses or provisions in employment agreements and other types of business agreements in accordance with the contract law of the country.

(1) Unfair competition law / Principles of tort

When misappropriation is done by competitors who have no contractual relationship or indulge in an act of theft, espionage, or of subversion by employees. The law of tort is judge-made law in 'common law' countries.

(2) Contract law

When the agreement between the parties seeks to protect the trade secret by using a non-disclosure clause or confidentiality clause, through an anti-reverse engineering clause, or where an implied confidential relationship exists, such as between an attorney and his client, or an employer and his employee, etc.

(3) Criminal law

When an employee steals trade secrets from a company or someone does espionage or in involved in acts that may be considered as invasion of privacy, etc., or circumvention of technical protection measures of *IT / non-IT* systems.

More Reference 3-1: Dealing with memorized trade secrets

The main difficulty is in separating a protectable trade secret from non-protectable knowledge and skills of former employee that are retained in the person's memory.

The courts of some countries have dealt with this issue in the following ways:

1. whether an employer can stop a former employee from using trade secrets retained in memory, i.e., "misappropriation by memory"

2. whether an employer can use trade secret law to enjoin a former employee from working in a job that would inevitably result in the use of trade secrets, i.e. "inevitable disclosure."

In fact, both protect against the use of a memorized trade secret, but they differ in the type of injunctive relief available. The doctrine of inevitable disclosure should be limited to the narrow factual situation where it is inevitable that a former employee will use a specific trade secret in the course of performing an identified job responsibility that is inherent in the person's new job.

LEARNING POINT 4: Violation of trade secrets

1. How to establish violation of trade secrets

Main issues are:

(1) Was the information indeed secret?

(2) Were reasonable steps taken to maintain the secrecy?

To establish violation of trade secret rights, the owner of a trade secret must be able to show the following:

(1) Infringement by or competitive advantage gained by the person/company which has misappropriated the trade secret.

(2) The owner had taken all reasonable steps to maintain it as a secret.

(3) There is misuse as the information obtained has been used or disclosed in violation of the honest commercial practices.

2. The remedie

(1) A court order restraining the person from further benefiting from or misusing the trade secret.

(2) A court order for monetary compensation in the form of damages, based on the actual loss caused as a result of the misuse of trade secret. (For example, lost profits or unjust enrichment)

(3) Seizure order by the court, based on a civil action, which may include a search of the defendant’s premises in order to obtain evidence to establish the theft of trade secrets at trial.

(4) Precautionary impoundment of articles that include misused trade secrets, or the products resulting from its use or misuse.

(5) A court may order the destruction of the products made by the infringing act, and/or destruction of the equipment used to carry out the infringing act.

(6) Some countries permit the imposition of punitive damages for willful encouragement of trade secret theft.

LEARNING POINT 5: A trade secret audit

1. How to conduct a trade secret audit

Basic steps for conducting a trade secret audit are as follows.

(1) Identify significant trade secrets

Consult with research and development, manufacturing, MIS, sales and marketing and human resources; compare your company's advantages vis-à-vis manufacturing processes, raw material ingredients, information management, contacts with customers, etc., as compared to competitors.

(2) Verify the company's title to trade secrets

Contact legal and human resources to determine if assignments from employees, consultants or other predecessors in interest are complete.

(3) Verify that confidentiality procedures are followed

Contact security, human resources and departments that maintain the trade secrets.

(4) Verify that employees, consultants, vendors, customers and other third parties do not disclose trade secrets of third party

Contact human resources to determine if new employees and consultants agree in writing not to disclosure confidential information from former employers; contact legal, purchasing, sales and marketing, research and development, MIS and manufacturing regarding other third party agreements.

QUIZ

Q 1. Identify the incorrect statement:

1) A trade secret generally referred to as "know-how" is any information, design, process, composition or technical formula that is not known generally and that affords its owners a competitive advantage.
2) Trade secret owners should take the reasonable precaution to keep the information confidential to acquire and maintain trade secret rights.
3) A trade secret does not need the government registration process and has the possibility of perpetual protection if kept secret.
4) Trade secrets may be legally safeguarded against accidental leakage.

Answer: 4)
Trade secrets may be legally safeguarded against misappropriation but not against wrongfulness or accidental leakage. Any third party who gains accidental knowledge of the secret information are under no obligation to the trade secret owner. No liability may arise in the absence of an obligation.

Q 2. Identify the incorrect statement about a trade secret:

1) Unlike other IP rights, trade secret owners may seek liability only when the appropriator acquires, reveals or uses the secret in a wrongful manner.
2) Companies need to conduct a trade secret audit to realize how much of their confidential business information may qualify as a protectable trade secret, and then should establish a trade secret program.
3) A commonly used way of protecting trade secrets is through non-disclosure and non-solicitation clauses in employment and other contracts.
4) Trade secrets relate mostly to aspects of business operations such as pricing and marketing techniques or list of customers.

Answer : 4)
Trade secrets relate not only to business and financial aspects but also to technological aspects of a business, especially those which cannot be protected by patents, or are chose not be patented even though they are patentable, or are associated with one or more patents, as everything known and useful in relation to

a patented technology is not required to be revealed in the relevant patent document. Only that is much required to be revealed in a patent document as would suffice for the grant of a patent. Technical know-how may be protectable as a trade secret.

Q 3. Identify the incorrect statement about a trade secret:

1) Both trade secrets and patents are forms of intellectual property that can be used to protect innovations.
2) One of the differences between patent protection and trade secret protection is that patent protection requires the protected information become available to the public (through publication of the patent application and/or patent), whereas trade secret protection requires the protected information be kept secret. Therefore, if you file a patent application, you lose all of your trade secret rights in the invention.
3) If a product has a short life cycle, trade secret protection may be preferable to patent protection.
4) Patents and copyright grant exclusive rights. In contrast, there is no guaranteed monopoly for trade secrets.

Answer: 2)

If you file a patent application, the information disclosed in your patent application will be made public at the time of the publication of the patent application/patent. However, that does not necessarily result in the loss of all of your trade secret rights related to a particular invention. Certain information with respect to the invention may still be kept as a trade secret. In your patent application, the description of your invention must be sufficiently complete so that someone skilled in the relevant technology area could make and use the invention based on the written description. However, subsequent to filing, improvements to the invention may be developed when the invention is actually constructed and tested. Also, engineering difficulties may be encountered and solved during the process of converting the invention into a commercially viable product. Such technological know-how developed after filing the patent application does not have to be disclosed in the patent. It may be kept as trade secret.