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 thatneed 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 uspicion 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.