I.POTENTIAL SOURCES OF TRADE SECRETS

Identifying potential trade secrets is generally not a difficult task, and there is no magic to it. A trade secret may consist of any information that the company feels is valuable enough to justify taking some measures to protect. Protection of such information can be accomplished on a sliding scale -- a few rudimentary steps for somewhat valuable information and a longer list of safeguards for more valuable information. However, the key is that putting something on the list of trade secrets does have some cost -- some protective measures will have to be taken. Simply making it a "wish list" of things that the company would just as soon the competitors not have access to is self-defeating. The following list provides some examples of information that may be considered trade secrets.

A.The cost of materials, where the company gets its materials, tests which may have been done to assure the quality of the materials, results with specific suppliers who may have proven either very valuable or less so, the amount and types of discounts the company may have negotiated with suppliers, and the details of any long term contracts with suppliers.

B.Profit margins -- including profit margins for certain products or in certain areas of the business.

C.Financial plans, banking relationships, the names of major investors, the capital structure of the company, and details about relationships where a supplier or business partner is also an equity owner of the company (increasingly common with e-commerce arrangements).

D.Relationships with distributors or dealers, including discount structures, the performance of various dealers or distributors, and plans for adding more or reducing existing dealers or distributors.

E.Management information systems.

F.Facts relating to the manufacturing operation including equipment types, usage, advantages and disadvantages of various types or pieces of equipment, number of employees in any given operation, and any methods of operation that have been developed after some experimentation and which the company believes gives it at least some competitive advantage.

G.Personnel information including a listing of key employees -- perhaps with some indication of why they are considered key and what meetings they have attended or interviews that have been conducted with them to make sure that they understand certain information is confidential.

H.Plans for acquisitions or divestitures -- either specific or in general terms.

I.New product plans, the results of previous new product introductions, and plans for entering new markets -- either product or geographic.

J.Information about customers, including their identity, what they have purchased, how they have paid, what they are charged if different from standard list prices, and the names of key contacts at those customers.

K.Advertising plans including budgets, history of ads (which ads have been successful, which ads failed), and market research and forecast.

L.Certain licenses -- either inbound or outbound -- may be legitimate trade secrets especially if they contain economic data such as royalty rates based on production or output.

M.Technical information including plant design, special equipment and its design and functions, formulas, results of research in terms of performance, character of products or components, research and development results, plans, and budgets.

N.Data relating to the company Web site including how many "hits," what has sold over the Internet and what has not, the details of any linking arrangements that have economic significance, and plans for the Web site in the future.

End Result: The end result of this exercise should be a listing of things the company considers to be trade secrets -- which list is itself a trade secret. It is this list on which the steps below would be based. The process is that the company thought these things (the list) were trade secrets, and for each it took certain protective steps (also listed) to safeguard the information.

II.PROTECTION OF TRADE SECRETS

The law on this is somewhat subjective -- there is no "safe harbor" in terms of a listing of things which, if done, will assure that the information is characterized as a trade secret. Instead, it is more of a commonsense notion of what steps would be reasonable under the circumstances given the sensitivity of the information and the practical business needs of the company. As a practical matter, however, at least from a legal perspective, a rule of thumb is whether counsel would feel comfortable going before a judge or arbitrator and explaining what was done, how it was done, why it was done, and the results of those efforts in the context of the information the company seeks to characterize as a trade secret. This generally would have to include documents that could be produced, procedures that could be observed, and records showing how the company dealt with any problems.

A.Physical Security Measures

1.Doors and Entrances

It is generally said that most unauthorized entries into residences are through unlocked doors. Similar arguments would appear to be possible in the case of many trade secrets -- the company claims something is a trade secret but it is clearly visible and accessible to anyone and everyone. We suggest that at least some physical security measures are necessary in all cases. It may be as simple as locked file cabinets, rooms that are locked and that only certain employees have access to, and fences around a plant and access only through certain gates. Doors and file cabinets with locks on them are only useful if the doors and files are actually locked when they are supposed to be.

2.Paper Files

Much trade secret information will be in the form of papers in files. These files should be segregated from nonsensitive material and handled differently. These trade secret documents should also be clearly labeled. Stamps are sometimes helpful. Cover sheets perhaps in colored paper are potentially useful. Procedures can be elaborate -- as they are with classified government material -- or more simple. However, there should be at least some procedures for locking the material up at night, restricting those who have access to it, restricting (or prohibiting) taking the material out of the restricted area, not allowing any copies to be made, and not allowing the material to be downloaded or stored on anyone's personal computer.

3.Individuals Responsible

Who is responsible for safeguarding what information? This obvious question often goes unanswered -- and that is a mistake. The person should be someone with reasonable authority -- not the file clerk. It should also not be the plant manager or someone such as that who -- while admittedly ultimately responsible -- is not close enough to the action in terms of where and how the files are used to have a practical effect on security.

4.Hide the Details

It is important to take steps to disperse or hide the details of the information so that as few people as possible have access to it. For example, if you have a process in the plant which involves different operations taking place at different temperatures, one might remove all the dials that show the temperatures and replace them with dials that do not show the details. Employees might simply be told that this process must take place while Dial A is in the green zone and Dial B is in the red zone. If special equipment is used, perhaps the name of the manufacturer can be taken off of it.

5.Divide Procedures

Another technique worth considering is dividing up processes or procedures among various groups so that no single person knows everything that could be damaging in the event of employees leaving the company.

6.Trash Disposal

Cases are legion where trade secrets have been stolen from dumpsters. Care and procedures for the disposal of confidential data should be a part of the process. It might be helpful to look into the company policies and practices on document destruction.

7.Visitors and Tours

Another embarrassing thing that has surfaced in litigation is that students from the local high school are brought into court and tell how they were shown the process and procedures the company now claims is a trade secret. Controlling visitors is important. A trade secret evaluation or audit might inquire as to the company policies and practices regarding outside visitors.

8.Cell Phones

There have been highly publicized cases of people overhearing sensitive information from cell phone calls. These are generally not secure, and sensitive information should not be discussed over a cell phone.

9.E-mail

E-mail is another potential problem. In some systems, e-mail is very difficult to remove and may end up being stored permanently. Its security may also be questionable. Restricting transmission of sensitive information via e-mail may be appropriate.

Some attention should be given to encryption. What are you sending over the Internet via e-mail and attachments? How and to what extent should encryption technology and software be used? This is somewhat technical, and it is evolving. In general, however, suitable encryption techniques are available, and there has been enough liberalization of the export control laws to allow the effective use of encryption technology in most organizations.

10.Computer and Software Access

The distribution of computer power throughout the organization creates significant problems. Restrictions may be required regarding laptop computer usage. Certainly those who travel should not be allowed to have a laptop computer with sensitive information on it. Laptops are high on the list of stolen items.

Additionally, the whole area of computer and software security needs to be addressed by those who are familiar with current techniques. This has to be repeated frequently as the technology changes. Passwords, techniques to prevent unauthorized use or access to certain programs or certain computers, techniques that will allow the company to trace access to certain computers, computer programs, or databases, are all techniques that need to be considered and addressed by those with the technical ability to make intelligent decisions as to what should be done.

11.Company Web Site

The previous item focuses on internal computer systems and networks. There also should be some attention to the company Web site. Of course, the company would not put trade secret information on the Web site for anyone to access, but the details and specifics about how the site works, what development was done and by whom, what contracts the company may have regarding the content of the Web site, etc., may all be confidential. In addition, the issue of "hacking" cannot be ignored. Whatever the company does to safeguard against hackers would be confidential.

B.Employees

It is frequently said that employees are the biggest potential problem in terms of loss of trade secrets. Those who make this observation are usually referring to deliberate theft of trade secret information -- often in the context of a change of job or leaving the company to go into business in competition with the former employer. On the employee side, the observation is sometimes made that the information was not treated as a trade secret at all until the employee decided to leave. In most cases, there is probably a little truth on both sides of that argument. That is why we list employees -- who are the biggest problem -- down the list. There are some things that can and should be done, but the physical measures and procedural safeguards must be in place in order for them to be effective. Following are some possibilities:

1.Prepare a company manual or memo telling employees how important the company trade secret information is to the financial success of the company -- and, therefore, presumably to the advancement and opportunities of the employees.

2.Have all employees sign appropriate nondisclosure agreements. These, however, should not be treated as routine documents. Instead, there should be an explanation of what the employee has been hired to do that may make it necessary for the employee to have access to confidential information -- in other words, provide some specifics. Then, if the employee leaves, there should be an exit interview where the nondisclosure requirements are reinforced, and where the employee is specifically asked about any documents or any other company property that the employee may have and asked to affirm that it has been returned. Specific mention of personal computers may be appropriate.

3.Certain employees should be required to document research and development work so that the company has a record of information they had access to and the discoveries they participated in developing.

4.Employees may be asked or required to report any attempts by outsiders to get confidential information from them.

5.Some attention to specific steps in the context of terminated employees may be appropriate. Restricting their access to the company facilities would be a minimum. Some sensitivity here (as in all of this) is required. Restricting current employees from talking with former employees would clearly be a mistake. One could restrict current employees from discussing company matters with former employees (or anyone else), but a presumption that any conversations with former employees is accompanied by evil motives would be inappropriate.

C.Contractual Relationships

Contractual relationships are also a place where trade secret information needs to be safeguarded. Arrangements with consultants -- broadly defined to include programmers or just about anyone else who does work for the company and who may come in contact with trade secret information -- are a place where the confidentiality portions of the agreement can be important. In this regard, we suggest direct contractual relations -- at least on this confidential information point -- with the individuals. Often the individuals will be working with a firm that will sign a confidentiality agreement with the company. The firm will also represent that they have similar agreements with each of their employees -- thus arguably "closing the loop." We suggest this does not emphasize the trade secret or confidential information sufficiently in the minds of the consultants, who are obviously the ones who will be going to another assignment, perhaps with your competitor, when finished with your work. Instead, each individual should be asked to sign a confidentiality agreement which includes a promise of confidentiality, and also contemplates an exit interview where they will represent that they reaffirm their confidentiality obligation and represent that they have returned all company documents and have not made any copies.

Any other contractual relationship is also a potential problem and, therefore, should have appropriate nondisclosure clauses. Arrangements involving "working together" with a supplier or customer to develop a better product or service are particularly sensitive in terms of each party respecting the trade secrets of the other.

D.Licensing Arrangements

Licensing or similar relationships are also worth specific mention. Often the question is procedural. The company asks, "How can we be assured that if we disclose our confidential trade secret to you it will be worthwhile? Is your product or program useful enough to us to justify the risk?" (Same questions on the other side.) The other side will basically say that they are unable to be specific enough about your needs and the likelihood of the product, service, or program being useful to you without the specifics. Often, a compromise is a "step" or "phased" transaction. We disclose a little and see the results, then disclosed additional information, etc. The same procedure may be useful in analyzing potential acquisitions or divestitures. Confidentiality and nonuse and nondisclosure agreements are the norm -- but as a practical matter, one can still lose a lot of competitive advantage in negotiating with a competitor about an acquisition or divestiture if the deal falls through.