Santa Clara High Technology Law Journal

Volume 5 | Issue 2 Article 4

January 1989

Trade Secret Protection: An Analysis of the Concept Efforts Reasonable Under the Circumstances to Maintain Secrecy

David W. Slaby

James C. Chapman

Gregory P. O'Hara

TRADE SECRET PROTECTION: AN ANALYSIS OF THE CONCEPT "EFFORTS REASONABLE UNDER THE CIRCUMSTANCES TO MAINTAIN SECRECY"

David W. Slaby†
James C. Chapman††
Gregory P. O'Hara†††

I. INTRODUCTION

The success of any business depends on its ability to obtain and maintain a competitive advantage in the marketplace. Quite often, a company's competitive advantage is provided by some form of formula, process, knowledge or product that a competitor does not possess. Once a company develops such a competitive advantage, it must take certain steps to ensure its protection. In many circumstances, trade secret law provides an effective means of protecting sensitive information that is at the foundation of a company's competitive advantage.

Unless reasonable efforts are undertaken to maintain the confidential nature of trade secrets, a competitor can legally appropriate the trade secret and thereby destroy or compromise another's competitive advantage. In light of the prevalence of industrial espionage today,[1] the trade secret owner must stand vigilant to protect

† David W. Slaby is a litigation partner in the San Jose Office of Pettit & Martin. Pettit & Martin is a full service law firm with seven offices throughout the United States and Hong Kong. The San Jose office handles litigation, government contract and corporate matters and represents a wide variety of high technology clients.

†† James C. Chapman is a corporate associate in the San Jose Office of Pettit & Martin.

††† Gregory P. O'Hara is a litigation associate in the San Jose Office of Pettit & Martin.

1. *See* E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970); Greenwald, *Corporate Cloak & Dagger*, TIME, Aug. 30, 1982, at 62, 63; *FBI, DuPont Foil Extortion Plot*, San Jose Mercury News, Feb. 28, 1989, at 5D. In December, 1988, an individual contacted DuPont offering to sell DuPont documents from the Company's Argentina subsidiary regarding its spandex technology. The individual demanded $10 million for the documents. If DuPont refused to pay the requested sum, the individual would use the information to go into business for himself or sell the information to one of DuPont's Com-

its competitive advantage against theft or other unlawful appropriation.

This article will first define and discuss the requirements for the legal standard of "efforts that are reasonable under the circumstances to maintain secrecy." It will then develop a model based on a cost-benefit analysis to aid companies in constructing or refining their trade secret protection programs. Finally, this article will demonstrate, within the constraints established by the requirements of "efforts reasonable under the circumstances," how any company, large or small, can develop an effective program using cost-benefit analysis.

II. TRADE SECRET PROTECTION

A. *Policy of Trade Secret Protection*

Trade secret protection has been traced back to 1851 in England[2] and 1868 in the United States.[3] Over the last 100 years, the common law of trade secret protection has developed from two fundamental policy objectives: (1) the maintenance of standards of commercial ethics; and (2) the encouragement of research and innovation.[4] Trade secret law protects against the misappropriation of one's investment of time and labor in developing information, products or processes.[5] Trade secret law does not protect secrecy as such, but protects against unlawful means of unveiling the secret.[6] Because the law affords no rights to the information if it is voluntarily disclosed, the trade secret owner must undertake reasonable efforts to prevent its disclosure.

B. *Trade Secret Status at Common Law*

Although the prerequisites for trade secret protection at common law have varied from state to state and from time to time, the cases indicate that three elements are generally required for trade

---

petitors. DuPont alerted the FBI and the sting operation was put into action. Police arrested four people carrying thousands of DuPont documents in Geneva, Switzerland.

2. Morison v. Moat, 68 Eng. Rep. 492, 9 Hare 241 (1851).

3. Peabody v. Norfolk, 98 Mass. 452 (1868).

4. Fleming Sales Co. v. Bailey, 611 F. Supp. 507 (D.C. Ill. 1985); E.I. duPont deNemours Powder Co. v. Masland, 244 U.S. 100 (1917); E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970). One commentator notes that the sole policy behind trade secret protection is that allowing a free ride on the intellectual endeavor of another is unjust. R.A. Klitzke, *Trade Secrets: Important Quasi-Property Rights*, 41 BUS. LAW. 555, 558 (1986).

5. E.I. duPont deNemours & Co. v. Christopher, 431 F.2d at 1015.

6. Clark v. Bunker, 453 F.2d 1006, 1009 (9th Cir. 1972).

secret status. The trade secret must (1) be used in one's business, (2) provide a competitive advantage to its owner, and (3) be secret.[7]

Secrecy is an illusive and critical requirement for the trade secret owner. In determining whether the secrecy element has been met by the claimant, courts will look to whether the information was generally known or available and whether reasonable efforts were undertaken by the claimant to maintain secrecy.[8] It is clear that the trade secret owner must take some affirmative steps to maintain secrecy; a plan of taking no special precautions for fear of arousing undue interest in the information is sure to fail.[9]

C. *Modern Developments in Trade Secret Protection*

In 1979, the commissioners on Uniform State Laws adopted the Uniform Trade Secrets Act (UTSA), attempting to normalize trade secret law among the states.[10] The UTSA essentially codifies the best-reasoned decisions at common law with regard to trade secret protection.[11] Case law prior to the adoption of UTSA is instructive for determining trade secret status in those states that have adopted the UTSA, as well as those that have not.[12]

The UTSA defines a trade secret as:

> [I]nformation, including a formula, pattern, compilation, program, devise, method, technique, or process, that: (1) Derives independent economic value, whether actual or potential, from

---

7. *See, e.g.*, Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 474 (1974); FMC Corp. v. Taiwan Tainan Giant Indus. Co., 730 F.2d 61, 63 (2nd Cir. 1984). This tripartite test is derived from the RESTATEMENT OF TORTS, § 757 comment b. Recently, courts have not required the trade secret to be actually used in the owner's business. Instead, the focus is on the actual or potential commercial value of the trade secret and the element of secrecy. *See* Syntex Ophthalmics, Inc. v. Tsuetaki, 701 F.2d 677, 683 (7th Cir. 1983); Reinforced Molding Corp. v. General Electric Co., 592 F. Supp. 1083, 1087 (W.D. Pa. 1984); *See* CAL CIV. CODE § 3426.1 (d) (Deering 1989).

8. Junkunc v. S.J. Advanced Technology & Mfg. Corp., 149 Ill. App. 3d 114, 498 N.E.2d 1179 (1986).

9. J.T. Healy & Son, Inc. v. James A. Murphy & Son, Inc., 357 Mass. 728, 260 N.E.2d 723 (1970).

10. Uniform Trade Secrets Act, 14 U.L.A. 537 (1980). The following states have enacted the Uniform Trade Secrets Act: Arkansas, California, Colorado, Connecticut, Delaware, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nevada, North Dakota, Oklahoma, Oregon, Rhode Island, Virginia, Washington, West Virginia and Wisconsin.

11. Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 898 (Minn. 1983); American Paper and Packaging Products v. Kirgan, 183 Cal. App. 3d 1318, 228 Cal. Rptr. 713 (1986); Uniform Trade Secrets Act, 14 U.L.A. 537, 538 (1980).

12. To the extent the Uniform Trade Secret Act modifies or clarifies the common law, it will be followed. Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 898 (Minn. 1983).

not being generally known; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[13]

The UTSA definition of trade secret reflects the most contemporary language developed at common law, omitting the requirement that the trade secret be used in one's business.[14]

Under the UTSA, as at common law, the two critical factors for trade secret status are commercial value and secrecy. Once commercial value and secrecy have been established, the focus of the inquiry shifts to the defendant's conduct in obtaining the trade secret. However, for the trade secret owner, the first and foremost consideration is establishing trade secret status.

A trade secret has commercial value if it derives independent economic value from being secret, or if substantial time and money would be required of a competitor to develop the same information.[15]

Because establishing the commercial value of a trade secret is a relatively simple task, the primary consideration is designing and implementing a trade secret program that will stand the "reasonable efforts" test and assure a determination of trade secrets status.

III. EFFORTS THAT ARE REASONABLE UNDER THE CIRCUMSTANCES TO MAINTAIN SECRECY

From a review of the history and policy of trade secret protection and the various cases defining reasonable efforts, a model can be constructed by which a trade secret claimant can design a trade secret protection program which accounts for the legal requirements as well as the situational factors. Efforts that are reasonable under the circumstances are those actual efforts directed at specific trade secrets which are rigorous enough to force another to use improper, unethical or illegal means to discover or make use of one's trade secrets yet which are not necessarily so extensive as to make discovery impossible. From this general proposition, the trade secret owner must identify the universe of applicable efforts which

13. Uniform Trade Secrets Act, 14 U.L.A. 537, 538 (1980); *See* CAL. CIV. CODE § 3426.1(d) (Deering 1989).

14. *See* Epstein and Levi, *Protecting Trade Secret Information: A Plan for Proactive Strategy*, 43 BUS. LAW. 887, 894 n.55 (1988).

15. *See, e.g.*, CAL. CIV. CODE § 3426.1(d) (Deering 1989); Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W. 2d 890, 900 (Minn. 1983). *See* Religious Technology Center v. Wollersheim, 796 F.2d 1076 (9th Cir. 1986), *cert. denied* 107 S. Ct. 1336 (1987), where one church sued a splinter church, alleging that stolen scriptural materials were trade secrets, the court held that a trade secret could not be based on spiritual advantage because no commercial advantage was established.

may be made to protect trade secret status. From this set, the trade secret owner must select, based on a cost-benefit analysis, which efforts will be undertaken.

By its very nature, the requirement of reasonable efforts calls for a factual determination on a case-by-case basis. There is no bright-line rule to ensure that the secrecy element is met in all cases.[16] A court will scrutinize the claimant's efforts from hindsight, deciding from the perspective of today's knowledge and insight whether yesterday's efforts were reasonable.

From a planning perspective, the trade secret owner must consider how a court will view the efforts in hindsight when determining whether they were reasonable under the circumstances. The trade secret owner must be aware of situational factors and how they will figure into a court's analysis. Because situational factors are constantly changing, a viable trade secret protection program requires regular evaluation and definition of the owner's secrets, as well as monitoring changes in the marketplace and in the status of available information.[17]

In designing a trade secret protection program, there are essentially two parameters with which to contend. The first parameter is the legal environment — requirements established by law to obtain trade secret status. The second parameter is the circumstances — situational factors which affect the determination of what is reasonable.

A. *Legal Requirements*

To meet the reasonable efforts test, the law requires the trade secret owner to undertake actual efforts[18] which are rigorous enough to force another to use improper, unethical or illegal means to discover the trade secret.[19] Stated another way, the law requires the claimant to take those steps necessary which substantially protect confidentiality and reduce the risk of voluntary or inadvertent disclosure, without requiring the claimant to employ such efforts as would guarantee continued confidentiality. Whether the steps actu-

16. Jet Spray Cooler, Inc. v. Crampton, 361 Mass. 835, 282 N.E.2d 921 (1972).

17. Future Plastics, Inc. v. Ware Shoals Plastics, Inc., 340 F. Supp. 1376, 1383 (D.S.C. 1972) (quoting J.T. Healy & Son, Inc. v. James A. Murphy & Son, Inc., 260 N.E.2d 723 (1970)) (trade secret owner must exercise constant vigilance).

18. Electro-Craft, Inc. v. Controlled Motion, Inc., 332 N.W.2d 890, 901 (Minn. 1983).

19. Clark v. Bunker, 453 F.2d 1006, 1009 (9th Cir. 1972); Henry Hope X-Ray Products, Inc. v. Marron Carrel, Inc., 674 F.2d 1336, 1340 (9th Cir. 1982); Anaconda Company v. Metric Tool & Die Company, 485 F. Supp. 410, 421 (E.D. Pa. 1980).

ally taken to reach that objective are reasonable depends on the situational factors.

There are four legal guidelines which a trade secret owner must consider: (1) the efforts to maintain secrecy need not prevent improper means of discovery; (2) the efforts must be actual; (3) the trade secret must be treated as secret; and (4) the efforts must be directed at the trade secrets.

1. Efforts Need Not Prevent Improper Means

Trade secret law does not protect secrecy. On the contrary, the trade secret claimant is charged with the burden of maintaining secrecy. The efforts required to maintain secrecy are only those which are reasonable under the circumstances, not all conceivable efforts or those which are so extensive as to make discovery impossible.[20] The trade secret owner is not required to "guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available."[21]

In *E.I. duPont deNemours & Company v. Christopher*,[22] the court noted that the law does not require unreasonable precautions to prevent another from doing that which he ought not do in the first place. While reasonable precautions are necessary, "an impenetrable fortress is an unreasonable requirement."[23]

The trade secret owner is primarily charged with maintaining secrecy such that there would be difficulty in acquiring the information except by use of improper, unethical or illegal means.[24] Reasonable efforts are those that leave little opportunity for misappropriation except by improper conduct.[25]

---

20. Surgidev Corporation v. Eye Technology, Inc., 828 F.2d 452, 455 (8th Cir. 1987).

21. E.I. duPont deNemours & Co. v. Christopher, 431 F.2d at 1016 (5th Cir. 1970); *See also* Aries Information Systems, Inc. v. Pacific Management Systems, Inc., 366 N.W.2d 366 (Minn. App. 1985).

22. 431 F.2d 1012 (5th Cir. 1970). The defendant was hired by an unknown third party to take aerial photographs of a new methanol plant while it was under construction. The photographs revealed the trade secret process which the plaintiff had developed for producing methanol. The court held that the defendants had improperly appropriated plaintiff's trade secret, noting that it would be too much to impose on the plaintiff the enormous expense of erecting a roof over the construction site to "prevent nothing more than a school boy's trick." *Id.* at 1016.

23. *Id.* at 1017.

24. Clark v. Bunker, 453 F.2d 1006, 1009 (9th Cir. 1972); Henry Hope X-Ray Products, Inc. v. Marron Carrel, Inc., 674 F.2d 1336, 1340 (9th Cir. 1982).

25. E.I. duPont deNemours & Co. v. Christopher, 431 F.2d at 1016 (5th Cir. 1970).

2. Efforts Must Be Actual

It is clear that the efforts must be actual, affirmative measures. Mere intent to maintain secrecy is not enough.[26] The trade secret claimant must manifest its intent by making some effort to keep the information secret.[27] The law also requires such efforts to be a continuing course of conduct, signalling to all concerned that the information is secret.[28]

3. Trade Secret Must be Treated as Secret

An overriding principle in determining whether efforts are reasonable is whether the trade secret claimant treated the information as confidential. In *Capsonic Group, Inc. v. Plas-Met Corporation*,[29] an employer brought a suit alleging that employees had improperly appropriated trade secrets. In ruling for the defendants, the court found that there was no showing that plaintiff treated its information as confidential or restricted.[30]

In *Electro-Craft Corporation v. Controlled Motion, Inc.*, the court noted that a necessary element of trade secret status is proof of a continuing course of efforts reasonable under the circumstances to maintain secrecy.[31] The court noted that the owner's efforts must include some combination of physical security measures and confidentiality procedures.[32]

a. Security Measures

In finding Electro-Craft's security measures inadequate, the court noted: the main plant had seven unlocked entrances without signs restricting access; employees were not required to wear badges; drawings and plans were discarded rather than destroyed; and sensitive documents were not kept in a central or locked location.[33]

There are many physical security measures which can be employed to maintain secrecy. Physical security measures include:

26. Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 901 (S. Ct. Minn. 1983).

27. *Id.*

28. *Id.*

29. 361 N.E.2d 41 (Ill. App. 1977).

30. *Id.* at 44.

31. 332 N.W.2d 890 (Minn. 1983). The plaintiff, a manufacturer of brushless electric motors, brought an action against a competitor, claiming misappropriation of trade secrets with respect to the internal operation of the motors.

32. *Id.* at 902.

33. *Id.*

locks on entrances; buzzer locks on doors to sensitive areas; visitor screening and the use of badges; exclusion of the general public; shredding of sensitive documents; disclosing information to employees on a need-to-know basis; physically separating sensitive work areas from the rest of the facility; locked files; exclusion of visitors from vicinity of machines which are proprietary in nature; use of screens and barriers during tours; and physically locating the plant in a geographically remote area.

b. Confidentiality Procedures

In finding Electro-Craft's confidentiality procedures inadequate, the court noted that the claimant: did not inform its employees of the secret nature of the information; did not mark as confidential the drawings, dimensions and parts sent to customers and vendors; did not restrict employee access to documents; conducted informal tours for vendors and customers without warning as to the confidential nature of the information; and conducted an "open house" at which the public was invited to observe manufacturing processes.[34]

i. General Procedures

There are various confidentiality procedures that may be used to preserve trade secret status, including: disclosure of sensitive information to employees and outsiders only on a need-to-know basis; proprietary markings restricting the use and disclosure of the secret; copyrighting; contract clauses acknowledging the secret to be the property of the owner; confidentiality agreements; posting notices in sensitive work areas warning of the confidential nature of the information; and obtaining acknowledgments from employees confirming their understanding that specific trade secrets are confidential and not to be disclosed or used except in carrying out the tasks of their employment.

ii. Notice to Employees

One of the most critical means of establishing the secrecy of information is to put employees on notice of its confidential nature and restrict access to those employees who need to use it to carry out their jobs.[35] The employees should be informed of the specific information which constitutes a trade secret and must be instructed

34. *Id.* at 902-03.

35. Aries Information Systems, Inc. v. Pacific Management Systems, Inc., 366 N.W.2d 366, 366 (Minn. App. 1985); Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 892

not to disclose the secret to others. An employee cannot be expected to keep in confidence that which he does not know is secret.[36] No special situational factors come into play here. The necessity of informing employees of the existence of trade secrets and restricting access to them is fundamental to any trade secret protection program.

iii. Disclosure to Third Parties

It may be necessary for the trade secret owner to disclose a trade secret to someone outside of his employment. Nonetheless, the trade secret owner can maintain trade secret status if appropriate steps are taken. In *RTE Corporation v. Coatings, Inc.*,[37] the claimant disclosed a welding process to a welding company so that the latter could manufacture a device according to specifications. Disclosure of the trade secret in this circumstance was necessary for the claimant to carry on its business. In such a situation, the owner may disclose the trade secret and maintain protection if it is disclosed in confidence and there is a legitimate need to disclose.[38] The claimant must make it clear to the other that the information is a trade secret, that disclosure is in confidence and further disclosure or use of the secret for other than the purpose for which it was disclosed is prohibited.[39]

If outside tours are to be conducted, the trade secret owner must ensure confidential information is not inadvertently disclosed. If a tourist is allowed to view a secret process or information, it may be viewed as an indiscriminate and unnecessary disclosure, indicating either that the claimant did not intend to keep the information secret or that the information was not, in fact, secret.

In *Anaconda Company v. Metric Tool & Die Co.*,[40] the trade secret claimant allowed visitors in the plant and conducted tours of its facilities.[41] In spite of the contact by outside persons, the court found in favor of the trade secret owner since the efforts to maintain

---

(Minn. 1983); Wilson Certified Foods, Inc. v. Fairbury Food Products, Inc., 370 F. Supp. 1081 (D.C. Neb. 1974).

36. *See* Dynamics Research Corp. v. Analytic Services Corp., 9 Mass. App. 254, 400 N.E.2d 1274 (1980).

37. 84 Wis. 2d 105, 267 N.W.2d 226 (1978).

38. *Id.* at 117-18, 267 N.W.2d at 232.

39. *Id.* at 117-18, 267 N.W.2d at 232.

40. 485 F. Supp. 410 (E.D. Pa. 1980).

41. *Id.* at 415. *See infra* notes 80-81, and accompanying text. Anaconda's maintenance staff erected screens and barriers around the machines when tours were conducted "with the greatest screening surrounding those machines closest to the tour aisle." 485 F. Supp. at 415.

secrecy were reasonable to restrict access and to signal the confidential nature of the information.

The cases demonstrate that, in dealings with third parties, certain rules must be observed. First, proprietary information should be disclosed only to those persons necessary for the claimant to carry on its business. Second, if the information must be disclosed, notice must be given that the information is a trade secret, is communicated in confidence, and is not to be disclosed to others or used beyond its intended purpose. These steps must be taken whether or not the third party is a competitor. Failure to do so indicates that the claimant does not consider the information confidential. If the claimant is operating in a highly competitive industry (a situational factor to be considered), plant tours and other marginally necessary disclosures may have to be restricted or even eliminated.

In *Electro-Craft*, the trade secret claimant should have informed its employees, in no uncertain terms, exactly what information constituted a trade secret.[42] Two situational factors, the prevalence of cross-hiring in the industry and the nature of the trade secret, were the circumstances that should have been accounted for by Electro-Craft in designing its trade secret protection program. Because Electro-Craft did not treat the information as confidential, the employees did not know, and could not infer from internal procedure, that certain information was confidential.[43] Had the employees been given proper notice of confidentiality, the subsequent appropriation would have violated the confidential relationship and would have been improper.[44]

4. Efforts Must be Directed at Trade Secrets

In establishing trade secret status, more is required than general business security. Reasonable efforts are those directed at specific information. In *Wilson Certified Foods, Inc. v. Fairbury Food Products, Inc.*,[45] the claimant's manufacturing plant had a security system requiring each person entering the plant to be questioned by a guard, issued a pass and accompanied by a Wilson employee at all times. Furthermore, the sole entrance to the processing area stood in front of the foreman's office.[46]

---

42. *Electro-Craft*, 332 N.W.2d at 902-03.

43. The court noted that security measures are one way to signal to employees that certain information is confidential. *Id.* at 902, n.15.

44. *Aries Information Systems*, 366 N.W.2d at 369 (Minn. App. 1985).

45. 370 F. Supp. 1081 (D.C. Neb. 1974).

46. *Id.* at 1085.

The *Wilson* court noted the following in holding that Wilson had failed to take reasonable efforts to maintain secrecy: sensitive documents were kept in an unlocked desk with unrestricted access; a general description of the manufacturing process was distributed to Wilson's sales brokers; operators were not cautioned that the process was confidential; and 10 to 12 tours per year were conducted through the production area.[47]

Although Wilson had a general security system, it failed to direct its efforts at preserving the confidentiality of secret information. Specifically, Wilson did not undertake efforts which would signal that certain information was confidential and which were rigorous enough to force another to use improper, unethical or illegal means to discover the information.

B. *The Circumstances — Situational Factors*

While there is an evergrowing list of efforts that can be undertaken by a trade secret owner, the primary concern is to select and implement those efforts which are reasonable under the circumstances yet not necessarily so extensive (commensurate with expenses) as to make discovery impossible. To make this selection, the trade secret owner must first define the universe of efforts which are applicable under the circumstances. The second step is to balance the costs and benefits of each applicable effort in making the final selection of applicable efforts for its trade secret protection program.[48]

There are essentially three situational factors to consider in choosing the applicable efforts to maintain secrecy: (1) the nature of the trade secret; (2) the nature of the industry (including the prevalence of industrial espionage); and (3) the nature of the company.

1. The Nature of the Trade Secret

a. Obviousness

The nature of the trade secret will determine what efforts are required to maintain trade secret status. Certain trade secrets, such as a secret formula, are discrete and of obvious value. Other trade secrets are not so discrete. In *Electro-Craft*,[49] the court noted that the claimed trade secret was of a nonintuitive nature, requiring the

47. *Id.* at 1085-86.
48. *See*, note 62 *infra* and accompanying text.
49. Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890 (Minn. 1983).

claimant to inform the employees of the confidential nature of the specific information.[50] Presumably, if the claimed trade secret had been a discrete formula, the value and secrecy of which was obvious to the employees, the court may have found trade secret status notwithstanding that the employees were never specifically instructed on the confidential nature of the information.[51]

b. Value

Similarly, the value of the trade secret to the company will determine, in part, what efforts are reasonable to maintain trade secret status. If a company derives all or a substantial portion of its revenues from a single trade secret, it is reasonable to expect the company to undertake more extensive efforts to maintain secrecy than if the trade secret is responsible for little or marginal revenue.[52] Conversely, one cannot reasonably be expected to spend more time and energy protecting a trade secret than is commensurate with its value.

2. Nature of the Industry

a. Competitive Industries

The nature of the industry is another situational factor for consideration in selecting applicable measures to protect trade secret status. In a highly competitive industry, such as the communications or computer fields, information is at a premium.[53] It is rea-

50. *Id.* at 902.

51. *See also* Anaconda Company v. Metric Tool & Die Company, 485 F. Supp. 410 (E.D. Pa. 1980). The owner did not specifically inform its employees of the trade secret status but security measures were enough to signal to the employees the trade secret nature of the information.

52. *See* Coca-Cola Bottling Co. v. Coca-Cola Co., 227 U.S.P.Q. 18, 22 (D. Del. 1985). Coca-Cola's valuable soft drink formula was the subject of extensive efforts. The written version of the secret formula was kept in a security vault; the vault could only be opened upon board resolution; only two persons in the company, whose identities were not disclosed, ever knew the formula; and the two persons were not allowed to fly on the same airplane.

53. The competitive battle between Proctor & Gamble and Wilson Harrell is illustrative of the value of protecting ones business plans. In the early 1960's, Wilson Harrell purchased an obscure wholesale cleaning spray liquid called "Formula 409." By 1967, after a nationwide retailing effort, Formula 409 had a 5% share of the U.S. market for cleaning products and a 50% share of the spray cleaning segment. In 1967, Proctor & Gamble began test marketing a spray cleaner called "Cinch." Wilson Harrell learned of Proctor & Gamble's plans to introduce the product and discovered that Denver was to be the first test market. Wilson suddenly withdrew Formula 409 from the Denver market. As a result of this tactic, Cinch did extraordinarily well in the test market. When Proctor & Gamble began its national launch of Cinch, Harrell retaliated. He had pumped up Proctor & Gamble's expectations with his withdrawal of Formula 409 from the Denver market, but the overall strategy was to make the Proctor & Gamble executives lose confidence in their product. Harrell bun-

sonable to expect a trade secret owner in a competitive industry to account for the fact that competitors are constantly lying in wait to obtain information at little or no cost.

It is quite common for businesses in a competitive industry to hire employees away from competitors to obtain information.[54] Therefore, the trade secret owner must define the trade secret, restrict its access on a need-to-know basis, inform employees of the specific trade secrets, and instruct them that disclosure is prohibited. This precaution will give rise to a duty on behalf of the employees not to disclose the trade secrets.[55]

b. Prevalence of Industrial Espionage

Another consideration is the prevalence of espionage in the particular industry. While a trade secret claimant will be protected from espionage which it could not have reasonably anticipated or prevented,[56] the claimant, in certain industries, may be called upon to take some measure to thwart industrial espionage in order to protect its trade secret status. In *Electro-Craft*, the court held that a lax security system by itself did not preclude a finding of reasonable efforts, noting that industrial espionage was not a major problem in the particular industry.[57] However, if the industry is one in which industrial espionage is common, a court may very well require the claimant to undertake security measures which would not otherwise be required. At the very least, manufacturing processes or other sensitive information should be blocked from plain view by four

---

dled his 16 ounce size of Formula 409 with the half gallon size and sold them at a low price. Harrell intended to load up the typical spray cleaner consumer with about six months worth of the product. He advertised and promoted the bargain heavily. While Proctor & Gamble was putting much of its huge Cinch investment into a national advertising campaign, Formula 409 users did not need any more spray cleaner. The only customers left were new users, and there were not nearly enough of them to justify Proctor & Gamble's expenditures on Cinch. Within a year, Proctor & Gamble withdrew its new spray cleaning product from the shelves. It was Harrell's ability to learn of the Proctor & Gamble plans for the introduction of its new spray cleaning product, that allowed him to develop a strategy to prevent the product's success. Similarly, if Proctor & Gamble was able to learn about Harrell's strategy, Proctor & Gamble could have adjusted its expectations and avoided the loss of millions of dollars. SOLMAN & FRIEDMAN, LIFE AND DEATH ON THE CORPORATE BATTLEFIELD, 24-27 (1982).

54. *See* Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 902 (Minn. 1983).

55. Aries Information Systems, Inc. v. Pacific Management Systems, Inc., 366 N.W.2d 366, 369 (Minn. App. 1985).

56. *Id. See also* E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970).

57. 332 N.W.2d at 902.

walls and a roof.[58]

3. Nature of the Company

The final situational factor for consideration is the nature of the company.

a. Size

In *Data General Corp. v. Digitial Computer Controls*,[59] the court noted that, due to the small size of the company, plant security did not need to be as thorough as that of IBM. It stands to reason that a small company with few employees need not undertake the extensive security measures that might be necessary for a large company with many employees. Assuring security for a small plant with few employees might be accomplished through simple devices like locking entrances or storing sensitive documents in a locked desk.

b. Plant Layout

The physical office or plant layout must also be considered in determining what measures should be undertaken to maintain secrecy. If sensitive areas are accessible to employees without a need to know, an inadvertent disclosure may result. Physical separation may be necessary to prevent inadvertent disclosure. One successful trade secret owner physically separated a sensitive department from the central facility and kept secret documents in locked files to establish trade secret status.[60]

c. Financial Strength

The financial strength of the company may be a relevant consideration in selecting applicable efforts. It will certainly be a relevant business consideration. It may be considered reasonable to require a financially strong company to implement extensive measures to maintain secrecy for a valuable trade secret. On the other hand, a new or financially unstable company may not be required to risk financial ruin in order to install an intricate security system. The financial strength of the company will likely be a consideration secondary to the value and nature of the trade secret and the nature of the industry because the trade secret owner will likely be com-

58. 431 F.2d at 1016 (5th Cir. 1970).
59. 357 A.2d 105, 111.
60. Surgidev Corporation v. Eye Technology, Inc., 828 F.2d 452, 455 (8th Cir. 1987).

pelled to undertake certain minimal efforts notwithstanding financial strength.

C. *General Approach*

Most trade secret protection programs will include certain minimum efforts. First, the trade secret owner should consciously identify the trade secret. Second, the trade secret should be marked as proprietary, whether it is viewed solely by employees or by outside parties. If a trade secret is embodied in a form other than a document, signs should be posted proclaiming its proprietary nature.[61] Third, access to the secret information should be restricted solely to those employees who have a need to know to carry out their job functions. Fourth, as to those employees to whom the information is accessible, notice must be given that the information is proprietary and secret. Furthermore, these employees must be instructed not to disclose the information to any other person or to use the information other than for carrying out their jobs. Fifth, if proprietary information must be disclosed to third parties (whether vendors, purchasers or licensees), a confidentiality agreement must be obtained prior to disclosure. The agreement should specifically set forth the information that is considered confidential and explicitly state that the information is not to be disclosed to any other party or used for any other purpose other than that for which it was disclosed. Finally, security measures must be implemented as a signal to employeee and outsiders that certain information is secret.

While the particular situational circumstances will determine the extent of security measures undertaken, certain minimum efforts must be made. Doors should be locked and access to sensitive areas restricted. Sensitive documents should at least be locked in a desk or cabinet to which access is restricted. Sensitive documents should not be discarded, but should be destroyed, if only by manual tearing.

In constructing a trade secret program, in addition to balancing the legal requirements with the situational factors, the trade secret owner should keep in mind that the overriding principle is to treat the information as confidential. The owner must put the world on notice, whether by security measures or confidentiality procedures, that the information is valuable, secret and not to be disclosed.

The following section evaluates, on a cost-benefit basis, the

61. For example, a machine.

business considerations of a trade secret program within the legal framework of common law decisions and the UTSA. It will examine the various business considerations (the value of the trade secret to the company, the costs of protecting the trade secret, and the risks of losing trade secret status) that must play a part in the final selection of applicable efforts to maintain trade secrecy.

IV. Using Cost-Benefit Analysis to Construct a Viable Trade Secret Protection Program

Companies that are in the process of developing a trade secret program and those already employing one can use cost-benefit analysis to determine the scope and desired effectiveness of their programs. This decision involves determining the desired protection by balancing the cost of the program with the goals of achieving adequate protection and minimizing the risks of disclosure.[62]

The costs expended and benefits obtained lie on a continuum of risk. At one extreme, there are efforts which courts have determined to be reasonable and are highly likely to remain so again in the future. These are comprehensive trade secret protection programs which include procedures for identifying and defining trade secrets, isolating or restricting access to them and putting others on notice that certain information is secret. Depending upon the economic value and nature of the trade secret, they require varying amounts of time, energy and money.

Towards the center of the continuum are efforts which courts have upheld as reasonable but with less conviction. Although the risk is greater, it is likely that these types of efforts will also be upheld as reasonable. The programs are less comprehensive, less expensive, but are characterized by a greater likelihood of being found inadequate by a court and thus provide less assurance to the trade secret owner. These programs include less formal and less clearly defined procedures for identifying and defining trade secrets, restricting access to them and putting others on notice that certain identified information is secret.

At the other end of the continuum are efforts which courts have held to be unreasonable or inadequate. These programs are modest and entail very high risk. They fail to include procedures in one or more of the critical areas or have been compromised in one fashion or another.[63] It is highly likely that the owner of the secret

62. Risk as used herein means the likelihood that the companies efforts to maintain secrecy will be found inadequate by a court of law.

63. CVD, Inc. v. Raytheon Company, 769 F.2d 842 (1st Cir. 1985). Raytheon claimed

information, who employs this type of program, will be denied the protection of trade secret law and will have no remedy against a misappropriator.

In order to avoid unnecessary mistakes, companies should pay close attention to the continuum of risk and use cost-benefit analysis when forming or evaluating their trade secret programs.

A. *Efforts Which Are Reasonable Under the Circumstances to Maintain Secrecy*

As previously discussed, efforts reasonable under the circumstances to maintain secrecy are actual efforts directed at specific trade secrets, rigorous enough to force another to use improper, unethical or illegal means to discover or make use of one's trade secrets, yet not so extensive as to make discovery impossible. Such efforts must include, to the extent appropriate relative to the nature of the trade secret, the nature of the company and the nature of the industry, identifying and defining one's trade secrets, marking them as proprietary, isolating or restricting access to them and putting others on notice that certain information is secret by means of security measures or confidentiality procedures.

In *Valco Cincinnati, Inc. v. N & D Machinery Service, Inc.*,[64] Valco claimed that information gathered over a twenty-four year period through its engineering, experimentation and expertise, which allowed Valco to develop a standard inspection of materials, processes, dimensions and tolerances of its product was its trade secret.[65] The appellate court affirmed the trial court's holding that Valco had taken reasonable precautions to safeguard its trade secrets.[66] Valco's plant had more than adequate locking devices; a receptionist screened every visitor to the building; Valco used a buzzer lock system on the door to the processing area which was operated by the receptionist; the general public was never taken through the plant; competitors were never authorized within the plant; Valco's drawings were made available to their suppliers only

---

elements of its chemical vapor deposition process used to manufacture zinc selenide and zinc sulfide were trade secrets. The court stated that Raytheon's failure to follow its own established procedures for the protection of trade secrets was a significant factor in denying Raytheon trade secret status for its manufacturing process. *Id.* at 853.

64. 24 Ohio 3d 91, 492 N.E.2d 814 (Sup. Ct. Ohio 1986). Valco Cincinnati, Inc., a manufacturer of parts for a commercial glue applicator, brought an action for wrongful appropriation of trade secrets and sought to enjoin N & D Machinery Service, Inc. from manufacturing certain replacement parts for Valco's products. *Id.* at 815.

65. *Id.* at 816.

66. *Id.* at 819.

for the limited purpose of bidding on the manufacture of certain parts; drawings were made available only to employees with a specific need for them; all drawings that left the plant were required to have a proprietary marking restricting their use and disclosure; a shredder was utilized to destroy all computer printouts and old drawings; and the company had a policy of obtaining nondisclosure agreements from its key employees.[67]

Valco's trade secret protection program was comprehensive. Its use of numerous locking devices and the screening of each visitor went beyond mere intent to maintain secrecy and provided sufficient, actual security measures. The exclusion of the general public and competitors from the plant, restrictions on dissemination of documents to suppliers and employees, proprietary markings on drawings and use of nondisclosure agreements were efforts directed at specific trade secrets and were adequate to maintain confidentiality. These techniques of restricting access to information and alerting individuals to its confidential nature clearly signaled to employees and others that certain information was secret and should not be disclosed. As a result, in making use of Valco's trade secrets, Valco's former employees engaged in improper conduct — a breach of their fiduciary duty of confidentiality.

However, this program was costly. The exclusion of the public from the plant may have prevented Valco from increasing community support and the value of its goodwill. Tight restrictions on dissemination of information may decrease employee efficiency and doing business with third parties may become more difficult and time consuming. As a result, a company using this type of trade secret protection program may lose business opportunities. In addition, tight security measures may create an atmosphere of distrust and employee morale may suffer, resulting in decreased employee loyalty and productivity.

In *Aries Information Systems, Inc. v. Pacific Management Systems Corporation*,[68] Aries claimed that information which constituted its software product was a trade secret.[69] Because all of the

67. *Id.*

68. 366 N.W.2d 366 (Ct.App. Minn. 1985). Aries, a developer of financial accounting software named POBAS III, brought an action against its former employees seeking to recover damages for misappropriation of its trade secret. The former employees which had access to Aries software materials and present and prospective clients formed a separate company to compete with Aries. *Id.* at 366-67.

69. *Id.* at 368. Aries spent over $100,000 for research and development for POBAS I. As a result of improvements and additions, POBAS II was developed. After eight or ten years and substantial capital investment, POBAS II was transformed into POBAS III. *Id.* at

source code listings and magnetic tapes incorporating the software bore proprietary notices, Aries user manuals were copyrighted and stated that the information was proprietary, every customer contract stated that the software was the exclusive property of Aries, and its key employees signed confidentiality agreements, the court held that Aries took reasonable efforts to maintain secrecy.[70] The efforts went beyond intent, were directed at specific trade secrets and indicated the secrets were confidential.

By employing a program of this nature, Aries obtained significant benefits at a relatively low cost. Proprietary notices, copyright notices and nondisclosure agreements can be employed with minimal cost. These low cost methods should be part of every company's trade secret protection program.

Because the misappropriation was accomplished by employees of Aries, the company's physical security measures were not at issue. It was the efforts taken to maintain confidentiality which led the court to rule in favor of Aries. The court noted that "[i]t is difficult, if not impossible, to prevent an employee from discovering his employer's trade secrets."[71] Although preventing discovery is difficult, an employer must still seek to limit access to information and prevent disclosure by employees and others by signaling that certain information is secret and should not be disclosed. Aries used proprietary notices to identify its trade secrets and confidentiality agreements to put employees on notice that information was secret.

The decision in *Surgidev Corporation v. Eye Technology, Inc.*,[72] is illustrative. Surgidev took actual efforts, which were directed at specific trade secrets which put others on notice that sensitive information was secret. Surgidev's security procedures, including separating a sensitive department from the central facility and keeping secret documents in locked files, were held to be reasonable under the circumstances.[73] By physically separating one department from the central facility, access to sensitive information was restricted and the information was protected from discovery by outsiders.

367-68. Without its trade-secret protection program Aries' former employees would had been able to forego such an investment in time and money and compete directly with Aries.

70. *Id.* at 368-69.

71. *Id.* at 369.

72. 828 F.2d 452 (8th Cir. 1987). Surgidev, a manufacturer of intraocular lenses brought an action against a competitor and former employees for misappropriation of trade secrets, breach of contract and tortious interference with contractual relations. The district court's ruling that Surgidev took efforts reasonable under the circumstances to maintain the secrecy was affirmed. *Id.* at 452.

73. *Id.* at 455.

The use of locked files made the information less accessible to outsiders, providing even more protection. As a result of these security procedures, it would be very difficult for an outsider to discover Surgidev's trade secrets.

The overall cost of Surgidev's security procedures is unclear. The use of locked file cabinets is an easy, low cost method of securing documents. If one of the criteria for designing a plant is security, then separating a sensitive department or manufacturing area from the main plant would cost less than obtaining such separation after the plant is built. The separation, however, may not be cost-effective to the company's operation.

In addition, Surgidev's efforts to maintain the confidentiality of its proprietary information were deemed adequate. By requiring employees to sign non-disclosure agreements and restricting the distribution of secret materials on a strictly need to know basis, Surgidev identified its trade secrets and put its employees on notice of the trade secret status of matters on which they were working.[74]

An example of distribution on a strict need to know basis is Surgidev's practice with respect to the dissemination of sales reports. The hierarchial structure of the company was important in developing the method used. Field sales representatives received sales data only for their assigned sales territory.[75] Regional sales managers received sales data only for the regions to which they are assigned.[76] Only certain high level executives were exposed to company-wide sales figures.[77]

Although this method of restricted dissemination is effective at limiting the distribution of sensitive information, it also prevents employees from using the information for comparison, performance appraisal and as a motivating tool. It is this type of cost-benefit analysis, including the analysis of qualitative as well as quantitative costs and benefits, that a company must undertake to develop a trade secret protection program which meets its needs relative to the amount of risk it desires to assume and costs it is willing to undertake.

In each of these cases, the owners of the trade secrets made a substantial investment in time, energy and money to protect trade secrets which were critical to the operation and success of each

74. *Id.*

75. Surgidev Corporation v. Eye Technology, Inc., 648 F. Supp. 661, 694 (D. Minn. 1986).

76. *Id.* at 694.

77. *Id.*

company. As a result, comprehensive trade secret protection programs which included actual measures to maintain the security and confidentiality of the trade secrets which were directed at specific trade secrets were necessary. In such circumstances, a larger investment in time, energy and money is not only justified but it is probably required. In light of the nature of the trade secrets, including their economic value, a company in a similar situation should make a substantial effort to protect trade secrets and reduce the risk of misappropriation.

It is also important to note that former employees of each company were named as defendants. This indicates that a threat to a company may come not only from other companies but also it may come from employees of the trade secret owner. Management must be aware of the dual threat when constructing a trade secret program and the greater the employee turnover in the industry, the greater the threat of misappropriation by former employees.

B. *Efforts Which Are Probably Reasonable Under the Circumstances But Are Higher Risk*

For companies not having a comprehensive trade secret program, there are still steps that can be taken to protect sensitive information which courts may accept as reasonable under the circumstances.

In *Anaconda Company v. Metric Tool & Die Company*, the court held that Anaconda had taken reasonable efforts to protect its trade secret of a machine for producing telephone cord armor.[78] Anaconda had a tight security system. It maintained strict rules with respect to visitors.[79] For example, all visitors were required to be escorted through the facilities and not allowed to be brought near machines which were deemed proprietary in nature.[80] Moreover, screens and barriers were erected around the machines when tours were conducted, with the greatest screening surrounding those machines closest to the tour aisle.[81] Such security measures were sufficient to restrict access to the machines and communicate to outsiders that such machines were secret.

78. 485 F. Supp. 410 (E.D. Pa 1980). A manufacturer of telephone cord armor brought an action against a competitor alleging misappropriation and wrongful use of its alleged trade secret, a profile and winding machine which it engineered and built for the purpose of producing telephone cord armor. Telephone cord armor is a strip wound metal hose which protects a telephone cord from wear, tear, abuse and vandalism. *Id.* at 413.

79. *Id.* at 422.

80. *Id.* at 415.

81. *Id.*

In addition, Anaconda's confidentiality procedures were adequate. Proprietary information was disclosed on a need to know basis to its employees.[82] Furthermore, Anaconda never advertised or publicized its machine in any manner[83] and none of the machines had been publicly exhibited, described in any publication or sold.[84]

This type of program was risky because in spite of the great value of this machine, which was so complex that it permitted Anaconda to be the only producer of telephone cord armor,[85] the company did not specifically instruct its employees as to the proprietary nature of the machine.[86] Instead, through the use of its security measures and confidentiality procedures, Anaconda implicitly identified what was secret and restricted access to it. Considering the economic value of this type of machine, a more direct approach in providing notice to reduce the risk would have been appropriate.

Another example of a reasonable but risky program is found in K-2 Ski Company v. Head Ski Co., Inc.[87] The court held that exhibition of K-2 skis by one of K-2's suppliers at a conference, limited tours of K-2's plant and generally loose security measures did not destroy the secrecy of K-2's manufacturing procedure.[88]

K-2 skis were displayed at a conference in Washington, D.C. with the permission of K-2.[89] The supplier displayed two models of K-2 skis. One of which was displayed intact and the other cut lengthwise displaying the internal construction of the ski.[90] Since there was no evidence of attendance by the defendant or any other ski manufacturer, the court found that there was no public disclosure.[91]

In addition, only limited tours of the K-2 plant were conducted. Personnel from competitor ski manufacturers were not permitted to view the manufacturing operation.[92] Finally, the court

82. *Id.* at 422.
83. *Id.*
84. *Id.* at 415.
85. *Id.* at 414. Over 200 drawings were required to manufacture the machine. Between 70 and 100 separate sets of tooling were held in inventory for making a variety of metal hoses. Competitors were required to design and build their own machines because none had been offered for sale by equipment manufacturers. *See also supra* note 52 and accompanying text.
86. *Id.* at 415.
87. 506 F.2d 471 (1974). Action by manufacturer of skis against its former employee and competitor for damages and injunctive relief on grounds of unlawful use of plaintiff's trade secret.
88. *Id.*
89. *Id.* at 474.
90. *Id.*
91. *Id.*
92. *Id.*

found that, although security at the plant was not tight, this did not destroy secrecy because the plant was located in a remote area.[93]

The actions taken by K-2 put its trade secrets at risk. The case may have turned out differently if the defendants were able to present evidence that personnel from competing manufacturers attended the conference in Washington, D.C. The competitors may have been able to learn much about the manufacturing process by looking at the skis on display.[94] In addition, K-2 never warned its supplier and did not post notices that the manufacturing process of the skis was confidential, and, that any information revealed by observation of the manufacturing process was confidential.

Lax plant security is dangerous. Even though the plant was in a remote location and gaining access to the plant was difficult, access to secret information must be restricted to the extent that an individual must use improper, unethical or illegal means to obtain secret information.

In *Fleming Sales Company v. Bailey*,[95] Fleming had a general policy of maintaining the confidentiality of customer lists and virtually all other business information.[96] Each employee received a copy of a rules and regulations letter specifying that an employee would be terminated for exposing confidential information.[97] Fleming generally restricted dissemination of complete customer lists to only a few people.[98]

However, complete customer lists were supplied to Fleming principals from time to time; the company had no written policy or clearly articulated procedures for ensuring the confidentiality of customer lists; lists were not kept under lock and key or marked confidential; and salesman kept copies of partial lists in their offices.[99]

---

93. *Id.*

94. Although a competitor could buy K-2 skis, cut them lengthwise and study the ski, thereby learning much about the manufacturing process, this would be reverse engineering and K-2's rights in its trade secrets would be maintained against all but the party that reverse engineered the skis. *See* CAL. CIV. CODE § 3426 (Deering 1988). However, if K-2 provided the skis and a cross sectioned view to a competitor, it would have disclosed its trade secret and probably lost the protection afforded by trade secret law.

95. 611 F. Supp. 507 (E.D. Ill. 1985). Fleming, a family owned manufacturers' representative business, through its OEM Division was engaged in the marketing of component parts of recreational vehicles to recreational vehicle manufacturers. Fleming alleged that its former employee misappropriated its trade secrets, which included customer lists, customer information and sources of supply.

96. *Id.* at 512.

97. *Id.*

98. *Id.*

99. *Id.*

The nature of the company allowed it to use less restrictive measures in protecting secrecy of its customer lists. Since Fleming was a sales organization, constant dealings with customers by its employees were the essence of its business.[100] Distribution of customer list information to principals or customers on occasion may well have been necessary to Fleming's business. However, as long as Fleming scrupulously limited distribution of customer list information to employees and outsiders whose access was necessary to Fleming's successful pursuit of its business, it was deemed to have satisfied the reasonable efforts requirement.[101]

Although the court held in favor of Fleming, such loose restrictions on the dissemination of information increases the risk that such information will fall into the hands of an outsider and trade secret status will be lost. The lack of clear guidelines and procedures to be followed in storing and restricting access to such information is dangerous. It not only implies the company is not serious about security, but it increases the risk of inadvertent disclosure. Finally, failure to mark important information may negate the effect of other confidentiality procedures which put people on notice that information is secret. Fleming assumed the higher level of risk in order to reduce the costs of doing business.

The *Fleming* court's analysis makes it clear that it is not necessary to take all conceivable or even stringent efforts to maintain secrecy. However, the less comprehensive the measures taken, the more likely it is that a court may find that such efforts are not reasonable under the circumstances. This case has important implications for smaller, financially unstable companies. These companies may still protect their sensitive information without extraordinary expense.

C. *Efforts Which Are Not Reasonable Under The Circumstances*

As there are measures which are clearly reasonable, and some that are risky but probably reasonable, there are measures which will surely fail to pass a court's scrutiny.

In *Capsonic Group, Inc. v. Plas-Met Corp.*,[102] the court held that Capsonic failed to make reasonable efforts to protect its trade

100. *Id.*

101. *Id.*

102. 46 Ill. App. 3d 440, 361 N.E.2d 41 (1977). A company brought suit to enjoin former employees from competing with it in the business of designing and engineering molds to be used to produce metal and plaster parts.

secrets; namely, it never treated its information as confidential or restricted.[103] Since there were no guards at the unrestricted plant, passes were not required to enter the premises and important engineering drawings were not kept under lock and key,[104] Capsonic's security measures were deemed inadequate.

Likewise, its confidentiality procedures were deficient. People were taken on tours of the plant and were never told they were viewing a confidential process; engineering drawings were not marked confidential; and employees were never told their work was secret.[105] Capsonic failed to take any of the steps required to achieve trade secret protection. Its lack of security procedures failed to restrict access to secret information. Its failure to use proprietary or confidential markings indicated that it had not identified its trade secrets and therefore did not direct its efforts at specific sensitive information. Finally, its general lack of security and confidentiality procedures made it impossible to put anyone on notice that certain information was secret.

The court in *Electro-Craft Corp. v. Controlled Motion*,[106] acknowledged that Electro-Craft took some precautions in screening its handbook and publications for confidential information and requiring some of its employees to sign confidentiality agreements.[107] However, it held that measures taken by Electro-Craft were inadequate.[108]

Electro-Craft's security measures did not demonstrate sufficient effort to restrict access to sensitive information and thereby maintain secrecy.[109] Not only was security inadequate but the con-

---

103. 361 N.E.2d at 44.

104. *Id.*

105. *Id.*

106. 332 N.W.2d 890 (Minn. 1983).

107. *Id.* at 895. The confidentiality agreements were part of employment agreements reading in part as follows:

> Employee shall not directly or indirectly disclose or use at any time, either during or subsequent to the said employment, any secret or confidential information, knowledge or data of Employer (whether or not obtained, acquired or developed by Employee) unless he shall first secure the written consent of Employer. Upon termination of his employment, Employee shall turn over to Employer all notes, memoranda, notebooks, drawings or other documents made, compiled by or delivered to him concerning any product, apparatus or process manufactured, used or developed or investigated by Employer during the period of his employment; it being agreed that that same and all information contained therein are at all times the property of the Employer.

Id. at n.1.

108. *Id.* at 901-02.

109. *Id.* at 902. *See also supra* note 32 and accompanying text.

fidentiality procedures were fatally lax.[110] Electro-Craft never identified what was secret or provided notice to others that certain information was confidential and not to be disclosed. The failure of Electro-Craft to implement more security measures and confidentiality procedures indicated that it did not treat its sensitive information as secret.

Electro-Craft could have implemented low-cost measures which would have significantly decreased the risk of disclosure without substantially increasing the costs of doing business. Issuing policy statements and warnings with respect to what is secret and marking documents as confidential are relatively inexpensive measures.

In *Defiance Button Machine Company v. C & C Metal Products Corp.*,[111] the court held that the company's customer lists lost their character as a trade secret because the company failed to take reasonable steps to protect the lists.[112] Testimony revealed that Defiance did not intend to disclose its customer list and the disks upon which the customer list was stored were kept in a locked room.[113] However, the information was also left in the memory of a computer sold by Defiance to C & C Metal, from which it could be retrieved by using a password readily available in source books to which C & C Metal had access.[114] In failing to segregate the source books and erase the lists from the computer, Defiance did not take reasonable efforts to ensure secrecy of the lists.[115]

Because Defiance failed to provide escorts for C & C Metal personnel that were on its premises and use any of the computer security devices for restricting access to the computer and information stored therein, its security measures were found inadequate. Such lax security failed to restrict access to sensitive information or

110. 332 N.W.2d at 902. "Confidentiality was important in this case, for testimony demonstrated that employees in the servo motor business frequently leave their employers in order to produce similar or identical devices for new employer." *Id. See also supra* note 54 and accompanying text.

111. 759 F.2d 1053 (2d Cir. 1985).

112. *Id.* at 1053. In June, 1982, the assets of Defiance, including a computer, tools, dies, jigs, fixtures, work in progress, raw materials and finished goods, were sold at an auction. The buyer of the assets was C & C Metal Products Corp. C & C Metal was permitted to enter the premises of Defiance for the purpose of removing property purchased by C & C that was still in the custody of Defiance. C & C Metal hired a former Defiance employee to demonstrate the use of the computer. During a demonstration, the Defiance customer lists, which was on disks located on the premises, were printed out. *Id.* at 1057-58.

113. *Id.* at 1063.

114. *Id.*

115. *Id.* at 1063-64.

make it such that they would have to use improper means to obtain the trade secret.

Additionally, its confidentiality procedures were non-existent. The use of a proprietary notice or confidential marking that would appear on the computer screen and on any hard copy of the data may have made the difference in this case. Such notices would have indicated that Defiance had identified the list as a trade secret and put C & C Metal on notice that the information was secret and belonged to Defiance.

This case is important because of the proliferation of computers and the widespread use of data bases. Reasonable efforts to maintain secrecy in this context include the use of a computer operating system that prevents users from reading data they are not authorized to access. In addition, each user should be assigned an access number or personal identification code before access can be achieved. Such numbers should be periodically changed and when an employee leaves the company, his or her password should be suspended or retired to prevent subsequent computer access.

From the above analysis, it is apparent that cost-benefit analysis within a risk continuum framework provides a useful tool for constructing and modifying trade secret protection programs. Such analysis allows a company to tailor its trade secret protection program to its needs and set the level of expenditures it desires to incur in light of the amount of risk it desires to assume.

V. CONCLUSION

In order to protect the secrecy of sensitive information, the owner need not prevent discovery by improper means but must take actual steps, aimed at protecting specific information, which indicate that such information is secret. In choosing the steps necessary to meet the above legal requirements from the universe of possible protective measures, the owner must consider the circumstances — situational factors. These include the nature of the trade secret, the nature of the company and the nature of the industry in which the company operates. This will allow the trade secret owner to narrow the universe of choices to a group of potential protective measures.

Finally, in constructing a trade secret program, a trade secret owner must balance the costs and benefits of potential protective measures in light of the amount of risk the owner desires to assume. The owner can evaluate his risk preference by using the continuum of risk framework. By using this framework an owner can employ more costly measures that are almost certain to protect its trade

secrets. Alternatively, the owner may employ less expensive measures which are likely to protect the trade secrets but have a higher risk of being found inadequate, or the owner can forego protective measures entirely, thereby saving the cost thereof and can assume a high risk of appropriation of his trade secrets and a high risk that a court would deny him trade secret status for his sensitive information. Using cost-benefit analysis based upon one's risk preference, the owner can select from the group of potential protective measures those that will make up the protection program and tailor the program to the business needs of the trade secret owner.