DEFINING THE METES AND BOUNDS OF ADEQUATE SECURITY FOR TRADE SECRETS

Suffolk University Law School
JD Candidate, 2012
5 Tannery Brook Row, #5
Somerville MA 02144
M: 831-594-5056
E: Lsinger@nexgen.org

TABLE OF CONTENTS

DEFINING THE METES AND BOUNDS OF ADEQUATE SECURITY FOR TRADE SECRETS

INTRODUCTION

Trade secrets comprise a vast store of the knowledge that many businesses and commercial entities rely upon in the day-to-day operation and profitability of their organizations. In a certain sense, a trade secret may be thought of as a corollary to a patent. In the case of a patent, the quid pro quo for publicly disclosing the details of an invention is that the patent holder obtains a negative monopoly for the invention, usually twenty years from the date of filing of the patent.[1] This negative monopoly provides the patent holder with the legal assurance that no others may practice the technology covered by the claims of the patent for the period of the patent exclusivity. Thus, the patent holder can reap an economic advantage over others who are legally excluded from utilizing the patented technology.

Unlike patents, trade secrets enjoy no such legal monopoly. The economic value of a trade secret rests solely in the fact that the technology embodied in the trade secret is simply that; a secret held by its owner. Unlike a patent that has a finite expiration period, a trade secret has no statutory time limits. A trade secret and the competitive advantage that if confers, may last indefinitely or, if the associated secret is lost, the economic advantage of the secret may also be lost. Therefore, an organization that has developed or acquired unique and valuable technology faces the decision as to whether to pursue a patent with its limited life span or, maintain a trade secret that could last indefinitely or be lost immediately.

The existence of a trade secret is not always a straightforward determination and ordinarily is a question of fact. "The term "trade secret" is one of the most elusive and difficult concepts in the law to define. The question of whether an item . . . constitutes a "trade secret" is . . . normally resolved by a fact finder after full presentation of [the] evidence."[2]

In layman's terms, a trade secret is essentially as its name implies. It is a secret that a business can exploit to economic advantage over its competition. Two of the more well known examples of trade secrets are the formulas for Coca-Cola® or WD-40®. There is nothing magical about these products; one

---

[1] 35 USC 154(a)(2) (2010)

[2] *Lear Siegler, Inc. v. Ark-Ell Springs, Inc.,* 569 F.2d 286, 288 – 89 (5th Cir. 1978).

is a beverage sold in over 200 countries around the world, and the other is the favorite lubricant and cleaning solvent of countless contractors. While anyone can buy these products, only their respective manufacturers know the formulae used to produce them. By guarding these formulations closely, both companies have built commercial franchises that total in the billions of dollars annually.[3] Although these products have been often challenged by competitors eager to take their market share, because these formulations have been kept secret, competitors have thus far been prevented from creating true copies of these products. However, were the formulations for these products publicly disclosed (ignoring any tortious conduct) or the products reverse-engineered, the market shares enjoyed by these organizations would quickly erode. Therefore the overriding theme of a trade secret from a layman's perspective is that it must create an economic advantage to its owner and, it must be kept secret.

DEFINITIONS OF TRADE SECRETS

Twenty-five states and have adopted the definition of a trade secret in accordance with the Uniform Trade Secrets Act [hereinafter, "UTSA"], as follows:[4]

> Trade Secret means information, including a formula, pattern, compilation, program, device, method, technique or process, that:
> (i) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
> (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[5]

Although the layman's definition of a trade secret seems self-evident, there is some variation between the definitions afforded to the term trade secret in various states. For example, Alaska defines a trade secret as "Information [that] (A) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (B) is the subject of efforts that are reasonable

[3] Coca-Cola Corporation 2009 Form 10-K, Item 6: Selected Financial Data, p. 28. (In 2009 the Coca-Cola Corporation had gross sales of $31 billion representing $6.8 in billion net income.)
[4] 50 State Comparative Legislation/Regulations Trade Secrets (LexisNexis 2010)
[5] Unif. Trade Secrets Act, §1(4)(i)-(ii) (1985)

under the circumstances to maintain secrecy."[6] California's version of the UTSA exemplifies the UTSA's effort to broaden and define both the scope of the information covered as well as the population of entities to which it applies: "'Trade secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[7] Similarly, Delaware's UTSA version defines a trade secret as "information, including a formula, pattern, compilation, program, device, method, technique or process, that: (a) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (b) Is the subject of efforts that are reasonable under the circumstances to maintain secrecy."[8] In contrast, Texas has adopted a much simpler definition of a trade secret, as follows: "'Trade secret' means the whole or any part of any scientific or technical information, design, process, procedure, formula, or improvement that has value and that the owner has taken measures to prevent from becoming available to persons other than those selected by the owner to access for limited purposes."[9]

Although there is obvious variation between the definitions of a trade secret in states such as Texas versus the UTSA, the important point is that all definitions include a requirement that efforts be taken to safeguard trade secrets.[10] Nevertheless, the Arkansas Supreme Court adopted a six-prong test (based on the Restatement of Torts[11]) to determine the existence of a trade secret in *Tyson Food v. ConAgra*.[12] In that case, the court adopted the requirements of the:

> (1) extent to which the information is known outside the business;
> (2) extent to which the information is known by employees and others involved in the business;

---

6 Alaska Stat. §45.50.940 (2009)
7 Cal. Civ. Code §3426.1(d)(1)-(2) (2010)
8 6 Del. C. §2001(4)a-b (2010)
9 Tex. Penal Code §31.05(a)(4) (2010)
10 50 State Comparative Legislation/Regulations Trade Secrets (LexisNexis 2010)
11 RESTATEMENT (FIRST) OF TORTS §737 (1939)
12 369 Ark. 469, 479 (2002).

> (3) extent of measures taken by the company to guard the secrecy of the information;
> (4) value of the information to the company and to its competitors;
> (5) amount of effort or money expended . . . in developing the information; and
> (6) ease or difficulty with which the information could be properly acquired or duplicated by others[13]

Interesting in the above analysis is that while items (1) and (3) tend to align with the definition of a trade secret according to the UTSA, the Arkansas court attempted to resolve the "reasonable security efforts" under the UTSA by adding a requirement relative to the extent that the information is known by employees within the business.[14] This is a departure from the usual definitions offered by the UTSA and other courts in that it implies that dissemination of trade secrets to employees carries a direct implication that failure to control such dissemination could vitiate court protection of the trade secret. In *Tyson*, the court held that,

> Hundreds of Tyson managers were educated about the nutrient profile [of Tyson products] and there was no proof that Tyson took any steps to swear them to secrecy, or warn them of the confidential nature of the profile. Relying on an ethical guide like the Corporate Code, which fails to identify what is a trade secret or to mention the nutrient profile, is simply not enough for Tyson to invoke trade-secret protection.[15]

One could argue that the information held by Tyson met the layman's definition of a trade secret. It was known only inside Tyson and it offered a marketplace advantage to Tyson. However, meeting the layman's definition of a trade secret was not sufficient to protect Tyson. There is a statutory requirement in essentially every jurisdiction that trade secrets be controlled with reasonable security measures. In *Tyson*, the widespread dissemination of the secret nutrient profile data together with a failure to identify the material as confidential lead to a finding by the court that trade secret protection was not available.

Trade secrets do not necessarily need to be tangible. Although the UTSA notes that a trade secret includes tangible items such as formulas, patterns, compilations, programs, and devices, the definition also includes information. This is important to note because information can provide a competitive advantage by directing the holder what to do. Further, it can provide an advantage by directing the holder what *not* to do ("negative information"). An organization that has invested resources and experimentation

---

[13] *Id*.
[14] *Id*.
[15] *Id*. at 483.

will likely learn what methods or techniques will not yield desired results. This negative information can represent a competitive advantage against companies who have yet to acquire this knowledge. Still, the UTSA and the iterations thereof as adopted by the states make no exceptions for negative information. Negative information must still be subject to the application of adequate security methods in order for it to be protected as a trade secret.

It is important to note that not all secrets held by an organization are actually trade secrets. Information that is independently developed by competitors within a given industry is not classified as a trade secret due to the fact that in the end, it simply is not a secret. Notwithstanding this however, it is possible for a trade secret to be shared between organizations, providing it is held in secret.

EFFECTS OF GOOD VERSUS POOR TRADE SECRET SECURITY

Both state law and the UTSA require at least some security to protect trade secrets and that security must be "*reasonable* to maintain its secrecy."[16] At the core of this thesis (as well as the related common and statutory law) is the question of what constitutes reasonable. Starting with what is not reasonable are examples where a trade secret was not given protection by the courts because the owner took little or no steps to guard its security.

Of particular note is *Omega Optical v Chroma Technology*.[17] In that case, Omega developed and produced thin-film optical filters and, a group of Omega employees who were intimately involved in the production of these filters left to form Chroma Technology.[18] These former employees acquired substantial knowledge regarding the production of these filters as part of their employment with Omega, a fact that was not contested by either party.[19] Omega argued, and the Vermont Supreme Court in quoting the trial court agreed that, "'The body of knowledge necessary to produce the thin-film optical interference filters was sufficiently valuable, and not generally well-known, that it [was] protectable as a

[16] Unif. Trade Secrets Act, §1(4)(ii) (1985)
[17] 174 Vt. 10 (2002)
[18] *Id*. at 12.
[19] *Id*.

trade secret.'"[20]

Fatal to Omega's case was not an absence of protectable trade secret information or, the misappropriation of such information by departing employees.[21] Specifically fatal to Omega's case was that court found Omega took no steps to protect its trade secret information.[22] Examples of this near total failure to ensure any type of security included findings of permitted public access to Omega work areas, an intentional failure to mark documents as "Confidential," and even the intentional lack of locks on the doors of Omega's facilities.[23] The court noted that this lack of external security was exacerbated by a lack of internal security, including no written policies regarding confidentiality, a lack of awareness by Omega employees as to what the company considered confidential, and non-existent record keeping.[24] Because Omega took essentially no steps to protect its confidential information, the court held that the departing employees did not receive any information in confidence and therefore, owed no duty of confidentiality to Omega.[25] The result of this is an excellent example that the mere existence of trade secret information is not sufficient for it to be protectable under the law. This is also in direct concurrence with the USTA definition of a trade secret which includes the requirement that appropriate and reasonable steps be taken to protect trade secret information.[26]

Many businesses find their roots in an employee who has gained sufficient knowledge of a craft as part of her employment, and then resigns in order to start her own company. *Omega* is a very a typical example of this. However, the case law is replete with claims that these former employees utilized more than just the general knowledge acquired during their employment in order to star their new businesses. Often, a claim is made that trade secrets learned from a former employer are wrongfully used as a basis to

---

[20] *Id*. at 14 – 15.
[21] Although employees are generally free to utilize knowledge gained during the course of their employment to start their own competing businesses or obtain additional employment in the field, sanctions are available under multiple theories such as Tort, Agency and Unfair Competition when this information is obtained through improper means such as theft or deception. Sanctions can even extend to criminal penalties.
[22] *Id*. at 15.
[23] *Id*. at 15 – 16.
[24] *Id*.
[25] *Id*.
[26] Unif. Trade Secrets Act, §1(4)(ii) (1985)

start these new businesses. While starting a business using general knowledge gained as an employee is acceptable, using a former employer's trade secrets as technological seed capital can be an unacceptable expropriation of trade secrets.

A typical example of this, and one that also illustrates once again the effects of failing to take even rudimentary security steps to protect trade secrets is that of *Zemco v. Navistar*.[27] Zemco manufactured parts for the automotive industry and as part of that process, had developed specialized machinery to reduce manufacturing times and lower its costs.[28] Following the dissolution of the original Zemco partnership, one of its former partners established a new organization to compete with Zemco and in order to do so, utilized the same specialized machinery as designed and built in house by Zemco.[29] Zemco ultimately filed suit, claiming misappropriation of Zemco's proprietary information.[30]

As a threshold analysis, the court focused on the two main prongs required for a trade secret as defined in the UTSA.[31] Although the court found for Zemco on the first prong (i.e., independent economic value), Zemco ultimately lost on summary judgment based on the second prong (i.e., efforts to protect secrecy).[32] The *Zemco* court held that, "Although Zemco took some measures within its own company and with its employees to protect . . . information . . . it did very little, if anything at all, to protect the information from outside sources. Under these circumstances . . . the information did not constitute a trade secret protected by the Trade Secrets Act."[33] The court noted that Zemco had no confidentiality agreements with employees or customers who toured the facility, that such customers were not informed that the machines viewed as part of these tours was secret, they were not asked to avoid disclosure of what they had seen, and that a mere reliance on a supposed custom within the industry that vendors and customers protect confidential information was wholly inadequate.[34] It is interesting that

---

[27] 759 N.E.2d 239 (Ind. Ct. App. 2001).
[28] *Id*. at 242.
[29] *Id*.
[30] *Id*. at 244 – 46.
[31] *Id*. at 245.
[32] *Id*. at 249 – 50.
[33] *Id*.
[34] *Id*.

Zemco purportedly relied on industry custom to maintain confidentiality without seeming to understand that its visitors could not maintain confidentiality of information that Zemco failed to point out as such. As a result of this, although the *Zemco* court found that a trade secret existed, it refused to afford it protection because of Zemco's failure to maintain reasonable security precautions.[35]

EFFECTS OF LOSS OF SECRECY

A particularly noteworthy example of the effects of the loss of secrecy is that of *J.T. Healy & Sons v. James A. Murphy & Son, Inc*.[36] In *Healy*, trade secret protection was denied based on the company's approach to managing trade secrets, which was to hide them in plain sight in the belief that employees would then be unaware of their existence. Nevertheless, while the results in *Healy* were likely due to a small family owned business that did not know better, a similar outcome befell the litigants in *Conagra v. Tyson,*[37] two of the largest food producers in the world, who presumably, were much more business savvy than the litigants in *Healy*. Tyson was the world's number one producer of poultry products with sales of $7.4 billion in 1998 and ConAgra, though number five in the poultry industry with 1998 sales of $1.2 billion, had total food sales of $24.2 billion.[38] Among their other operations, both were actively involved in the sale of their products to large, multi-national food corporations such as Burger King, KFC, and Subway. ConAgra and Tyson were experienced businesses and nothing related to trade secrets should have come as a surprise to them.

As has happened in many trade secret cases, Tyson accused ConAgra of raiding (intentionally hiring away) three of Tyson's top management executives, each of whom had access to confidential, trade secret information, including pricing, cost of goods sold, profit margins, and marketing strategies.[39] Tyson claimed that its pricing information was a trade secret and that the departed Tyson executives

---

[35] *Id*. *See Flotec, Inc. v. Southern Research,* 16 F. Supp. 2d 992 (S.D. Ind. 1998). (Flotec took essentially no steps to mark its engineering drawings as confidential or proprietary or to stamp or mark any other similar legend on its technical drawings and as such, trade secret protection was denied by the court.)
[36] 260 N.E.2d 723 (Mass. 1970)
[37] 342 Ark. 672 (2002).
[38] *Id*.
[39] *Id*.

would necessarily disclose this information as part of their new employment with ConAgra.[40] The court found that although this pricing information was confidential, it was noteworthy that none of the Tyson sales contracts contained a provision preventing customers from disclosing their pricing to others and therefore, the information was not a trade secret.[41] The court dismissed Tyson's claim that its customers would be unlikely to disclose their pricing as to do so would be to the benefit of the disclosing customer's competitors.[42] The court held that Tyson failed to protect its confidential information and stated,

> The fact remains that Tyson neglected to include any restriction in its customer contracts that prevented disclosure to third parties. Regardless of whether proof was presented that such disclosure by Tyson customers had transpired, Tyson manifestly failed to take steps to guard the secrecy of this information. Moreover, without a curb or some restriction on its customers, the information was readily ascertainable by third parties from some, if not all, of Tyson's customers. This lapse is important to this court. If Tyson did not consider it necessary to preclude the dissemination of pricing information by its customers, why should this court on *de novo* review enforce the secrecy of that same information?[43]

The court concluded that if the information was not sufficiently critical to Tyson for it to take the simple step of including a confidentiality clause in its most important contracts, the court was unwilling to afford that information trade secret protection. Worse for Tyson was that the organization did not establish separate confidential disclosure agreements [hereinafter, "CDA" or "CDA's"] with these executives, relying instead on its Corporate Code of Conduct and Compliance Policy and verbal understandings. This lead the court to comment that, "In short, Tyson had in place no protection against postemployment revelation of confidential information by these executives."[44]

One can easily speculate as to what the cost of this loss of trade secret protection was to Tyson. Tyson's poultry sales in the year in question totaled $7.4 billion. Even a one-cent change in the price of Tyson's products translates to a $7 million loss. More importantly, the foregoing assumes that Tyson's market share remained unchanged. It is impossible to estimate the potential loss in market share that resulted to Tyson from the failure to simply include CDA's in its sales contracts. One is left to wonder

---

[40] *Id*. at 678.
[41] *Id*.
[42] *Id*.
[43] *Id*. at 678 – 79.
[44] *Id*.

how an organization the size of Tyson could use logic analogous to a small operation such as Healy.

EFFECTS OF EXCESSIVE SECURITY MEASURES FOR TRADE SECRETS

While adequate security is a fundamental prerequisite to legally protect a trade secret, a balancing act that is required. A tension exists between maintaining minimally adequate protection versus maintaining protection that is excessive. Excessive security utilizes funds that could be put to otherwise more productive uses. Further, the incremental cost associated with maintaining excessive intellectual property [hereinafter, "IP"] security programs does not necessarily yield additional judicial protection.

An instructive example of potentially excessive security is *USM Corp. v. Marson Fastener Corp.*[45] In that case, Marson received a declaratory judgment against claims that it had misappropriated trade secrets related to USM's technology for the manufacture of blind rivets.[46] Former officers of USM left the organization to start their own competing business and, unsatisfied with the initial performance of their production machinery, Marson hired an engineer from USM to build new equipment.[47] In hearing the initial case, the master determined that the former USM engineer brought with him, "[A] group of about 100 [blue]prints without identifying title blocks but which [the former USM officers] recognized as . . . [parts] drawings of the USM Machine."[48] As a result of this, Marson succeeded in constructing a blind rivet assembly machine that was, "substantially the same as the USM Machines."[49]

Nevertheless, the master concluded that USM was not entitled to trade secret protection for its production technology because USM had taken inadequate precautions to preserve its secrecy.[50] To reach this strikingly unsupportable result, the master focused on the security measures taken at the USM manufacturing plants where the machine were developed and operated.[51] During the development period of the machine, the USM facility was fenced, and employees and visitors entered through guarded gates.[52]

---

[45] 379 Mass. 90 (1979).
[46] *Id.* at 91.
[47] *Id.* at 93.
[48] *Id.*
[49] *Id.*
[50] *Id.* at 94.
[51] *Id.*
[52] *Id.*

Once inside, employees were expected to remain in their immediate work areas and supervisors questioned any employee who was outside his work area.[53] Visitors to the plant were logged in and out, they were required to state their business and were at no time permitted to walk unescorted in the plant.[54]

During development, the USM machines were located in an isolated area of the plant and, USM treated the machines as items intended solely for use in production of items to be sold to others and not themselves to be sold.[55] All drawings and blueprints were kept in the engineering department and whenever a drawing was required for use outside this department, the employee needing the print was required to complete a written request.[56] Issued prints were also stamped with the work order number and the phrase, "for the above only," before being released from the engineering department.[57] In addition, all employees signed a CDA that read in part:

> I will carefully guard and keep secret all confidential information which does or may concern the business and affairs of [USM], and at no time while in the employ of said Corporation or thereafter shall disclose any such information without first securing the written consent of said Corporation. I also agree that all documents or other data relating to the business of said Corporation which shall come into my possession shall be surrendered upon request whether before or after my employment shall have ceased.[58]

Despite these extensive security measures, the master who first heard this case held that USM had not exercised adequate diligence in protecting its trade secrets.[59] The master concluded that these security precautions did not entitle USM to claim trade secret protection for its production machine, measured against a standard of conduct that required USM to, "exercise a degree of eternal vigilance or pursue an active course of conduct sufficient to maintain the secrecy of the information embodied in the USM Machine."[60] This rather draconian conclusion was based on the master's sole finding that not all USM prints were stamped "Confidential."

On appeal, the Massachusetts Supreme Judicial Court reversed, stating that, "where a plaintiff has

---

[53] *Id*.
[54] *Id*.
[55] *Id*.
[56] *Id*.
[57] *Id*. at 95.
[58] *Id*. at 96.
[59] *Id*.
[60] *Id*.

actively sought to protect its trade secret, the question then becomes whether the protective measures are reasonable.".[61] 'Reasonable precautions against predatory eyes we may require, but an impenetrable fortress is an unreasonable requirement, and we are not disposed to burden industrial inventors with such a duty in order to protect the fruits of their efforts.'"[62] The court was persuaded by what were quite extensive security measures and found for USM. Nevertheless, although USM prevailed, the extensive security USM employed came with an opportunity cost. Funds that USM expended towards security could have been potentially directed toward further research and development or corporate growth.

Also warranting discussion are the cases of *DuPont v. Christopher*[63] and *Dow Chemical v. US*.[64] These cases are illustrative in that they demonstrate the extreme lengths to which a trade secret holder will go in order to protect that secret. The protective methods employed in these cases may be viewed as the upper limit of what courts expect to see in order to find adequate security. These cases also demonstrate the extreme measures others will use to discover trade secrets.

In *DuPont*, the company had developed a secret process for manufacturing methanol that gave it a competitive price advantage and was constructing a facility to employ this new procedure.[65] Competitors were eager to learn this process and unknown parties hired the respondents who flew over the uncompleted facility, taking photographs. These photographs were delivered to the unknown parties, presumably, DuPont's competitors.[66] DuPont filed suit to compel the respondents to reveal the name of the parties that hired them and the respondents answered by claiming that:

> They committed no "actionable wrong" in photographing the DuPont facility and passing these photographs on to their client because they conducted all of their activities in public airspace, violated no government aviation standard, did not breach any confidential relation, and did not engage in any fraudulent or illegal conduct. [F]or an appropriation of trade secrets to be wrongful there must be a trespass, other illegal conduct, or breach of a confidential relationship.[67]

---

[61] *Id*. at 97.
[62] *Id*. (*USM* quoting *E.I. duPont deNemours & Co*. v. *Christopher*, 431 F.2d 1012, 1017 (5th Cir. 1970)).
[63] 431 F.2d 1012 (5th Cir. 1970).
[64] 476 U.S. 227 (1986).
[65] *DuPont* at 1013.
[66] *Id*.
[67] *Id*. at 1014.

The court rejected this theory, concluding that a competitor is entitled to use the trade secret of another only if the competitor obtains this information through his own research efforts, rather than by stealing it.[68] The court concluded that DuPont took reasonable security precautions, including the use of fences and roofs, but that to require constructing a roof on an uncompleted building simply to avoid the "the unanticipated, the undetectable, or the unpreventable methods of espionage" was unreasonable.[69]

The conclusion that ordinary protective measures such as fences, roofs, and the like were reasonable to protect a trade secret in *DuPont* is contrasted to the different conclusion reached on a very similar fact pattern in *Dow*. In *Dow*, the facility consisted of over 2,000 acres of manufacturing buildings to which Dow strictly controlled access.[70] Nevertheless, based on Dow's refusal to admit the Environmental Protection Agency [hereinafter, "EPA"] for inspectional purposes, the EPA conducted low level aerial photography flights, much like those in *DuPont*.[71] The Supreme Court held that the EPA did not use unreasonable efforts to obtain a trade secret. This ruling can be squared with the result in *DuPont* by noting that the EPA's sole intent in taking these images was to perform its regulatory functions, not for the purpose of obtaining a competitive advantage.[72]

DuPont and *Dow* can help define the upper limits of what courts expect when attempting to determine if adequate security is afforded to trade secrets. For example, *Dow* (as quoted in the appellate level decision) took the following steps to safeguard its IP:

1. A chain-link fence . . . completely around the production facility;
2. gates . . . at various intervals in the fence have an attendant (guard) on duty . . . ;
3. closed-circuit television surveillance for continuously monitoring the various entrance and exit gates and . . . the fence surrounding the facility;
4. alarm systems which will indicate unauthorized entry at various locations;
5. motion detectors at strategic locations . . . within the facility;
6. roving patrols which travel throughout the facility and guard the perimeter . . .;
7. liaison with local public law enforcement officials including radio communication to assist in the apprehension of persons engaged in unlawful activities . . .;
8. employees . . . must exhibit an identification badge in every instance of entry;
9. non-employees who wish to visit the facility must be approved and must obtain a

[68] *Id*.
[69] *Id*. at 1016.
[70] *Dow* at 231 – 32.
[71] *Id*. at 232.
[72] *Id*.

visitors pass . . . which must be exhibited at all times while in the facility;
10. a requirement that non-employees . . . be greatly restricted in their movements and that some areas of the facility remain off-limits to all non-employees;
11. a requirement that cameras by anyone other than an authorized representative of Dow are prohibited at all times and in all places in the facility;
12. persons visiting . . . must obtain a technical pass [requiring] . . . that the visitor will not disclose any technical information learned as an incidence to his visit;
13. security personnel are on duty twenty-four hours a day and seven days a week with at least twenty-five such people on duty at all times and with about fifty people on duty during normal duty hours;
14. a security budget whereby Dow spent at least 3.25 million dollars in each of the last ten years on the security of the Midland production facility; and
15. in the event engineering drawings and/or blueprints . . . were to be disposed of . . . [they] would be packaged and incinerated under the direction of security personnel who would also witness the incineration.[73]

In addition, all Dow employees and contractors signed secrecy agreements, and its plant layout was designed to keep proprietary areas out of view to persons on the right-of-way outside the fence.

The circuit court found that these security measures represented a comprehensive program to maintain physical control of the corporate premises while at the same time, securing legal control over those with which Dow maintained business relationships. Therefore, these security measures represent the upper limit of what courts expect when considering whether adequate means were employed.

Before departing from a discussion of the extensive security measures taken by *USM*, *DuPont* and *Dow*, it is important to note that the security measures in these cases came with a cost. Wrapping a fence around an entire facility as USM did costs thousands, if not hundreds of thousands of dollars. Likewise, security guards at all entrances as in *Dow* comes with a heavy ongoing cost and an easy calculation with more specificity can be made by referring to standard labor costs from sources such as the Bureau of Labor Statistics. Similarly, while the acts associated with controlling a document can be calculated in a time and labor manner, the cost of access-controlling and signing out each document as USM did becomes quite large when one considers that USM had over 250,000 such documents. As a result, the requirement of reasonable security for trade secret protection takes on a dimension beyond that which might be required for protection by the courts. Again, security measures that go beyond reasonable come with a calculable cost of funds that could otherwise be applied to growing the business further.

[73] *Dow Chemical Co. v. U. S.*, 536 F. Supp. 1355, 1364 – 65 (E.D. Mich. 1982).

A full quantitation of the costs to organizations such as Dow, DuPont, or USM would require an in-depth organizational analysis and would itself be a treatise. Nevertheless, a rough gauge can be made to get a general sense of the opportunity costs associated with the security measures each company employed. For example, in *Dow*, the court noted that twenty-five security personnel were on duty around the clock. In order to have twenty-five personnel present at all times (assuming an eight hour/day/person work shift), Dow would have had to hire at least seventy-five such security persons. Using Bureau of Labor Statistics historical data, the median annual earnings for a full time, wage and salary worker in 1982 (the year the case was decided), was approximately $16,000.[74] Given this pay rate, these seventy-five personnel cost Dow approximately $1,200,000 annually. The important point is that these personnel were but a fraction of the costs Dow expended in security. As the *Dow* court noted, Dow spent at least $3.25 million annually on security for its Michigan production facility, money which was not otherwise available to be directed back into the business to fuel further growth.

MEANS TO SAFEGUARD TRADE SECRETS; WHAT DO COURTS LOOK FOR?

This paper is ultimately about the tension between all or nothing. All, as in cases such as *USM,* are heroic measures aimed at protecting confidential information and trade secrets. Conversely, nothing is a total or near total lack of efforts to provide such protection, as is seen in cases such as *Healy*.

Based on the cases cited herein, the UTSA and the relevant statutes, nearly all courts will look for at least some effort expended toward protecting what a company considers to be confidential information. These efforts can be broken down into documentation controls and physical controls.

The simplest documentation control begins with a CDA, which defines the information to be disclosed between the parties and the steps they must take to safeguard this information. Given that there are literally hundreds of variations of these forms available from multiple sources, the failure to establish a CDA prior to disclosing any type of confidential information borders on unpardonable.

---

[74] Bureau of Labor Statistics, Databases, Tables & Calculators by Subject, Weekly and hourly earnings data from the Current Population Survey, Constant (1982-84) Dollar Adjusted to CPI-U- Median Usual Weekly Earnings, Employed Full Time, Wage and Salary Workers, http://data.bls.gov/PDQ/servlet/SurveyOutputServlet (last visited Nov. 17, 2010).

In general, all CDAs contain five elements; (1) a definition of the material considered to be confidential, (2) a definition of what material is excluded from the CDA, for example confidential information that was available to the receiving party before the CDA was executed, (3) what the obligations of each party are in regard to handling, protecting, and further disclosing the confidential information, (4) the remedies available to a party if the other party breaches or threatens to breach the CDA and (5) the term of the CDA. From the case law, it is clear that a party seeking trade secret protection will face a higher burden to prove that its information was confidential if it failed to take the very simple step of establishing a CDA. While the absence of a CDA does not necessarily obviate the existence of a trade secret, the presence of a CDA is prima facie evidence that the party seeking trade secret protection from the courts took at least minimal steps to protect its trade secret.[75]

On a more practical level, courts frequently look for what are relatively simplistic means of putting employees and other persons on notice that given access documents, drawings, or systems, that are confidential in nature. Mechanisms such as stamping documents "Confidential" or maintaining a system of controlled access to plant areas where trade secret operations take place can be used to demonstrate that reasonable security measures have been taken. Organizations should use caution in trying to define each and every type of trade secret with particularity as such an approach could fail if something is overlooked in the process.[76] A more logical and efficient approach to identifying trade secrets and keeping employees abreast of them is to appoint key leaders within each department to routinely evaluate and manage the trade secret information being used.[77] Regular IP review meetings with employees will reinforce what is and is not considered confidential and, will demonstrate to a court

---

[75] *See Elmer Miller, Inc. v. Landis,* 253 Ill. App. 3d 129, 134 (1993). (Plaintiff owner of a small tailor shop and sought injunction against former employees for using his customer lists. Customer information was kept in a closed file drawer, only specific salesmen had access to customer information, and employees were informed upon hiring and upon employment termination that customer files were confidential. The court held that given the very small size of the business, these were reasonable efforts to protect secrecy of these customer lists.) *See also* Roger M. Milgrim, *Milgrim on Trade Secrets* § 1.04, at 1-173 (2002). ("A trade secret does not lose its character by being confidentially disclosed to agents or servants, without whose assistance it could not be made of any value.") *And see Learning Curve Toys, Inc. v. PlayWood Toys, Inc.,* 342 F.3d 714 (7th Cir. 2003). (Disclosure of a secret toy manufacturing process by a small manufacturing shop under only an oral promise of confidentiality was considered reasonable protection of its trade secret given the small size of the business.).

[76] Milgrim on Trade Secrets, Ch. 18, Anatomy of a Trade Secret Protection Program, §18.03[4] (Matthew Bender)

[77] *Id.*

that the organization took steps to control trade secret security. A failure to take the simple precaution of establishing CDA's with employees, vendors, and customers or, establishing simple physical access controls will be viewed by the courts as failure to take adequate control over trade secret security.

MANAGING COMPUTER, NETWORK, AND OTHER ELECTRONIC SECURITY

Intellectual property and security of computers and related systems are increasingly common issues in the control of trade secrets. Parties within organizations as well as those outside, including customers, vendors, and competitors can be threats to IP security. For example, an employee seeking revenge for a perceived wrongful termination or, desiring to expropriate information from an employer in order to start his own business represent a major weak point in an employer's trade secret database. High capacity, inexpensive USB stick drives make it exceptionally easy for an employee to download and steal highly valuable trade secret data and other IP from an employer's networked computers.

RKI, Inc. v. Grimes is highly instructive of the ease with which company trade secrets can be accessed via computer networks (and numerous other computer-related security issues).[78] In *RKI*, the court noted the case was, "about how an employee who signed a non-disclosure and non-compete agreement chose to join a competitor [and was] a textbook case of how not to do it."[79] In *RKI*, a former employee (Grimes) executed the following CDA with RKI as part of his hiring process:

> Employee agrees as follows:
> (a) That during the term of this Agreement and at any time after Employee leaves the Company, Employee shall not, without prior written consent of the Company . . . directly or indirectly, communicate, disclose, transmit, disseminate or otherwise publish or reveal in any form whatsoever to third parties, the Proprietary Information . . . imparted to Employee by the Company . . . "Proprietary Information" shall mean any and all information, including, but not limited to, information concerning the design and development of tooling used in the Company's business, not generally known or recognized as standard practices, and information which is disclosed to, developed by, or known by Employee concerning any and all of the technology, research, test procedures and results, inventions, concepts, documentation, and computer programming, formulae, manufacturing processes and products, produced or developed by the Company, its successors or assigns.[80]

As part of RKI's efforts to expand its business, RKI spent millions of dollars and substantial time

[78] 177 F. Supp. 2d 859 (N.D. Ill. 2001).
[79] *Id*. at 862.
[80] *Id*. at 864.

developing a new customer database and, in his capacity as a salesman for RKI, Grimes had direct access to this database as well as the ACT® database which RKI had used previously.[81] The court applied the typical two-prong test to determine if these databases constituted trade secrets of RKI. The court found that RKI had taken reasonable steps to safeguard the security of these databases and, that the data was of such an extensive nature that it offered RKI a competitive advantage.[82]

Following approximately two-and-one-half years of employment with RKI, Grimes resigned to join RKI's direct competitor, Chicago Roll.[83] As Grimes worked toward transitioning to Chicago Roll, a decision he made based in part on poor performance reviews he received at RKI, he contacted the Regional Sales Manager at Chicago Roll, a personal friend of his, and made it clear that he (Grimes) had, "everything he need[ed] including customer contact information."[84] After joining Chicago Roll, Grimes confirmed to his new management that he had used customer contact information from RKI to steal active RKI accounts, and "that he was looking forward to stealing all of Roll-Kraft's customers and that he had a lot of customers that were coming with him."[85] Unfortunately, the criminal behavior did not end at this point, as Grimes took complete advantage of the inadequate computer systems security at RKI before he departed his employment there. Grimes was approached by RKI management who asked whether he was leaving to work for RKI's competitor. Grimes thus realized he would likely be asked to leave in the next few days and he set about copying much of RKI's trade secret database.[86] What is of particular importance is that RKI had enabled its employees to access these databases from remote computers. Grimes exploited this poor security by copying much of RKI's databases onto his home computer.[87]

RKI illustrates many aspects related to the management of computers, networks, and employees,

---

[81] *Id*. at 865.
[82] *Id*. at 865 - 66. (The court noted that, "This system was devised in order to give Roll-Kraft a competitive advantage in servicing its existing customers, in developing new business and enabling a new salesperson to step in without missing a beat. This information was accumulated over many years and at a cost of millions of dollars.")
[83] *Id*.
[84] *Id*. at 868.
[85] *Id*.
[86] *Id*.
[87] *Id*. (A computer forensics expert testified that a significant amount of data had been downloaded from RKI's databases to Grime's home computer and, that according to data date stamps, these data had been deleted during the time period of the investigation.)

in relation to IP. While RKI took all the normal precautions to safeguard its trade secrets, it still suffered substantial harm due to a disgruntled employee. It is important to note exactly what RKI both won and lost. Because the court found that RKI had, among other statutory requirements, maintained adequate security over its trade secrets, the court provided protection to those trade secrets. However, the court also noted that,

> Grimes used Roll-Kraft's confidential information to hit the ground running at Chicago Roll. He immediately solicited business for Chicago Roll from customers whom he had called on for Roll-Kraft just a few days earlier, using Roll-Kraft's confidential information to gain a competitive advantage. In just a few days, Grimes made several sales to such customers.[88]

Although RKI was able to obtain a permanent restraining order against Grimes, and win compensatory damages of $100,000 and punitive damages of $150,000,[89] the more important issue is what RKI lost. Returning to the original definition of a secret, once a secret is lost, it cannot be restored. Although RKI proved its case, the data it lost can never be restored, nor can less easily defined items such as customer loyalty and goodwill.

As this section deals with electronic security issues and, other sections deal with how to manage employees, a discussion of what an employer such as RKI could have done differently is warranted. There is nothing wrong with allowing employees to access company computer systems remotely and in fact, this is frequently necessary for sales or other field-based personnel to properly perform their jobs. However, missing from RKI's otherwise reasonable computer security systems was any type of software to manage large volumes of downloading in relatively short periods of time. Also missing was any regular review of simply which employee downloaded what data during any given period or, which employee accessed the system at what time. While RKI had a requirement that employees update and expand the customer management database, this effort was aimed at boosting sales, not at controlling access. The very thing Grimes was ultimately demoted for was failing to add sufficient new data to the database on a regular basis. However, this is quite different from a proactive approach designed to

---

[88] *Id*. at 869.
[89] *Id*. at 881.

determine which employee is adding (and more importantly removing) what data, and when.

If RKI can also be faulted for anything else, it would be for not more affirmatively managing at-risk employees. The term at-risk means an employee who has resigned (but not yet left), is on probation, or that management has other reason to believe might be at-risk of misappropriating company IP. As the case law and practical experience have shown, departing, disgruntled, and even happy employees often download trade secret data from employer databases for the employee's own benefit. RKI was well aware that Grimes was at least potentially talking to its major competitor and therefore, RKI should have considered him an at-risk employee. Yet despite this knowledge, RKI took no steps to immediately shut down his access to their trade secret database or otherwise affirmatively manage his at-risk status. Given the value of this database to RKI and, that RKI knew Grimes was an at-risk employee, one could posit an entirely different outcome for RKI. Another court might have found that RKI's inaction amounted to a failure to take adequate precautions to safeguard its trade secrets and as a result, deny protection to RKI's trade secrets.

CREATING A CULTURE OF IP PROTECTION

The unique aspect of not just a trade secret but also any secret at all is, that by practical definition, the secret remains a secret if only one person knows it. On a practical basis however, in order to exploit a trade secret, its owner must disclose it to employees and thus, one of the greatest weaknesses in the development of IP protection programs is the interface between employees and IP. Complicating this general problem are two additional issues. First, in many cases, employees may simply either not know what qualifies as IP or, may be unaware how to properly control and secure it. Second, as with anything valuable, a trade secret is subject to theft, in this case by employees who very much understand the value of the trade secret. For these reasons, it is important for a company to create a culture that reinforces the importance of protecting IP. In addition to the obvious value of controlling valuable information and decreasing the likelihood of loss or diversion, courts frequently view a comprehensive program of IP protection as evidence that an organization has met the adequate security prong for protection of trade secrets. Cases such as *USM*, *Dow,* and *DuPont* are excellent examples of this principle.

The responsibility for implementing an adequate IP management program, especially in larger organizations where such control inevitably becomes more difficult, ultimately rests not with the legal department but with corporate leadership. While the relationship between even an ordinary rank and file employee and an employer is often (though certainly not always) by nature a confidential one,[90] a special level of fiduciary duty exists between a corporation and its officers. Some jurisdictions have found that corporate officers owe a special duty of loyalty to their employers as a result of their status as officers.[91] This special duty of loyalty to the employer coupled with the sound business logic of protecting a corporation's assets dictates that senior executives have a legal duty and business responsibility to establish cultures, and systems within those cultures to protect IP.

A corporate culture aimed at the respect and management of IP starts with new employees since new employees often bring with them restrictions relating to IP from their former employers. New employees should be taken through a standardized process to determine if they are subject to any prior agreements of confidentiality, non-competition, or other restrictive covenants that could be a bar to their new employment.[92] Similarly, the vetting process for new employees should include developing an understanding of their role at their prior employer. Even in the absence of express agreements, the hiring of a former corporate officer can bring special duties of non-disclosure that do not necessarily exist for lower level personnel. Once new employees are vetted, companies seeking to protect their trade secrets should use restrictive covenants executed by the new employee to advise the employee of the need to respect and protect the company's trade secrets.[93]

As employees are brought into the company, the organization once again needs to find a balance

---

[90] *Christopher M's Hand Poured Fudge v. Hennon,* 699 A.2d 1272, 1276 (Pa. Super. Ct. 1997). *See also Air Products & Chemicals, Inc. v. Johnson,* 442 A.2d 1114, 1120 (Pa. Super. Ct. 1982). (Despite the absence of a restrictive covenant incident to employment, a former employee was enjoined from disclosing trade secrets learned during the course of his employment due to the confidential nature of the employer/employee relationship.) *But see Dalton v. Camp,* 353 N.C. 647 (2001). (An at-will employee with which no special relationship of trust has been established does not meet the criteria of a fiduciary relationship and therefore, the relationship was construed to not be of a confidential nature.)

[91] *Maryland Metals, Inc. v. Metzner,* 282 Md. 31, 36 (1978).

[92] Milgrim on Trade Secrets, Ch. 18, Anatomy of a Trade Secret Protection Program, §18.02 [4] 1 (Matthew Bender)

[93] Milgrim on Trade Secrets, Ch. 18, Anatomy of a Trade Secret Protection Program, §18.02 [2] 3 [a] (Matthew Bender)

regarding trade secret protective measures. A total lack of security with an open door policy such as in *Omega* will not satisfy most courts. However, an overly repressive IP management program will frustrate employees, stifle creativity, and is expensive, with *Dow* or *DuPont* being excellent examples of this.

As mentioned, in order for a trade secret to be useful, it usually must be disseminated to employees. However, dissemination of this information creates a risk in relation to the termination of employment. As shown in *RKI*, departing employees frequently have little if any loyalty remaining to their soon-to-be former employers and the incentives and opportunities to misappropriate trade secret data are often great with these employees. The case law is replete with examples of departing employees stealing or otherwise misappropriating trade secrets of their former employers, in many cases, for the purposes of these employees setting up their own competing businesses, as shown in *Omega*. Companies are well advised to understand which employees are at-risk of misappropriating trade secrets. This includes employees who have received poor performance reviews, those who might be interviewing at competitors, and even previously loyal employees who have given their notice to depart. In the case of these employees, while it may seem draconian, an employer should have procedures and systems in place to immediately remove (or at least control) computer and network access as well as physical access to trade secret areas and information. As mentioned in *RKI*, one could easily argue that RKI failed to fundamentally control a highly at-risk employee and as a result, other courts might have been much less sympathetic to RKI's loss. A program to manage departing employees is as important as a program aimed at the hiring of new employees.

OVERALL SUMMARY

Trade secrets represent an extremely valuable source of competitive IP for many organizations. Since the law recognizes trade secrets as property, like any other piece of property, trade secrets come with a bundle of rights. These include the right to buy, sell or trade the secret, the right to demand its return following misappropriation, the right to injunctive relief to stop threatened or actual misappropriation and in general, a right of dominion and control as the law provides for any piece of property. However, in order for these rights to be enforced by the courts, the owner must take reasonable

steps to secure this property.

While it is relatively easy to define what a trade secret is, the difficulty is in defining what constitutes the metes and bounds for the reasonable security that must be provided for a trade secret by its owner. Of course, the challenge in quantifying the word *reasonable* would be much easier if the relevant statutes (i.e., the USTA or comparable statutes adopted by each state) gave some definition or guidance as to what is considered reasonable. However, as with most uses of the adjective reasonable, the interpretation of the limits of this word are left to the judgment of the reader in the context in which the word is used. For example, could a person leave her new car unlocked with the windows down and have been found to have taken reasonable precautions to prevent its theft during the night? If the car were located in a large city such as Los Angeles, most likely the answer would be, No. Most persons living in any large, US metropolitan city would not reasonably expect to find their car the following morning if it was left unlocked with the windows rolled down. However, if that same car were located on a rural ranch in Wyoming, the answer might very reasonably change to, Yes. Thus, the analysis of reasonableness (or adequacy) for security measures to protect trade secrets is necessarily a contextual one and there is no easy answer.

In general, regardless of the trade secret involved, courts are unimpressed when even minimal security protections are not taken, especially given the ease with which these measures can be achieved. An owner of a trade secret would do well to implement controls such as the stamping of documentation as confidential, establishing physical controls over trade secret data and tangible items, as well as establishing CDA's with those who have contact with trade secrets. The foregoing is considered the absolute minimum a trade secret owner must have in place to be able to successfully argue for relief from the courts for misappropriation of its trade secrets. Stated differently, courts find that a failure to take the minimal efforts required to establish confidentiality agreements, stamp documents, lock outside doors, and control computer network access tends to indicate that adequate security measures have not been taken to protect trade secrets, and the courts will deny relief.

At the other extreme, excessive security measures, the previous automobile metaphor is again an

apt reference point. Should it be necessary for a finding of reasonableness or adequacy of security to need to lock ones' car in a specially designed concrete bunker which includes around-the-clock monitoring via security cameras and motion sensors, with armed patrols and guard dogs? Clearly, the only scenario in which this type of security might possibly be deemed reasonable is if the locale is, for example, Los Angeles during the 1992 civil riots. Were the locale the aforementioned ranch in rural Wyoming, while the car would nevertheless be secure, the conclusion would be that the security measures were excessive. An important business corollary to this metaphor is that while the car is secure in the Wyoming locale, the funds devoted to this excessive security could have otherwise been devoted to other more beneficial uses, such as purchasing a larger car or, a car with additional options.

Courts look to increasing levels of security as the value and scope of the trade secret to be protected increase, however, based on the case law and sources reviewed in this paper, a point is reached where the security is adequate and additional security measures represent funds which could have otherwise been put back into growing the business. The best example of the upper limits of adequate trade secret security are embodied in *USM*, *Dow*, and *DuPont*. In general, all three organizations had the basics of trade secret security protection in place, however, they had also taken these protections to an extreme. While physical access control is an important part of any trade secret protection program, it is likely excessive to fence in an entire production site as was done in the foregoing cases. Similarly, while access control by way of secure ingress and egress is important, to go to the extent of having constant roving patrols is likely excessive; these are production facilities, not prisons. Thus, the best way to define the upper limits of security that should be applied to the protection of trade secrets is to simply use the baseline described previously, and, in a measured and planned fashion, expand that baseline as the scope of the trade secret expands. An example of this would be a company that utilizes a trade secret internally to produce a commercial product. As discussed before, the company would be wise to have all employees execute CDA's and, as the company and number of trade secrets grows, establish written company policies and training manuals that define the scope of trade secrets for employees. However, the upper limit of trade secret security comes when an organization has comprehensive programs to, (1)

identify trade secrets, (2) inform and legally bind those who handle trade secrets and, (3) control access to those trade secrets by common methods such as locked doors and computer network access management. Security measures beyond that tend to be excessive and the courts typically do not require elaborate measures in order to find that reasonable security was afforded to the trade secret. Note however, that as technology changes, organizations that utilize trade secrets would be wise to ensure that their procedures for managing trade secrets keep abreast of such changes in technology. Again, adequacy for trade secret security is a contextual analysis and therefore, security programs need to keep abreast of the times.