University of Florida Levin College of Law
UF Law Scholarship Repository

Faculty Publications | Faculty Scholarship

1-1-2009

Contributory Negligence, Technology, and Trade Secrets

Elizabeth A. Rowe
University of Florida Levin College of Law, rowe@law.ufl.edu

Follow this and additional works at: http://scholarship.law.ufl.edu/facultypub

 Part of the Commercial Law Commons, and the Intellectual Property Commons

Recommended Citation
Elizabeth A. Rowe, *Contributory Negligence, Technology, and Trade Secrets*, 17 Geo. Mason L. Rev. 1 (2009), *available at* http://scholarship.law.ufl.edu/facultypub/89

This Article is brought to you for free and open access by the Faculty Scholarship at UF Law Scholarship Repository. It has been accepted for inclusion in Faculty Publications by an authorized administrator of UF Law Scholarship Repository. For more information, please contact outler@law.ufl.edu.

CONTRIBUTORY NEGLIGENCE, TECHNOLOGY, AND TRADE SECRETS

*Elizabeth A. Rowe**

INTRODUCTION

In tort law, the doctrine of contributory negligence captures conduct by the plaintiff that falls below the standard to which he should conform for his own protection.[1] Whether one has been contributorily negligent is determined by an objective standard of reasonableness under the circumstances.[2] This Article, for the first time, applies contributory negligence principles to trade secret law.[3] It draws upon this doctrine to frame and analyze a challenge posed by modern technology. The very technological tools in use today that increase the efficiency with which companies do business also create challenges for trade secret protection. The same tools that make trade secrets easier to store, easier to access, easier to disseminate, and more portable, also increase the risks that trade secrets will be destroyed. According to a report by the Federal Bureau of Investigation ("FBI"), the mobility of trade secrets makes them "one of the country's most vulnerable economic assets."[4] Many well-known companies such as Apple Inc., Caterpillar Inc., Charles Schwab Corp., E.I. du Pont de Nemours & Co., Estée Lauder Cosmetics Ltd., Four Seasons Hotels, Inc., and Hewlett-Packard Co. have all recently been litigants in trade secret misappropriation cases where

---

* Associate Professor of Law, University of Florida, Levin College of Law. I am grateful to Bill Page, Michael Risch, Jeff Childers, and Lea Johnston for their comments or conversations about earlier drafts of this work. I also thank, for their comments, participants at (1) the Feist, Facts, and Fiction Conference at George Washington University Law School, (2) a faculty workshop at Case Western University Reserve Law School sponsored by the Center for Law Technology and the Arts, and (3) the Intellectual Property Scholars Conference held at Cardozo School of Law. For research assistance, I am very grateful to Alicia Phillip, Mi Zhou, and Abbey Morrow. Finally, thank you to the University of Florida, Levin College of Law, for its research support.

1 KENNETH S. ABRAHAM, THE FORMS AND FUNCTIONS OF TORT LAW 144 (3d ed. 2007).

2 RESTATEMENT (SECOND) OF TORTS § 464(1) (1965).

3 A few scholars have briefly discussed these or similar tort concepts in relation to other areas of intellectual property. *See, e.g.*, Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1604-07 (2005) (discussing contributory negligence, comparative negligence, and assumption of risk as possible defenses to a negligent security claim against software companies); Roger D. Blair & Thomas F. Cotter, *Strict Liability and its Alternatives in Patent Law*, 17 BERKELEY TECH. L.J. 799, 821 (2002) (discussing a strict liability framework in the patent law context).

4 FED. BUREAU OF INVESTIGATION, STRATEGIC PLAN 2004-2009, at 40 (2004), http://www.fbi.gov/publications/strategicplan/strategicplanfull.pdf.

the alleged misappropriation involved the use of technological tools to transfer the trade secret information.[5]

As a general matter, trade secret law protects valuable business information and inventions more easily and inexpensively than patent protection.[6] Modern trade secret law simply requires that the information be of value and that it be kept secret.[7] Secrecy is thus the *sine qua non* of trade secret protection,[8] but it can be difficult to accomplish. Because the final determination of whether information is entitled to trade secret protection is not made until the trade secret owner is in litigation, courts, in an ex post fashion, second-guess whether the owner did enough to keep the information secret.[9] Thus, at a fundamental level, "the extent of the property right [in a trade secret] is defined by the extent to which the owner of the secret protects his interest from disclosure to others."[10]

The doctrinal lens through which a court evaluates the sufficiency of a trade secret owner's protection measures is the "reasonable efforts" requirement.[11] The question becomes: did the putative trade secret owner take reasonable efforts to protect the trade secret? While absolute secrecy is not required, the trade secret owner is expected to show that it took efforts reasonable under the circumstances to protect the secret.[12] This standard is very flexible, and intuitively necessitates a fact-intensive case-by-case determination that considers a host of factors in trying to ascertain reasonableness.[13]

---

[5] Hiawatha Bray, *Website to be Closed as Part of Deal with Apple*, BOSTON GLOBE, Dec. 21, 2007, at 4E; Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268 (S.D. Fla. 2003), *aff'd in part, rev'd in part sub nom.* Four Seasons Hotels v. Consorcio Barr S.A., 138 F. App'x 297 (11th Cir. 2005); Caterpillar Inc. v. Sturman Indus., Inc., 387 F.3d 1358 (Fed. Cir. 2004); Charles Schwab & Co. v. Karpiak, No. 06-4010, 2007 WL 136743 (E.D. Pa. Jan. 12, 2007); Metcalf v. E.I. du Pont de Nemours & Co., No. 05-1035 (MJD/SRN), 2006 WL 1877069 (D. Minn. July 6, 2006); Estee Lauder Cos. v. Batra, 430 F. Supp. 2d 158 (S.D.N.Y. 2006); Hewlett-Packard Co. v. Byd:Sign, Inc., No. 6:05-CV-456, 2007 WL 275476 (E.D. Tex. Jan. 25, 2007).

[6] *See* Andrew Beckerman-Rodau, *The Choice Between Patent Protection and Trade Secret Protection: A Legal and Business Decision*, 84 J. PAT. & TRADEMARK OFF. SOC'Y 371, 400-01 (2002).

[7] UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2005); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

[8] *See, e.g.*, Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) ("Information that is public knowledge or that is generally known in an industry cannot be a trade secret."); Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974) ("The subject of a trade secret must be secret, and must not be of public knowledge or of a general knowledge in the trade or business."); MBL (USA) Corp. v. Diekman, 445 N.E.2d 418, 425 (Ill. App. Ct. 1983).

[9] *See In re* Innovative Constr. Sys., Inc., 793 F.2d 875, 883 (7th Cir. 1986) ("An indispensable element of a trade-secrets claim is that the information, for which legal protection is sought, be genuinely secret.").

[10] *Ruckelshaus*, 467 U.S. at 1002.

[11] *See infra* Part I.B.

[12] *See, e.g.*, *MBL (USA) Corp.*, 445 N.E.2d at 425-26 (reviewing plaintiff's security measures and finding that such measures were insufficient to demonstrate the existence of a protectable trade secret).

[13] *See infra* Part I.B.3.

It is, however, at the heart of every trade secret misappropriation case and often determines the outcome.[14]

This Article explores a question previously unaddressed in the literature: should the greater risks presented to trade secrets in a digital world change the way that courts evaluate reasonable efforts when a trade secret is misappropriated using some form of computer technology? Should reasonableness be pegged to a "should have known" standard such that courts impute an objective expectation (similar to a contributory negligence determination) that higher safety precautions will be utilized because of the risks that in today's digital world trade secrets are easier to access and disseminate? Because the reasonable efforts requirement necessitates consideration of what is reasonable under the circumstances, I argue that the changing circumstances that have come about as a result of new technology require a reexamination of what security measures are reasonable. As such, the changing landscape indirectly places a higher duty of care on trade secret owners since the increased risks from technology are foreseeable. At a normative level, reasonableness requires not necessarily a checklist of specific items, but a conscious, risk assessment approach that better anticipates and ultimately stems the inappropriate dissemination or disclosure of the secrets. While this seems intuitive, the courts' approach and outcomes in these kinds of cases have been inconsistent.[15] Accordingly, I propose guidelines that infuse a more meaningful objective standard into the reasonable efforts analysis.[16]

This approach is informed and supported by contributory negligence principles that consider the plaintiff's conduct relative to the reasonably prudent person.[17] Where the plaintiff is in a better position than the defendant to decide whether to risk being injured, or at least the extent of that risk, based on the precautions it selects, then it seems sensible to allocate the burden of that choice to the plaintiff.[18] It is also entirely consistent with

---

14 Enter. Leasing Co. v. Ehmke, 3 P.3d 1064, 1070 (Ariz. Ct. App. 1999) ("Indeed, the most important factor in gaining trade secret protection is demonstrating that the owner has taken such precautions as are reasonable under the circumstances to preserve the secrecy of the information." (citing Michael A. Epstein & Stuart D. Levi, *Protecting Trade Secret Information*, 43 BUS. LAW. 887, 895 (1988))).

15 *See infra* Part I.B.

16 *See infra* Part III.A.

17 *See* RTE Corp. v. Coatings, Inc., 267 N.W.2d 226, 233 (Wis. 1978) ("Where the owner of the secret disregards caution and fails to take steps to safeguard against disclosure, the courts will, at times, deny him any relief whatever, principally on the theory that he courted his own disaster." (quoting RUDOLF CALLMANN, THE LAW OF UNFAIR COMPETITION TRADEMARKS AND MONOPOLIES § 55.1 (3d ed. 1968))). The standard for trade secret misappropriation is closer to negligence than to an intentional tort. The Uniform Trade Secrets Act, for instance, defines misappropriation, in part, as "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means." UNIF. TRADE SECRETS ACT § 1(2)(i) (amended 1985), 14 U.L.A. 538 (2005).

18 ABRAHAM, *supra* note 1, at 164-65 (discussing conscious reasonable risk-taking).

trade secret doctrine as it currently exists, which requires that trade secret owners take reasonable precautions to protect their trade secrets as a prerequisite for proving that a defendant (regardless of his conduct) misappropriated the trade secret.[19] This is especially powerful where such reasonable efforts are necessary for determining whether a trade secret exists in the first instance and because modern trade secret law is derived, at least in part, from tort law principles.[20]

Part I of this Article provides some relevant background on trade secret law and the "reasonable efforts" requirement. Part II introduces the digital world and the way in which electronic technology affects how we store, access, and disseminate trade secrets. In Part III, the Article urges courts to give special consideration to the known technological risks that a trade secret owner may or may not consider, rather than continuing to focus on traditional facilities-based measures.[21] The Article proposes guidelines for judges and fact finders doing the reasonable efforts analysis that includes consideration of such factors as (1) the nature of the industry; (2) the nature of the trade secrets and how they were stored; (3) the nature of the measures taken to protect the secrets; and (4) the known risks from storage and protection choices. Accordingly, the framework proposed here should infuse greater consistency and objectivity into digital misappropriation cases,[22] which are likely to constitute the bulk of trade secret misappropriation cases within the next few years. Part IV places the challenge of protecting trade secret information in the larger context of data security and discusses the lessons that can be learned from that parallel struggle. The Article concludes that trade secret protection cannot be an afterthought. Rather, in order to be reasonable, trade secret protection requires a more conscious, risk assessment approach that better anticipates and ultimately stems the inappropriate dissemination or disclosure of the secrets.

---

19 *See infra* text accompanying notes 36-41.

20 Trade secret law in this country was first synthesized and published in the *Restatement (First) of Torts*, and it may very well be that the reasonable efforts standard derived from the tort law underpinnings of this area of law. *See* RESTATEMENT (FIRST) OF TORTS § 757 cmts. a, g (1939).

21 *See infra* Part I.B.1.

22 I use this phrase to refer to circumstances when trade secret misappropriation occurs, at least in part, using electronic or digital means.

I. THE REASONABLE EFFORTS REQUIREMENT

United States publicly traded companies own an estimated five trillion dollars in trade secret information.[23] Trade secrets are important to businesses of all sizes, from the smallest operations to the largest multi-national entities.[24] Trade secrets are often a company's most valuable intangible assets,[25] and a company's survival may depend on its ability to protect its trade secrets. In the digital age, securing information can be especially daunting because once a trade secret has been disclosed, even if inadvertently, it ceases to be a trade secret.[26]

A trade secret can be any information of value used in one's business that has been kept secret and provides an economic advantage over competitors.[27] The wide range of information that is entitled to trade secret protection includes customer lists, costs, sales records, customer information, marketing strategies, secret contract terms, unpublished pricing information, and chemical formulas.[28] Trade secrets sometimes encompass a majority of a company's assets,[29] and prior to obtaining patent protection, virtually all inventions are covered by trade secret protection.[30] The reasonable efforts requirement is probably the most important factor in determining whether a trade secret holder owns a protectable trade secret.[31]

---

23 *See* John P. Hutchins, *The Corporation's Valuable Assets: IP Rights under SOX*, *in* 26TH ANNUAL INSTITUTE ON COMPUTER & INTERNET LAW 289, 292 (PLI Intellectual Prop., Course Handbook Series No. G-859, 2006).

24 *See generally id.*; ROBERT P. MERGES, ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 34-35 (4th ed. 2006) (discussing the importance of trade secrets to small companies).

25 R. Mark Halligan, *Trade Secrets and the Inevitable Disclosure Doctrine*, BRIEFLY . . . PERSP. ON LEG. REG. & LITIG., Oct. 2001, at 7.

26 While the risk of loss is one that is inherent in choosing this form of protection, it does not necessarily suggest that a trade secret owner should have instead chosen patent protection. The choice of trade secret protection or patent protection must be based on a very careful assessment of the particular information involved and thorough consideration of business and legal factors involving, for example, the nature of the information, the ease with which it can be reverse engineered, and the feasibility and cost of obtaining patent protection. *See generally* Beckerman-Rodau, *supra* note 6. Accordingly, one who chooses trade secret protection over patent protection has not necessarily forgone a "better" form of protection, especially since there is a wide range of information that is eligible for trade secret protection but not patent protection. *See* JAMES POOLEY, TRADE SECRETS § 3.01[1][a] (1997).

27 *See* UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2005); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. d (1995).

28 *See, e.g.*, PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1265-70 (7th Cir. 1995); ConAgra, Inc. v. Tyson Foods, Inc., 30 S.W.3d 725, 728-30 (Ark. 2000); McFarland v. Brier, No. C.A. 96-1007, 1998 WL 269223, at *3 (R.I. Super. Ct. May 13, 1998), *vacated*, 769 A.2d 605 (R.I. 2001).

29 Hutchins, *supra* note 23, at 291-92.

30 *See* Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 155 (1989).

31 *See, e.g.*, MBL (USA) Corp. v. Diekman, 445 N.E.2d 418, 425 (Ill. App. Ct. 1983) ("Although many factors should be considered to determine if a trade secret exists, what is of primary importance is

A. *Sources of the Reasonable Efforts Requirement*

Trade secret law is governed by state law, and the manner in which the reasonable efforts requirement enters into a trade secret misappropriation analysis is determined by the source of trade secret law followed by that state.[32] As this subpart will illustrate, whether the state follows the *Restatement of Torts*, the Uniform Trade Secrets Act ("UTSA"), or the *Restatement of Unfair Competition*, the reasonable efforts[33] requirement is an important part of the analysis in every trade secret case. As a general matter, the two main legal questions in a trade secret case are first, whether the plaintiff owns a legally protectable trade secret and, if so, second, whether the defendant misappropriated it.[34]

In almost every state, the reasonable efforts requirement is embedded in the threshold legal question of the misappropriation analysis: whether the plaintiff owns a legally protectable trade secret.[35] The UTSA, which has been adopted by forty-six states and the District of Columbia,[36] includes reasonable efforts as part of the definition of a trade secret.[37] Reasonable efforts require that in order to qualify for trade secret protection, the information must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[38] The states that have not adopted the UTSA rely on the older codification of trade secret law in the *Restatement of Torts*.[39] However, even the *Restatement of Torts* requires a trade secret holder to show more than mere intent to protect something as a trade secret; actual effort to keep the information secret is necessary.[40] Thus, the *Restatement of Torts* includes "the extent of measures taken by [the trade secret owner] to guard the secrecy of the information" as one of six factors to

---

'whether and how an employer acts to keep the information secret.'" (quoting Lincoln Towers Ins. Agency v. Farrell, 425 N.E.2d 1034, 1037 (Ill. App. Ct. 1981))).

32 Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 6 (2007).

33 *Id.* at 42-52.

34 UNIF. TRADE SECRETS ACT (prefatory note) (amended 1985), 14 U.L.A. 538 (2005) ("For liability to exist under this Act, a . . . trade secret must exist and either a person's acquisition of the trade secret, disclosure of the trade secret to others, or use of the trade secret must be improper . . . .").

35 Risch, *supra* note 32, at 6-7.

36 Unif. Law Comm'rs, *A Few Facts About the Uniform Trade Secrets Act*, http://www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-utsa.asp (last visited Sept. 16, 2009).

37 *See* UNIF. TRADE SECRETS ACT § 1(4)(ii) (amended 1985), 14 U.L.A. 538 (2005).

38 *See id.*

39 *See* POOLEY, *supra* note 26, §§ 2.02[3], 2.04[3].

40 Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 901 (Minn. 1983) ("[E]ven under the common law, more than an 'intention' was required—the plaintiff was required to show that it had manifested that intention by making some effort to keep the information secret.").

be considered in determining whether information qualifies as a trade secret.[41]

The *Restatement (Third) of Unfair Competition* has supplanted the *Restatement of Torts* in codifying the common law of trade secrets.[42] Unlike the UTSA and the *Restatement of Torts*, the *Restatement (Third) of Unfair Competition* does not include reasonable efforts in defining a trade secret.[43] Rather, the determination of reasonable efforts is part of the second question in the misappropriation analysis, focusing on whether the defendant misappropriated the trade secret.[44] In determining whether a defendant's acquisition of a trade secret was improper, the *Restatement (Third) of Unfair Competition* calls for an evaluation of "the extent to which the acquisition was facilitated by the trade secret owner's failure to take reasonable precautions against discovery of the secret by the means in question."[45] The *Restatement* further suggests that the "foreseeability of the conduct through which the secret was acquired" should be relevant to determining reasonableness.[46] This principle from the *Restatement (Third) of Unfair Competition*, although different from the UTSA's formulation for determining the ultimate question of misappropriation, nonetheless supports this Article's premise that a trade secret owner's failure to guard against foreseeable technological incursions should bar recovery.[47]

---

41 RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939). The remaining five factors are: "(1) the extent to which the information is known outside of [the] business; (2) the extent to which it is known by employees and others involved in [the] business; . . . (4) the value of the information to [the business] and to [its] competitors; (5) the amount of effort or money expended by [the business] in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others." *Id.*

42 When the *Restatement (Second) of Torts* was published in 1979, the reporters decided that trade secret law was best addressed under the principles of unfair competition law rather than tort law, and therefore omitted it. RESTATEMENT (SECOND) OF TORTS div. 9, introductory note (1979). In 1995, trade secret law was restated in the *Restatement (Third) of Unfair Competition*, and those rules are intended to apply to both common law actions and actions under the Uniform Trade Secrets Act. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 reporters' note (1995).

43 Rather, it defines a trade secret as "any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995). The comment to this section notes, however, that "precautions taken to maintain the secrecy of information are relevant in determining whether the information qualifies for protection as a trade secret," but "if the value and secrecy of the information are clear, evidence of specific precautions taken by the trade secret owner may be unnecessary." *Id.* at cmt. g.

44 *Id.* at cmt. f.

45 *Id.* § 43 cmt. c.

46 *Id.*

47 To some extent, this premise bears some similarity to Guido Calabresi's least-cost-avoider approach in law and economics theory, because it requires the court to assign loss to the trade secret owner, the party who was in a better position to take optimal precautions, partly to incentivize this and other trade secret owners to take better precautions in the future. *See generally* GUIDO CALABRESI, THE COSTS OF ACCIDENTS 135, 155 (1970). While Calabresi's analysis of finding the least-cost-avoider is

Similar to the UTSA, the Economic Espionage Act ("EEA"), the federal criminal trade secret statute, also includes a reasonable efforts requirement in defining a trade secret.[48] The EEA requires that "the owner thereof has taken reasonable measures to keep such information secret."[49] This provision withstood a void for vagueness challenge, with the court finding that the term "reasonable measures" is not unconstitutionally vague.[50] As a result, apart from the perennial difficulty in nailing down the definition of "reasonable," for the purposes of this Article we need not quibble about the use of a *reasonable* efforts standard. Since courts continue to rely on the *Restatement of Torts*, and the *Restatement (Third) of Unfair Competition* is applicable in both UTSA and non-UTSA jurisdictions,[51] the reasonable efforts requirement appears securely grounded in trade secret jurisprudence.

In sum, the modern view of trade secret law under the UTSA (and the EEA) makes the reasonable efforts requirement a separate requirement for secrecy, whereas the alternative common law view in the Restatements includes it as evidence of secrecy. Normatively, it makes sense to treat the reasonable efforts requirement as a separate requirement because it encourages courts and litigants to filter out those putative trade secrets whose value is only recognized by the plaintiff after the alleged misappropriation occurs.[52] In addition, it helps clarify that secrecy is a requirement separate from the requirement that the information not be generally known.[53] As a practical matter, treating reasonable efforts as a requirement provides consistency to the definition of a trade secret, and preserves the evidentiary importance of steps to protect the secret in trade secret litigation.[54]

B. *Principles from the Case Law*

While the above sources of law provide the underpinning for the reasonable efforts requirement, they do not provide precise standards to the

---

much more complex than this, and this Article does not approach the problem from a law and economics perspective, it is worth noting the strands of overlap with the essence of his theory.

48 18 U.S.C. § 1839(3)(A) (2000).

49 *Id.*

50 United States v. Kai-Lo Hsu, 40 F. Supp. 2d 623, 628 (E.D. Pa. 1999).

51 Many courts, in both UTSA and non-UTSA jurisdictions, continue to rely on and cite to the *Restatement (First) of Torts*. POOLEY, *supra* note 26, § 2.02[3] n.12.

52 *But see* Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 349-50 (2008) (arguing that reasonable efforts should not be used as a separate requirement, but as evidence of secrecy).

53 Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974) ("The subject of a trade secret must be secret, and must not be of public knowledge or of a general knowledge in the trade or business.").

54 *See infra* Parts I.B.1-3.

courts on how to determine whether the requirement has been met.[55] The interpretation of the requirement appears to be similar in all jurisdictions such that for the purposes of this Article no further distinctions are necessary between UTSA and non-UTSA states. Whether a trade secret owner has utilized appropriate safeguards sufficient to meet the reasonable efforts requirement is a question of fact, based on the particular circumstances.[56] These decisions necessitate a balancing between using sufficient precautions to protect a company's secret on the one hand, while not imposing overly-burdensome precautions that would impair the functioning of its business on the other hand.[57] The inquiry necessarily calls for a cost-benefit analysis, which varies in each case based on the costs of the protective measures relative to the attendant benefits of protecting the information.[58] The costs to the trade secret owner will not only include direct financial costs, but also indirect costs, such as the ability to make appropriate use of the information in the business by sharing it with employees and others who need to use it.[59]

1. Relative, Not Perfect, Secrecy Required

It is clear that reasonable efforts do not require absolute secrecy.[60] Rather, the standard is one of relative secrecy; a trade secret owner needs to take steps that are reasonably necessary under the circumstances to maintain secrecy.[61] The plaintiff must take affirmative steps and show concrete efforts to preserve the confidentiality of the alleged secret information.[62] Some courts note, for example, that in addition to requiring employees to sign confidentiality agreements, "reasonable efforts" can include "advising employees of the existence of a trade secret, limiting access to the information on a 'need to know basis,' ... and keeping secret documents under

---

55 See Note, *Trade Secret Misappropriation: A Cost-Benefit Response to the Fourth Amendment Analogy*, 106 HARV. L. REV. 461, 462 (1992).

56 *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 176-77 (7th Cir. 1991).

57 *See id.* at 178-80.

58 *See id.* at 179.

59 *Id.* at 180.

60 UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2005); *see also* Sheets v. Yamaha Motors Corp., 849 F.2d 179, 183-84 (5th Cir. 1988); Computer Assocs. Int'l v. Quest Software, Inc., 333 F. Supp. 2d 688, 696 (N.D. Ill. 2004) (noting that the Illinois Trade Secrets Act, which is based on the Uniform Trade Secrets Act, requires "reasonable measures, not perfection").

61 *Sheets*, 849 F.2d at 183.

62 *See, e.g.*, Niemi v. Am. Axle Mfr. & Holding, Inc., No. 269155, 2007 WL 29383, at *4 (Mich. Ct. App. Jan. 4, 2007) (granting summary judgment in favor of defendant, and finding that plaintiff did not take concrete efforts to preserve the confidentiality of designs by, for instance, failing to mark the documents as confidential or requiring confidentiality agreements); Dicks v. Jensen, 768 A.2d 1279, 1284 (Vt. 2001) (granting summary judgment in favor of defendant where there was "no evidence in the record that plaintiff took any measures to indicate that the customer list was confidential").

lock."[63] The use of security guards, closed-circuit television monitors, access codes for information stored on a computer, and varying security access levels for different areas of the facilities have also proven reasonable.[64] For ease of reference, this Article refers to these efforts as traditional facilities-based measures (vis-à-vis technical measures and processes).

2. Inferences Regarding Value and Improper Means

Efforts to protect secrecy are also tied to the requirement that trade secrets have value and, indeed, whether or not a company took adequate steps to protect a secret is evidence of the subjective belief that the information was a trade secret and thus worthy of protection.[65] Some courts may reason that there is a direct relationship between the value of the information and the extent to which the company made efforts to protect it such that the more valuable the information to the company, the more costly or extensive the measures ought to be to protect it.[66] Moreover, where a plaintiff makes a strong showing of reasonable efforts to protect trade secret information, a court is also more likely to infer that the defendant used improper means to obtain the information.[67] However, a trade secret owner who is lax about taking precautions to prevent the secret from escaping cannot expect to bar others from using it.[68] Thus, a court may use the reasonable efforts requirement to deny a plaintiff any protection under trade secret law.[69] As one court aptly noted:

---

[63] *See, e.g.*, Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., 923 F. Supp. 1231, 1253 (N.D. Cal. 1995); Twin Vision Corp. v. BellSouth Commc'n Sys., Inc., 152 F.3d 929, 1998 WL 385135 (9th Cir. 1998) (unpublished table decision); *see also* Surgidev Corp. v. Eye Tech., Inc., 648 F. Supp. 661, 693-94 (D. Minn. 1986), *aff'd*, 828 F.2d 452 (8th Cir. 1987).

[64] Schalk v. State, 767 S.W.2d 441, 447-48 (Tex. Ct. App. 1988), *aff'd*, 823 S.W.2d 633 (Tex. Crim. App. 1991) (en banc).

[65] Metallurgical Indus. Inc. v. Fourtek, Inc., 790 F.2d 1195, 1199-1200 (5th Cir. 1986) (reasoning that secrecy measures constitute evidence probative of existence of a trade secret).

[66] Jermaine S. Grubbs, Comment, *Give the Little Guys Equal Opportunity at Trade Secret Protection: Why the "Reasonable Efforts" Taken by Small Businesses Should be Analyzed Less Stringently*, 9 LEWIS & CLARK L. REV. 421, 426 (2005).

[67] *Id.* at 427; Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179 (7th Cir. 1991) ("The greater the precautions that [plaintiff] took to maintain the secrecy of the piece part drawings, the lower the probability that [defendant] obtained them properly and the higher the probability that it obtained them through a wrongful act . . . .").

[68] *See, e.g.*, Fisher Stoves, Inc. v. All Nighter Stove Works, Inc., 626 F.2d 193, 196 (1st Cir. 1980) (where plaintiff carelessly left customer data at customer's store, competitor who accidentally discovered it should not be enjoined); Defiance Button Mach. Co. v. C & C Metal Prods. Corp., 759 F.2d 1053, 1056-57, 1063 (2d Cir. 1985) (finding that defendant's use of consumer list could not be enjoined when plaintiff left the file in an old computer that was subsequently sold).

[69] *See, e.g.*, Dicks v. Jensen, 768 A.2d 1279, 1284 (Vt. 2001) ("It would be anomalous for the courts to prohibit the use of information that the rightful owner did not undertake to protect.").

> [i]f [plaintiff] expended only paltry resources on preventing its . . . drawings from falling into the hands of competitors . . . , why should the law, whose machinery is far from costless, bother to provide [plaintiff] with a remedy? The information contained in the drawings cannot have been worth much if [plaintiff] did not think it worthwhile to make serious efforts to keep the information secret.[70]

Indeed, even when a plaintiff creates a trade secret protection plan, which provides for how the secrets will be safeguarded, but fails to adequately follow it, a court could find such conduct to be unreasonable vis-à-vis the hypothetical reasonable person.[71]

3. Evidence of Reasonable Efforts

In practice, the question of whether the reasonable efforts requirement has been met necessarily varies from case to case.[72] The plaintiff must produce sufficient evidence to prove that the alleged trade secret was the subject of reasonable efforts to protect its secrecy.[73] The language the courts use is not always consistent, but courts often look for the use of the following kinds of security measures in assessing reasonableness: (1) confidentiality agreements; (2) exit interviews reminding departing employees of their confidentiality obligations; (3) security badges to enter the premises or secured areas; (4) security guards and closed-circuit television cameras; and (5) computer passwords or access codes restricting access to certain personnel.[74] Even where a trade secret owner implements security measures internally with employees, it must also be mindful of external protections, such as with customers and vendors, and failure to do so could lead to a court denying trade secret protection.[75]

---

70 *Rockwell*, 925 F.2d at 179.

71 *See* Gemisys Corp. v. Phoenix Am., Inc., 186 F.R.D. 551, 558, 567 (N.D. Cal. 1999) (granting summary judgment in favor of defendant licensee where plaintiff failed to use confidentiality legends on documents pursuant to the terms of its license agreement).

72 *See supra* notes 56-59.

73 *See, e.g.*, Gillis Associated Indus., Inc. v. Cari-All, Inc., 564 N.E.2d 881, 886 (Ill. App. Ct. 1990) (finding that plaintiff had not produced sufficient evidence of affirmative measures to keep its customer list secret).

74 Schalk v. State, 823 S.W.2d 633, 637-40 (Tex. Crim. App. 1991); *Gillis Associated*, 564 N.E.2d at 886 (finding that plaintiff failed to take such affirmative measures as using internal or external physical security, confidentiality agreements, confidentiality stamps, or entrance and exit interviews imparting the importance of confidentiality). *See also* Otis Elevator Co. v. Intelligent Sys., Inc., 17 U.S.P.Q.2d 1773, 1775 (Conn. Super. Ct. 1990) (finding that plaintiff employed reasonable measures to protect its trade secrets when plaintiff limited access to premises by personally escorting visitors while on site, video monitoring doors and parking lots, and requiring photo identification badges).

75 *See, e.g.*, Flotec, Inc. v. S. Research, Inc., 16 F. Supp. 2d 992, 1004-05 (S.D. Ind. 1998) (noting that plaintiff used safeguards internally with its own employees but failed to do so with prospective supplier); Carboline Co. v. Lebeck, 990 F. Supp. 762, 767-68 (E.D. Mo. 1997) (noting that plaintiff

4. Digital Misappropriation

When alleged misappropriation occurs by electronic means, many cases analyzing reasonable precautions nonetheless continue to focus on traditional facilities-based security measures.[76] Thus, for instance, courts generally examine the use of non-disclosure agreements, steps to secure the facility, notice to employees about protecting trade secrets, and the use of passwords.[77] In more recent cases, however, courts are beginning to pay more attention to technical protection measures, going beyond the use of traditional measures.[78] In such recent circumstances, steps omitted can be just as important as steps taken.[79] For instance, in a case where an employee downloaded a file consisting of a nine-hundred-page electronic document that allegedly contained trade secrets, the plaintiff argued that its efforts to protect the file were reasonable because it

> (1) required its employees to sign confidentiality agreements that covered "this sort of information," (2) it was available only to [plaintiff's] employees on its password- and firewall-protected main network, and (3) because [plaintiff] instituted physical security measures to make sure no outsiders could access it.[80]

The court disagreed, however, noting that the plaintiff failed to show that it

> (1) labeled the file confidential or otherwise communicated the confidentiality of the ... file directly to its employees, (2) directed its employees to maintain the secrecy of the file (other than through a general confidentiality agreement which did not expressly mention the ... file), or (3) tracked or otherwise regulated the use of [the] file.[81]

Accordingly, the court held that the plaintiff's efforts were not reasonable under the circumstances.

Unfortunately, the only thing consistent about the way in which the courts analyze reasonable efforts in these digital misappropriation cases is the inconsistency in both the approach and outcomes. In one case, the court found that the plaintiff had taken reasonable measures to protect a trade secret that was kept on a computer and protected by a password because the plaintiff used licensing agreements, a password protected Web site, and

---

required employees to sign confidentiality agreements and limited their access to secret data on its computer system, but did not use adequate safeguards in circulating the information to customers).

76 *See, e.g.*, Schalk v. State, 767 S.W.2d 441, 447-48 (Tex. Ct. App. 1988), *aff'd*, 823 S.W.2d 633 (Tex. Crim. App. 1991) (en banc) (defendant accused of stealing computer programs).

77 *Id.*

78 *See, e.g.*, Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1334-35 (N.D. Ga. 2007).

79 *See id.* at 1335.

80 *Id.*

81 *Id.*

generally kept the secrets out of the public display at conventions.[82] In another case, a court found that the use of encrypted e-mail to transmit the alleged trade secret and password protection were insufficient to meet the requirement given the lack of other security measures.[83] Still, other courts do not address the issue directly, disposing of the cases on other grounds.[84]

5. The *Four Seasons* Illustration

The facts of *Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A.*[85] provide a vivid and dramatic illustration of digital misappropriation. The story occurs mostly in Caracas, Venezuela, where the corporate defendant, Consorcio, is the owner of the building which housed the Four Seasons Hotel Caracas.[86] Consorcio entered into various agreements with Four Seasons Hotels whereby the Four Seasons would manage the operations of the hotel and license its brand name and trademarks to Consorcio in connection with the operation of the hotel.[87] Pursuant to these agreements, while Consorcio could have received from Four Seasons hard copy printouts of guest histories upon request, it was not entitled to any of the proprietary electronic data that Four Seasons considered trade secret information, such as detailed guest information in databases and financial management information.[88]

When Four Seasons refused to grant Consorcio access to this information, Consorcio took drastic measures to obtain the information. To begin with,

> a group of Consorcio's personnel, including armed security guards, forcibly entered the Four Seasons' computer systems room . . . [and u]nder the pretext of self-executing a Venezuelan court order . . . downloaded onto back-up tapes all of the guest information and data stored electronically on [one of Four Seasons' servers] in Caracas, as well as all of the financial information and data stored electronically on [another Four Seasons] server.[89]

---

82 QSRSoft, Inc. v. Rest. Tech. Inc., 84 U.S.P.Q.2d 1297, 1303 (N.D. Ill. 2006).

83 Heartland Home Fin., Inc. v. Allied Home Mortgage Capital Corp., No. 1:05CV2659, 2007 WL 436048, at *4-5 (N.D. Ohio Feb. 5, 2007), *aff'd*, 258 F. App'x 860 (6th Cir. 2008).

84 *See, e.g.*, Twin Vision Corp. v. Bellsouth Commc'n Sys., Inc., 152 F.3d 929, 1998 WL 385135, at *3 (9th Cir. 1998) (unpublished table decision) ("We need not decide whether encryption alone is adequate evidence that [plaintiff] made a reasonable effort to preserve the secrecy of its factory access code because we find that it has not met its burden in regard to misappropriation.").

85 267 F. Supp. 2d 1268, 1271-72 (S.D. Fla. 2003), *aff'd in part, rev'd in part sub nom.* Four Seasons Hotels v. Consorcio Barr S.A., 138 F. App'x 297 (11th Cir. 2005).

86 *Id.* at 1271-72.

87 *Id.* at 1272.

88 *Id.* at 1280-81.

89 *Id.* at 1279-80.

Consorcio personnel (more specifically, the former assistant to the Four Seasons' Manager of Information Technology) then transferred the downloaded information to a laptop, and using the Four Seasons' IT Director's password gained full access to the databases.[90]

Prior to that time, Consorcio also took other steps to acquire Four Seasons' proprietary data by, for instance, intercepting the hotel's e-mail communications[91] and using a program to attempt to crack Four Seasons' passwords.[92] Consorcio also hired Bencomo, the former Assistant Systems Administrator at the Four Seasons,[93] who came equipped with inside knowledge of the Four Seasons computer networks, as well as the administrative and user passwords.[94] A forensic examination of Bencomo's laptop revealed thirty-eight e-mails sent to Consorcio that contained Four Seasons' data in encrypted spreadsheets.[95] Bencomo was also believed to have engaged in "spoofing" to access the Four Seasons network.[96] As described in the case, spoofing occurs when a person, in attempting to gain access to a network, sets up a fake internet protocol ("IP") address which is not traceable back to their own IP address.[97] Not surprisingly, the court found Consorcio liable for misappropriation.[98]

While not all trade secret misappropriation cases are this dramatic, misappropriation through technology occurs regularly and often surreptitiously.[99] The next Part discusses the ways in which trade secrets have become more vulnerable because of the use of technological tools in the workplace. The Part examines some of the tools that augment the ease with which trade secrets can be stored, accessed, and disseminated.

II. THE DIGITAL WORLD

Computers are present in virtually every workplace. A reported seventy-seven million people use a computer at work.[100] Employees most often use computers to access the Internet or to communicate by e-mail,[101] the very kinds of conduct that could quickly disseminate trade secrets. The em-

---

90 *Id.* at 1281, 1283.

91 *Four Seasons*, 267 F. Supp. 2d at 1289.

92 *Id.* at 1292.

93 *Id.* at 1293.

94 *Id.* at 1293, 1294-95.

95 *Id.* at 1296.

96 *Id.* at 1298.

97 *Four Seasons*, 267 F. Supp. 2d at 1298, 1304.

98 *Id.* at 1325.

99 *See infra* Parts II.A. and II.B.1.

100 Press Release, Dep't. of Labor, Computer and Internet Use at Work Summary (Aug. 2, 2005), *available at* http://www.bls.gov/news.release/ciuaw.nr0.htm.

101 *Id.*

ployer's workplace has also expanded into homes, as approximately twelve million[102] employees work full-time from home as telecommuters, an increasing trend in recent years.[103] Management, professional, and sales employees are especially likely to use technology in the workplace and also are among those most likely to telecommute.[104]

The digital world complicates the protection of trade secret information and increases the likelihood of destroying trade secret status of misappropriated information.[105] This is because information in digital form can be stored and processed in so many ways that it becomes very difficult to track and control.[106] There is a tension between the need to keep information secret and modern technological methods that allow the information to be easily accessed, reproduced, and disseminated. Of course, the social benefit of modern technology is perhaps incalculable. Nevertheless, information breaches occur most commonly through such activities as "unauthorized access to information, loss of laptop and mobile devices, theft of proprietary information, and insider e-mail abuses," and more than half of these breaches occur as a result of corporate mismanagement of the information or from insiders who abuse their access.[107] A 2008 report of data breaches to date revealed that most were the result of lost or stolen laptops, hard drives or thumb drives, and the posting of sensitive data on Web sites or distribution through e-mail.[108]

Unlike the traditional options of file cabinets or boxes, laptops, personal digital assistants ("PDAs"), cell phones, Universal Serial Bus ("USB")[109] flash drives, portable hard drives, iPods, and MP3 players are among the many possible locations where one might download and store electronic information.[110] As even Congress observed, "[c]omputer technology enables rapid and surreptitious duplications of the information. Hundreds of pages of information can be loaded onto a small computer diskette,

---

102 Alison Grant, *Taking a Big Risk: Surge in Telecommuters Creates New Twists, Novel Legal Questions and Employer Problems*, CLEVELAND PLAIN DEALER, Feb. 4, 2007, at G1 ("More than 12 million Americans are full-time telecommuters, and another 33 million do at least part of their job at home, according to the nonprofit WorldatWork.").

103 Sue Shellenbarger, *Some Companies Rethink the Telecommuting Trend*, WALL ST. J., Feb. 28, 2008, at D1 (noting that from 2005 to 2007 there was a 30 percent increase in the number of full-time employees working from home).

104 *See* Grant, *supra* note 102, at G1.

105 Robert P. Green & Glenn Dickinson, *Inside Job: Without the Right IP Protection Internal Abuse is a Fear-Inducing Threat*, CAL. CPA, July 2007, at 19.

106 *Id.*

107 *Id.*

108 Brian Krebs, *Data Breaches Hit 8.3 Million Records in First Quarter*, WASH. POST, Apr. 3, 2008, at D3.

109 Universal Serial Bus drive is a type of serial bus that allows peripheral devices such as disks, modems, printers, digitizers, and data gloves to be easily connected to a computer. Joseph Kahn, *Between Wall Street and Silicon Valley, a New Lexicon*, N.Y. TIMES, Jan. 1, 2000, at C1.

110 Green & Dickinson, *supra* note 105, at 19.

placed into a coat pocket, and taken from the legal owner."[111] While this Article focuses on trade secret misappropriation, there may be other causes of action available where a computer has been used inappropriately to transmit or intercept information.[112]

A. *Easier Storage and Accessibility*

While once it might have required several file cabinet drawers filled with paper to store sensitive business information, today that information can be stored in a single spreadsheet or document, or stored on a computer's hard drive. It can then be downloaded onto a USB thumb drive, which is literally about the size of one's thumb, and connected to another computer anywhere to read the information. This means that for someone intending to steal the information, instead of having to photocopy hundreds of pages of documents and load them into boxes or folders to leave the building, it is a simple matter to either download the information, within seconds, onto a thumb size storage device that fits easily into a pocket, or attach the information to an e-mail sent to an outside account where it can later be easily retrieved.

The risk of misappropriation involving these new storage devices is already evident in trade secret misappropriation cases. For example, in one case, an employee misappropriated his employer's trade secrets by downloading the equivalent of 1.5 million pages of raw text onto two USB drives.[113] The employee attached a thumb drive to his desktop computer

---

[111] S. REP. No. 104-359, at 6 (1996).

[112] For instance, the Computer Fraud and Abuse Act ("CFAA") prohibits accessing a computer without authorization to obtain information. 18 U.S.C. § 1030 (2000). The phrase "without authorization" is not defined in the Act and it is questionable whether it would cover an employee who at the time of accessing the information was permitted to access the computers, even if the later use of the information were unauthorized. *See* Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1341-44 (N.D. Ga. 2007) (recognizing a split among the courts on the interpretation of "without authorization," but holding that "a violation does not depend upon the defendant's unauthorized use of *information*, but rather upon the defendant's unauthorized use of *access*."). It may therefore be applicable where employees use the employer's computer to send "unauthorized" e-mail with confidential information to others, including prospective new employers. 18 U.S.C. § 1030. The CFAA provides both criminal and civil remedies, including a private right of action against a person who intentionally causes damage to a protected computer. *Id.* § 1030(g), (a)(5)(A). A "protected computer" is a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." *Id.* § 1030(e)(2)(B). In addition, use of e-mail to encourage an employee to reveal trade secrets can be prosecuted as wire fraud insofar as it comprises a scheme to defraud the employer. *Id.* § 1343. The Electronic Communications Privacy Act ("ECPA") may also apply where one intercepts, or endeavors to intercept, any electronic communication. *Id.* § 2511(1)(a).

[113] Anadarko Petroleum Corp. v. Davis, No. H-06-2849, 2006 WL 3837518, at *6 (S.D. Tex. Dec. 28, 2006).

several times before his departure in order to copy files, which he then transferred to the desktop computer at his new employer and also onto the new employer's computer servers.[114]

In another case, a departing employee transferred, among other things, a sensitive five-hundred-page document to his home computer while working for the plaintiff, but after he had already accepted employment from the plaintiff's principal competitor.[115] The employee made the transfer by downloading the files from his employer's computer system to a zip drive and then later transferring the information from the zip drive to his home computer.[116] In yet another case, an employee provided confidential customer lists on a USB drive to a competitor.[117] Thus, the very ease with which large amounts of information can now be stored rapidly, transported quickly, and later accessed in the original format provides greater incentive and opportunity for it to be removed.

The use of servers to consolidate, store, and publish information can also pose risks to trade secrets. Information that previously might have been locked away in dusty file cabinets scattered across many offices, or even the globe, can now be accessed immediately by every employee in an organization.[118] Employees can then download a wide range of information onto personal laptops or miniaturized storage devices.[119] Wireless networks are popular because of the lower cost and greater convenience that they offer relative to wired connections.[120] Unfortunately, these wireless networks are much more vulnerable to intrusion than hard-wired networks and pose high security risks if left unprotected.[121]

Finally, laptop computers epitomize information portability. They enable employees to take valuable data to any location. When an employee connects her corporate laptop to wireless networks such as public Wi-Fi[122]

---

114 *Id.*

115 *Diamond Power*, 540 F. Supp. 2d at 1329.

116 *Id.* at 1330.

117 AirDefense, Inc. v. AirTight Networks, Inc., No. C 05-04615JF, 2006 WL 2092053, at *1 (N.D. Cal. July 26, 2006).

118 *See, e.g.*, Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1283 (S.D. Fla. 2003), *aff'd in part, rev'd in part sub nom.* Four Seasons Hotels v. Consorcio Barr S.A., 138 F. App'x 297 (11th Cir. 2005) ("The Lotus Notes server was connected to all of the servers for all Four Seasons' worldwide to allow e-mail communication. Aside from that, it also provided access to Four Seasons' corporate databases which provided other information.").

119 *See, e.g.*, Liebert Corp. v. Mazur, 827 N.E.2d 909, 917 (Ill. App. Ct. 2005) (employee downloaded sensitive pricing information from company server onto his laptop computer).

120 See Anita Ramasastry, Jane K. Winn & Peter Winn, *Will Wi-Fi Make Your Private Network Public? Wardriving, Criminal and Civil Liability, and the Security Risks of Wireless Networks*, 1 SHIDLER J.L. COM. & TECH. 9 (2005).

121 *Id.*

122 "Wi-Fi is the wireless equivalent of [a] wired internal local area network" and it permits a connection to the Internet. PCMag.com, Wi-Fi Definition from PC Magazine Encyclopedia, http://www.pcmag.com/encyclopedia_term/0,2542,t=Wi-Fi&i=54444,00.asp (last visited Aug. 9, 2009).

connections or "hot spots,"[123] information stored on the laptop is susceptible to hackers.[124] In addition, the theft of a laptop can expose a company's most sensitive information to misappropriation, posing challenges to data security and trade secret protection. For instance, the personal data of about twenty-six million veterans and military troops was recently exposed when a burglar stole a laptop from the home of an employee of the U.S. Department of Veterans Affairs.[125] If this kind of theft led to a large scale exposure of trade secrets, it could be devastating to a company, as the trade secret protection in all of the now public data would be lost.

Companies should therefore pay closer attention to laptop security and to policies governing employees' use of laptops. Boeing Co., for instance, "requires employees to access most sensitive information through company servers instead of downloading the data to a laptop . . . [and] employees working with payroll data must use a cable lock to physically secure their laptops to a desk at all times."[126] ING America requires the installation of encryption software[127] on all laptops before they can leave the premises.[128] Both of these companies' laptop policies resulted from having suffered recent, high profile laptop thefts;[129] with trade secrets there are no second chances at protection once the secrets have been exposed.[130]

---

123 A hot spot is the "geographic boundary covered by a Wi-Fi . . . wireless access point." PCMag.com, Hot Spot Definition from PC Magazine Encyclopedia, http://www.pcmag.com/encyclopedia_term/0,2542,t=HotSpot&i=44405,00.asp (last visited Aug. 9, 2009).

124 *See* Paola Singer, *A Secure Laptop on the Go*, WALL ST. J., May 13, 2008, at D1.

125 Pamela Yip, *Firms Ready to Put Leash on Laptops*, DALLAS MORNING NEWS, July 15, 2006.

126 *Id.*

127 Encryption software changes plain text into non-readable form, requiring a "key" to decrypt the information. It provides enhanced security because if the information is intercepted in transit and the receiver does not have the appropriate key, the encrypted information will generally be unreadable. WiseGeek.com, What is Encryption?, http://www.wisegeek.com/what-is-encryption.htm (last visited Aug. 10, 2009).

128 Yip, *supra* note 125.

129 The Boeing thefts, which occurred in November 2005 and April 2006, exposed thousands of current and former employees' social security numbers and addresses. The ING laptop stolen in June 2006 contained retirement plan information on 13,000 employees. *Id.*

130 As of the writing of this Article, I am not aware of any trade secret losses as a result of stolen laptops. However, this may be explained by the fact that such instances would not be reported. Companies have no incentives to report this kind of trade secret theft since it could cause embarrassment to the company and might lead to other kinds of losses as well, such as a drop in stock prices. Privacy laws and state breach notification laws require disclosures when companies suffer data security breaches. *See, e.g.*, CAL. CIV. CODE § 1798.29 (West 2008), N.Y. GEN. BUS. LAW § 899-aa (McKinney 2008), DEL. CODE ANN. tit. 6, § 12B-102 (2008), ARK. CODE ANN. § 4-110-105 (2008). However, no such mandatory disclosure is in place for trade secret losses.

B. *Easier Dissemination*

Trade secret law only protects secret information.[131] With the click of a mouse or the push of a button, e-mail, the Internet, and even cell phones can expose trade secrets to potentially millions of people within seconds. Once a trade secret becomes public, its owner may be rendered powerless to stop third parties, including competitors, from using it, and the trade secret owner also faces the complete loss of trade secret status.[132] Accordingly, the grave risks posed by these technologies cannot be left unaddressed.

1. E-Mail

One need not even attach a physical device to a work computer to transfer information. E-mail can transfer most files and other data with little effort. Furthermore, even without attachments, information can also be exchanged in the text of the message. Many trade secret cases involve employees transmitting files containing trade secret information through e-mails. For example, in a case prosecuted under the EEA,[133] a product development manager gained access to secret product information belonging to a customer of his former employer.[134] After he later accepted new employment from a competitor of that customer, he downloaded the secret information and e-mailed it to his new employer.[135] In another case, an engineer with knowledge of secret software source codes was terminated from work.[136] In resentment, he sent e-mail messages to several competitors of his former employer, offering the secret software source codes for sale.[137] The terminated employee sent all of the messages from an alias e-mail ac-

---

131 *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) ("Information that is public knowledge or that is generally known in an industry cannot be a trade secret."); Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974) ("The subject of a trade secret must be secret, and must not be of public knowledge or of a general knowledge in the trade or business.").

132 *See* Lockridge v. Tweco Prods., Inc., 497 P.2d 131, 134 (Kan. 1972) ("Once the secret is published to the 'whole world' . . . it loses its protected status and becomes available to others for use and copying without fear of legal reprisal from the original possessor.").

133 18 U.S.C. § 1832 (2000).

134 Press Release, Dep't of Justice, Silicon Valley Engineer Indicted for Stealing Trade Secrets and Computer Fraud (Dec. 22, 2005), *available at* http://www.usdoj.gov/criminal/cybercrime/zhangIndict.htm.

135 *Id.*

136 Press Release, Dep't of Justice, Former Engineer of White Plains Software Company Receives Two Years in Prison for Theft of Trade Secret (Oct. 15, 2002), *available at* http://www.usdoj.gov/criminal/cybercrime/kissaneSent.htm.

137 *Id.*

count at a public library in order to mask the sender's identity.[138] To his surprise, the competitor brought those messages to the attention of his former employer.[139] His identity was eventually revealed when the FBI's Computer Hacking and Intellectual Property Squad detected accesses to the alias e-mail account through his home Internet connection.[140]

Trade secret information can also be transmitted by employees from their corporate e-mail account to their private e-mail accounts and to competitors.[141] In a case that made headlines recently, seven former Citibank employees were accused of e-mailing secret client data from work to their personal e-mail addresses before leaving to join a competitor.[142] As a result of these bankers' use of Citibank's trade secret information to lure away clients, Citibank is alleged to have lost about $50 million of business.[143]

In another example, a researcher who was responsible for developing and manufacturing veterinary diagnostic kits for IDEXX became dissatisfied with her job and began to consider leaving the company.[144] As part of her plan to find new employment, she exchanged e-mails with a competitor who tried to lure her away with promises of potential employment opportunities.[145] During her e-mail exchanges with the competitor, the researcher disclosed proprietary company information and transmitted to the competitor software and computer files containing a variety of IDEXX trade secrets.[146] Ironically, the researcher's activities were only discovered after she accidentally sent her supervisor one of the e-mails—addressed to the competitor—that contained the company's trade secret files.[147] The employer's discovery was especially fortuitous because the dissatisfied employee had resigned from the company the day before she inadvertently sent the e-mail to her former supervisor.[148] Absent her mistake, it is very unlikely that she would have been caught.

Instant messaging is on the rise in the workplace, providing what e-mail does not: real-time conversations and an indication of which contacts are available at a given time.[149] Messaging poses the same kinds of security risks as e-mail, and it is estimated that about one-third of employees in the

---

138 *Id.*

139 *Id.*

140 *Id.*

141 *See, e.g.*, Posdata Co. v. Kim, No. C-07-02504 RMW, 2007 WL 1848661, at *2-3 (N.D. Cal. June 27, 2007).

142 Nur Dianah Suhaimi, *Stealing Office Data? Computer Forensics Can Track You Down*, STRAITS TIMES (Sing.), Jan. 27, 2008.

143 *Id.*

144 United States v. Martin, 228 F.3d 1, 6 (1st. Cir. 2000).

145 *Id.* at 7.

146 *Id.* at 8.

147 *Id.* at 10.

148 *Id.*

149 Carola Mamberto, *Instant Messaging Invades the Office*, WALL ST. J., July 24, 2007, at B1.

United States use instant messaging, often without the knowledge of their employers.[150] The security risks posed by instant messaging is a concern.[151] Some companies may choose to restrict instant messaging to intra-company communication between company employees rather than allowing the use of the public instant messaging network that can be vulnerable to inappropriate outsider access.[152] Other companies may decide to block employees' access to instant messaging at work all together.[153]

2. The Internet

Approximately 1.4 billion people use the Internet, and it is undoubtedly a powerful communication tool.[154] It has changed the way in which the world does business, and many companies today rely on computers and the Internet to survive.[155] Furthermore, employees access the Internet not only from their workplaces, but from home as well, as over 50 percent of all households are connected to the Internet.[156]

However, the Internet is a dangerous place for trade secrets.[157] Many courts assume that a trade secret posted on the Internet is generally known and consequently has lost its trade secret status.[158] Even when a party post-

---

150 *Id.*

151 *See, e.g.*, *Employers Fail to Manage Instant Messaging, Says Survey*, OUT-LAW NEWS, May 18, 2005, http://www.out-law.com/page-5713 (reporting on a survey in the United Kingdom that revealed 16 percent of employees used instant messaging to send or receive sensitive company materials).

152 *See, e.g.*, Nathan Eddy, *Concentric Offers Secure Messaging for MSBs*, EWEEK.COM, Mar. 24, 2009, http://www.eweek.com/c/a/Midmarket/Concentric-Offers-Secure-Messaging-for-SMBs-812940.

153 *See, e.g.*, John E. Dunn, *Worried Companies Block Facebook*, ABC NEWS, Aug. 21, 2007, http://abcnews.go.com/Technology/PCWorld/story?id=3505273; Shawn Young, *Security Fears Prod Many Firms to Limit Staff Use of Web Services*, WALL ST. J., Mar. 30, 2006, at A1 (mentioning General Electric Co. and J.P. Morgan Chase Co. as companies that have banned instant messaging in the workplace).

154 *See Global Internet Freedom: Corporate Responsibility and the Rule of Law: Hearing Before the Subcomm. on Human Rights and the Law of the Comm. on the Judiciary*, 110th Cong. 12-15 (2008) (statement of Mark Chandler, Senior Vice President, Cisco Sys., Inc.).

155 *See* Andrea M. Matwyshyn, *Of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction through Data Privacy*, 98 NW. U. L. REV. 493, 499 (2004) (discussing trends in the Internet economy).

156 *See* Daniel W. Park, *Trade Secrets, the First Amendment, and Patent Law: A Collision on the Information Superhighway*, 10 STAN. J.L. BUS. & FIN. 46, 47 (2004).

157 Parts of this subpart are adapted from Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet through Sequential Preservation*, 42 WAKE FOREST L. REV. 1, 3-5 (2007) [hereinafter Rowe, *Saving Trade Secret Disclosures*].

158 *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., No. C-95-20091 RMW, 1997 WL 34605244, at *12 (N.D. Cal. Jan. 6, 1997); Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1368 (E.D. Va. 1995); DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 192-93 (Ct. App. 2004). *But see id.* at 190 (finding that the mere posting of information on the Internet does not destroy a trade secret).

ing[159] trade secret information may not have intended to cause harm to the trade secret owner, the nature of the Internet is such that the secret could nonetheless be destroyed.[160]

Unlike other mass media, the Internet has no editors who scrutinize submissions and decide what materials will be published. Any person sitting at a computer can post proprietary information onto the Internet, resulting in immediate and irreparable harm. One judge captured the problem in these words:

> The court is troubled by the notion that any Internet user . . . can destroy valuable intellectual property rights by posting them over the Internet, especially given the fact that there is little opportunity to screen postings before they are made. Nonetheless, one of the Internet's virtues, that it gives even the poorest individuals the power to publish to millions of readers can also be a detriment to the value of intellectual property rights. The anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation.[161]

The nature of the Internet is such that the trade secret owner may never know the identity of the person making the disclosure. Furthermore, the person posting the information may very well be far removed from the person who originally misappropriated the secret, making it difficult to even identify potential defendants in misappropriation actions involving disclosures on the Internet.

Because the value of a trade secret lies in its secrecy, most misappropriators who acquire another's trade secrets and plan to use them for their own competitive advantage have no incentive to publicize the secret.[162] The culture of the Internet, however, has led to a higher likelihood that those in possession of another's trade secrets will make them public, rather than continuing to keep them secret for personal gain. The great ease with which virtually anyone can post information on the Internet, coupled with its "dis-

---

159 Posting "consists of directly placing material on or in a Web site, bulletin board, discussion group, newsgroup, or similar Internet site or 'forum,' where it will appear automatically and more or less immediately to be seen by anyone with access to that forum." O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 91 (Ct. App. 2006). Therefore, posting allows direct self-publication of information, or one may also send information to a site, the owners or moderators of which make decisions about what to post. *See id.*

160 *See, e.g.*, Jerome Stevens Pharms., Inc. v. FDA, 402 F.3d 1249, 1250, 1254 (D.C. Cir. 2005) (reversing district court dismissal, holding that the Food and Drug Administration could be liable for misappropriation of trade secrets where it posted plaintiff's trade secrets on its Web site for five months, and remanding).

161 Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., 923 F. Supp. 1231, 1256 (N.D. Cal. 1995) (citations omitted).

162 *See, e.g.*, *DVD Copy Control*, 10 Cal. Rptr. 3d at 195 (noting that a defendant in a trade secret case typically "has as much interest as the plaintiff has in keeping the secret away from good faith competitors and out of the public domain").

inhibiting effect,"[163] and a general decline in employee loyalty in the workplace,[164] have allowed disgruntled employees to achieve the ultimate revenge against their former employers by destroying trade secrets.

One court articulated this phenomenon in the following words: "With the Internet, significant leverage is gained by the gadfly, who has no editor looking over his shoulder and no professional ethics to constrain him. Technology blurs the traditional identities of David and Goliath."[165] Accordingly, Internet disclosures are likely to become a greater problem than they have been in the past, and the few cases highlighted below illustrate that a trade secret owner generally has no satisfactory recourse when trade secrets are published on the Internet.[166]

In *Religious Technology Center v. Lerma*,[167] a disgruntled former member of the Church of Scientology published documents taken from a court record on the Internet.[168] The Church[169] considered these documents to be trade secrets and sued the former employee, Lerma, to enjoin him from disseminating the alleged trade secrets.[170] The court refused to issue the injunction, though, because by the time the Church sought the injunction, the documents no longer qualified as trade secrets.[171] The court explicitly stated that "[o]nce a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve."[172]

In another Scientology case, the Church sought an injunction against another disgruntled former member who posted Church writings on several Internet newsgroups.[173] Despite being "troubled by the notion that any Internet user . . . can destroy valuable intellectual property rights by posting them over the Internet," the court held that since the writings were posted

---

163 Lyrissa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 NOTRE DAME L. REV. 1537, 1575 (2007) (discussing the phenomenon whereby users of the Internet are less inhibited when expressing themselves).

164 *See generally* Katherine V.W. Stone, *The New Psychological Contract: Implications of the Changing Workplace for Labor and Employment Law*, 48 UCLA L. REV. 519, 540, 542 (2001); Benjamin Aaron & Matthew Finkin, *The Law of Employee Loyalty in the United States*, 20 COMP. LAB. L. & POL'Y J. 321, 339 (1999).

165 Ford Motor Co. v. Lane, 67 F. Supp. 2d. 745, 753 (E.D. Mich. 1999).

166 For a more detailed discussion of the legal significance of the effect of trade secrets appearing on the Internet, see Rowe, *Saving Trade Secret Disclosures*, *supra* note 159; Elizabeth A. Rowe, *Introducing a Takedown for Trade Secrets on the Internet*, 2007 WIS. L. REV. 1041 [hereinafter Rowe, *Introducing a Takedown for Trade Secrets*].

167 Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362 (E.D. Va. 1995).

168 *Id.* at 1364.

169 The Religious Technology Center is a nonprofit corporation formed by the Church of Scientology to protect its religious course materials. Religious Tech. Ctr. v. Netcom On-Line Commc'n Serv., Inc., 923 F. Supp. 1231, 1239 (N.D. Cal. 1995).

170 *Lerma*, 908 F. Supp. at 1364.

171 *Id.* at 1368.

172 *Id.*

173 *Netcom*, 923 F. Supp. at 1239.

on the Internet, they were generally available to the public and therefore there were no trade secret rights available to support an injunction.[174]

In *Ford Motor Co. v. Lane*,[175] the defendant, Lane, operated a Web site that contained news about Ford and its products.[176] Lane published some documents on his Web site relating to the quality of Ford's products.[177] He did so despite knowing that the documents were confidential.[178] Ford sought a restraining order to prevent publication of the documents, claiming that the documents were trade secrets.[179] Ultimately, however, Lane's First Amendment defense prevailed, with the court reasoning that an injunction to prevent Lane from publishing trade secrets would be an unconstitutional prior restraint on speech.[180]

The advent of blogging[181] also poses risks, as employees and others discuss a myriad of company-related issues in public online, not all of which may be suitable for disclosure. Even though some employees have been fired for blogging about work, business blogs are on the rise.[182] Two new blogs are created every second,[183] and an estimated 89 percent of corporations are either blogging now or intend to set up blogs in the future.[184] Some blogs may even focus on breaking stories about their competitors, as for instance, when a blog sponsored by Miller Brewing Co. revealed that competitor Anheuser-Busch was preparing a new kind of brew.[185] Accordingly, individuals or companies could be liable for trade secret misappropriation actions when their blogging allegedly reveals others' trade secrets. In one case, for example, Apple Inc. sued and settled with a Web site for publishing trade secrets and allegedly soliciting Apple employees to reveal secrets about a new miniature Apple computer.[186] The blogging culture,

---

174 *Id.* at 1256-57.

175 67 F. Supp. 2d 745 (E.D. Mich. 1999).

176 *Id.* at 747.

177 *Id.*

178 *Id.* at 748.

179 *Id.*

180 *Id.* at 750, 753. For an overview of First Amendment issues presented by trade secret disclosures on the Internet see Rowe, *Introducing a Takedown for Trade Secrets*, *supra* note 168, at 1071-74.

181 Blogs are Web sites that contain commentary or other entries written by one or multiple authors on a particular topic. *See* Michael J. DeMaria, *Blogs: Only Half-Baked*, NETWORK COMPUTING, Sept. 30, 2002, at 19.

182 *See generally* Matt Villano, *Blogging the Hand that Feeds You*, N.Y. TIMES, Sept. 27, 2006, at G5.

183 Steve Johnson, *I Blog, Therefore I Am; With 175,000 New Ones Created Every Day, Blogs About to Join the Mainstream*, CHI. TRIB., Oct. 24, 2006, at 1.

184 GUIDEWIRE GROUP, BLOGGING IN THE ENTERPRISE: A GUIDEWIRE GROUP MARKET CYCLE SURVEY 2 (2005), http://www.guidewiregroup.com/site/pdf/CorporateBloggingSurvey.pdf.

185 David Kesmodel, *For All You Do, Bud, This Blog's For You*, WALL ST. J., Apr. 24, 2008, at A1.

186 *See* Bray, *supra* note 5.

generally unrestricted by editors and gatekeepers, sets the stage for the easy dissemination of trade secret information, even if inadvertent.

3. Cellular Phones

Cellular ("cell") phones are another potential source for the dissemination of trade secrets. About 87 percent of those living in the United States today use a cell phone,[187] a dramatic increase from the 38 percent who used cell phones in December 2000.[188] Today's phones combine camera, e-mail, and Internet capability in one small device, and have become ubiquitous.[189] As a result, they can serve as a great tool for stealing and transmitting company secrets. These increased risks have led security-conscious organizations, and even countries, to ban or limit the use of cell phones. Saudi Arabia and North Korea have apparently banned the importation and sale of camera phones in an effort to protect government secrets.[190] The U.S. Air Force has also banned camera phones from all areas that contain classified information.[191] Companies like General Motors and Texas Instruments have instituted policies limiting the use of camera phones by visitors and employees on company premises.[192] Samsung Electronics, the former DaimlerChrysler, and BMW also prohibit camera phones at some manufacturing sites.[193] In addition to the risks that cell phones may be used to capture trade secrets, smart phones[194] (which have many of the same functions as a desk-

---

187 This is according to 2008 figures compiled by the International Association for the Wireless Telecommunications Industry. *See* CTIA—THE WIRELESS ASSOCIATION, WIRELESS QUICK FACTS, YEAR END FIGURES [hereinafter CTIA YEAR END FIGURES], http://ctia.org/advocacy/research/index.cfm/AID/10323 (last visited Aug. 17, 2008).

188 U.S. Census data noted that there were 158,722,000 cell phone subscribers in 2003, compared to more recent 2008 industry figures at 270,300,000. *Compare* U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES: 2008, 714, tbl. 1120 (2008), *available at* http://www.census.gov/prod/2007pubs/08statab/infocomm.pdf, *with* CTIA YEAR END FIGURES, *supra* note 187.

189 *See, e.g.*, Teresa M. McAleavy, *Camera Phones Pose Problems for Workplace Privacy and Security*, ST. LOUIS POST-DISPATCH, Aug. 30, 2004, at E01.

190 Jon Van, *Hear Me Now*, CHI. TRIB., Feb. 28, 2005, at CN1; *Saudis Ban Use of Cell-Phone Cameras*, FOXNEWS.COM, Sept. 30, 2004, http://www.foxnews.com/story/0,2933,134091,00.html; ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 347-49 (Ronald Deibert et al. eds., 2008).

191 Van, *supra* note 190, at CN1.

192 *Id.*

193 *See* McAleavy, *supra* note 189, at E01.

194 "A Smartphone combines the functions of a cellular phone and a handheld computer in a single device." Michael Juntao Yuan, *What Is a Smartphone*, O'REILLY NET, Aug. 23, 2005, http://www.oreillynet.com/pub/a/wireless/2005/08/23/whatissmartphone.html.

top computer) are also at risk of being infected with viruses and other malicious software.[195]

The widespread use of cell phones and the other technological tools discussed above suggest that trade secret owners need an infrastructure in place to protect their secrets—one that includes specific processes and technological measures. Conducting a risk analysis of potential threats to the company's trade secrets should be comprehensive, paying attention to people, processes, and technology. Reliance on technological measures alone will not be sufficient. At a minimum, companies should give careful deliberation to policies regarding remote access to company computer networks and systems, telecommuting, e-mail and Internet usage, and access rights to sensitive information.[196]

III. SHOULD REASONABLENESS BE REDEFINED IN LIGHT OF KNOWN TECHNOLOGICAL RISKS?

As the earlier discussion illustrates, the widespread use of technology in the workplace enhances the risks of trade secret misappropriation through electronic means.[197] This Article posits that these risks are foreseeable to a trade secret owner, and that a court in determining reasonableness should deem it relevant to consider what specific security precautions were utilized to protect a secret in light of those risks. Because this argument draws on contributory negligence principles, a brief summary of the essence of that defense is in order here. The contributory negligence defense in tort law bars a plaintiff from recovery when her own conduct in protecting herself falls below that of a reasonable person in like circumstances and that conduct was a substantial factor in causing her injury.[198] Thus, as applied here, where the trade secret plaintiff is in the best position to decide whether to risk being injured, or at least the extent of that risk based on the precautions it selects, it seems sensible to allocate the burden of that choice to the plaintiff.[199]

---

195 Joseph De Avila, *Do Hackers Pose a Threat to Smart Phones?*, WALL ST. J., May 27, 2008, at D1.

196 *See* Antony J. McShane & Sarah E. Smith, *Implement an Effective Trade Secret Protection Plan—Before It's Too Late*, INTELL. PROP. TODAY, July 2003, at 16.

197 *See supra* Part II.

198 *See generally* RESTATEMENT (SECOND) OF TORTS § 463. The comparative negligence defense is inconsistent with trade secret law principles and is also inapplicable here because it focuses more on damages than on liability. *See generally* PROSSER AND KEETON ON TORTS 470 (W. Page Keeton et al. eds., 5th ed. 1984). While it may be of some use in analyzing the defendant's conduct as part of the misappropriation question, it does not appear to have a role in the threshold question of whether reasonable efforts were employed, thus qualifying the information as a trade secret.

199 *See* ABRAHAM, supra note 1, at 165 (discussing conscious reasonable risk-taking).

This is consistent with existing trade secret law principles as even the modern codification of trade secret law in the *Restatement (Third) of Unfair Competition* provides that the "foreseeability of the conduct through which the secret was acquired" should be relevant to determining reasonableness.[200] Furthermore, trade secret law already provides (under the UTSA) that a putative trade secret owner cannot make out a claim for trade secret misappropriation unless it can show reasonable efforts to protect the secret.[201] That is because in most jurisdictions, the reasonable efforts requirement is part of the threshold question in determining whether the plaintiff owns a legally protectable trade secret.[202]

To be clear, this Article does not advocate changing the reasonable efforts requirement. Rather, because the requirement mandates consideration of what is reasonable under the circumstances, the argument is that the changing circumstances that have come about as a result of new technology require a reexamination of what security measures are reasonable. Reasonableness requires not necessarily a checklist of specific items, but a conscious, risk assessment approach that better anticipates and ultimately stems the inappropriate dissemination or disclosure of the secrets. This reflects both a normative and prescriptive observation about the appropriate direction for digital misappropriation cases. It is especially important given that the courts do not appear to be considering specific technical measures and processes in the reasonable efforts analysis, and because the case law is unsettled on this question.[203] Further, because trade secret law and the definition of trade secret itself (even more than the other areas of intellectual property) is based on "evolving concepts and ideas,"[204] a reexamination of what are reasonable measures to protect information based on current business norms is not only logical but is consistent with trade secret law.

To that end, this Article proposes guidelines for the reasonable efforts determination in digital misappropriation cases.[205] Courts should pay greater attention to the technical measures and processes that companies use to protect their trade secrets, rather than merely focusing on the traditional facilities-based measures. In light of the foreseeability of the greater dangers posed by technology, reasonableness requires evidence of a risk analysis and steps to address those risks. Trade secret owners must avoid ex post facto justifications and explanations for trade secret protection and instead show affirmative measures generated from conscious recognition and assessment of the need to protect putative trade secrets.

---

200 RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. c. (1995).

201 *See supra* notes 36-41.

202 *Id.*

203 *See supra* Part I.B.4.

204 United States v. Kai-Lo Hsu, 40 F. Supp. 2d 623, 630 (E.D. Pa. 1999).

205 *See infra* Part III.A.

A. *Introducing Greater Objectivity into the Analysis*

This Article recommends that courts reinforce a transparent, objective layer into the reasonable efforts analysis. As it currently stands, a trade secret owner impliedly makes a subjective judgment as to the reasonableness of its safety precautions in deciding which safety measures to implement, and which to reject. This determination probably entails, among other things, a cost-benefit analysis, where the owner weighs the costs of protection relative to the value of the secret.[206] However, it is the court that ultimately decides whether those steps were reasonable enough under the circumstances, thus injecting an objective standard that trumps the trade secret owner's subjective belief about the sufficiency of its security measures. When, however, courts merely defer to the trade secret owner's judgment without making an independent evaluation and subjecting it to scrutiny, the required objectivity is missing. Accordingly, the guidelines proposed below will help to ensure that the fact finders' objective analysis of reasonableness is more meaningful. The fact finder must determine whether additional measures were necessary to protect the putative trade secrets in light of the particular circumstances. On the surface, this bears some resemblance to the "reasonable expectation of privacy" analysis in criminal procedure,[207] where the reasonableness of the defendant's expectation of privacy must be one "that society is prepared to recognize as 'reasonable.'"[208]

As a matter of policy, a truly objective standard encourages trade secret holders who would likely under-protect to take more precautions, thus avoiding some of the problems that could be caused by the moral hazard phenomenon.[209] More specifically, without greater objective oversight, trade secret holders will likely under-protect because of the costs associated with additional measures and because they may have no incentive to take more than the minimum precautions sufficient to achieve trade secret status under a subjective standard. Thus, in this context, there would be no incentive to spend more on technological measures to protect the trade secret if, for in-

---

206 *See* Note, *Trade Secret Misappropriation*, *supra* note 55, at 473.

207 Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). While there may be parallels between the Fourth Amendment's reasonable expectation of privacy standard and trade secrecy's reasonable efforts requirement, ultimately I do not think it appropriate to adopt these Fourth Amendment principles in wholesale fashion into the reasonable efforts analysis. *See* Note, *Trade Secret Misappropriation*, *supra* note 55, at 465-72 (explaining the shortcomings in applying the Fourth Amendment analogy to trade secret law).

208 *Katz*, 389 U.S. at 361 (Harlan, J., concurring). It is worth noting that in direct parallel to the reasonable efforts requirement discussed in this Article, failure to take steps to protect one's privacy in the Fourth Amendment context may mean that one does not receive Fourth Amendment protection. *See generally* Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 392 (1997).

209 *See generally* Gary T. Schwartz, *The Ethics and the Economics of Tort Liability Insurance*, 75 CORNELL L. REV. 313, 338 (1990) (discussing moral hazard in the context of tort liability insurance).

stance, the reasonable efforts standard merely requires traditional facilities-based measures to secure trade secret rights. With a more meaningful objective standard, however, a trade secret holder must aim for optimal protection to not only reduce the risk of loss through misappropriation, but also to ensure that a court will find that it acted in a reasonably prudent manner under the circumstances.

Thus, in determining reasonableness, the court ought to not only review evidence of the cost-benefit analysis that the plaintiff trade secret owner might have considered, but also the nature of the risks involved, with special consideration to the known technological risks that may or may not have been considered by the trade secret owner. Factors that could aid in that determination include: (1) the nature of the industry, (2) the nature of the trade secrets and how they were stored, (3) the nature of the measures taken to protect the secrets, and (4) the known risks from storage and protection choices. While some of these are interrelated, the benefit of having each considered separately is that it allows a more comprehensive, methodical, and consistent analysis of the reasonable efforts requirement in each case, something that is currently lacking in the case law. A discussion of each of these factors follows below.

1. Nature of the Business and the Industry

The nature of a plaintiff's business, including its size (both in terms of personnel and financial strength), the type of services or products offered by the business, the manner in which the business operates, and the related question of the nature of the trade secrets are all relevant considerations. In highly competitive industries, or industries that rely heavily on technology to not only generate but store trade secret information, greater efforts ought to be required to meet the reasonableness requirement.[210] That is because the "circumstances" would suggest that these trade secrets are particularly vulnerable. It is noteworthy, for instance, that a majority of the victims in cases that have been prosecuted under the EEA for trade secret theft are technology companies in computing and engineering related fields.[211] Moreover, among the data at highest risk of theft are research and development data, customer lists, financial data, and strategic plans and roadmaps.[212] The size and nature of a plaintiff's business, along with cost of

---

210 *See* Scott M. Alter, *Mixing Trade Secrets and LANs: Are We Looking for Trouble?*, 28 COMM. NEWS (U.K.), June 1991, at 23.

211 Since 2003, ten out of thirteen prosecutions under the EEA involved theft of trade secrets from high technology companies. *See* Dep't of Justice, Intellectual Property Cases, http://www.usdoj.gov/criminal/cybercrime/ipcases.html#eea (last visited Aug. 24, 2009).

212 Bradford K. Newman, *Protecting Trade Secrets: Dealing with the Brave New World of Employee Mobility*, BUS. L. TODAY, Nov. 2007, *available at* http://www.abanet.org/buslaw/blt/2007-11-12/newman.shtml.

measures and the degree to which those measures could reduce the risk of disclosure, are important in determining whether the plaintiff's choices were reasonably prudent.[213]

2. Nature of the Trade Secrets and How They Were Stored

Trade secrets vary tremendously and can be virtually any kind of business information.[214] Accordingly, there can be no one-size-fits-all approach to protecting the information. Rather, storage and protection measures must be carefully tailored to fit the particular situation. Thus, it may make a difference to the misappropriation analysis whether the purported trade secret consists of technical specifications and source code or formula, in which case perhaps only limited access should be granted to a select group of employees on a need-to-know basis, versus a customer list which might need to be more widely accessible to employees with lower level access rights. As this Article makes clear, trade secrets that are stored on a computer must be given special protection, and attention must be paid to the accessibility and portability of that kind of information.[215]

In today's business environment, it is likely that at least some, if not all, trade secrets are stored electronically.[216] As such, the traditional facilities-based measures may be insufficient to protect sensitive information. Sometimes, however, the very persons trusted with keeping information secure can betray the trade secret owner.[217] For instance, as discussed *supra*, in *Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A.*,[218] a member of the Information Technology Department with responsibility for network security and with total access to the system information and files, inappropriately printed and diverted information for the benefit of the defendant company.[219] In a case such as this, there was practically no way to avoid the misappropriation, unless perhaps there were checks in place to protect against rogue information technology staffers. While this may certainly be advisable, a court may not, in the context of other precautions taken by the company and in light of industry custom, consider the failure

---

213 *In re* Innovative Constr. Sys., Inc., 793 F.2d 875, 884 (7th Cir. 1986).

214 *See* UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2005); RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

215 *See* Maxine S. Lans, *Can You Keep the Lid on your Trade Secrets?*, MARKETING NEWS, Aug. 29, 1994, at 9 (discussing practical suggestions to protect trade secrets, including computer related trade secrets).

216 *See* R. Mark Halligan, *Duty to Identify, Protect Trade Secrets has Arisen*, NAT'L L.J., Aug. 29, 2005 (noting that "[t]rade secret assets often are created and stored electronically").

217 *See supra* Part I.B.5.

218 267 F. Supp. 2d 1268 (S.D. Fla. 2003), *aff'd in part, rev'd in part sub nom.* Four Seasons Hotels v. Consorcio Barr S.A., 138 F. App'x 297 (11th Cir. 2005).

219 *Id.* at 1283, 1290.

to fully protect against internal network security personnel unreasonable. That is because the absence of such additional measures, consistent with contributory negligence principles,[220] may not have been a substantial factor in causing the misappropriation. Moreover, as stated earlier, the standard is not one of absolute secrecy, but relative secrecy under the circumstances.[221]

3. Nature of the Measures Taken to Protect the Secrets

While the reasonableness of security precautions requires a contextual analysis based on the particular circumstances of the trade secret owner's business, this factor evaluates the kinds of measures (beyond confidentiality agreements and passwords) that were utilized to address the disclosure risks from computer technology.[222] Effective protection of trade secret information in this digital era requires both legal and technical approaches.[223] The goal is not perfect security, since absolute security of the information would make its beneficial use impracticable, if not impossible. Thus, "perfect security is not optimum security."[224] Rather, the trade secret owner needs to have an infrastructure in place to protect its secrets—one that includes specific processes and technological measures, in addition to the traditional facilities-based security precautions.

Agreements that go beyond a general confidentiality agreement and provide employees with specific notice or instructions on the use of technology in and related to the workplace can be helpful.[225] At a minimum, companies should give careful deliberation to policies regarding remote access to company computer networks and systems, telecommuting, e-mail and Internet usage, and access rights to sensitive information.[226] Some companies may even choose to ban camera-phones or other recording devices where such devices could easily expose certain secrets.[227]

Among the available options, a trade secret owner must select those measures that are the best fit given the preceding factors (i.e., the nature of

---

220 *See* PROSSER AND KEETON ON TORTS, *supra* note 198, at 456.

221 *See supra* text accompanying notes 60-62.

222 For an example of traditional (i.e., non-technological) preventive measures, see Randy Kay, *Guide to Trade Secret Protection—Maintaining Secrecy*, SAN DIEGO BUS. J., June 5, 2000, at 31.

223 *See generally* McShane & Smith, *supra* note 196, at 16 (outlining strategies for developing a trade secret protection program); Victoria A. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, 49 IDEA 359 (2009) (discussing practical steps to protect trade secrets in a digital environment).

224 Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991).

225 *See* Cundiff, *supra* note 223, at 370-71.

226 *See* McShane & Smith, *supra* note 196, at 16.

227 *See, e.g.*, Dan Gillmor, *Picture This*, CIO INSIGHT, Apr. 6, 2006, http://www.cioinsight.com/c/a/Past-Opinions/Picture-This (discussing Samsung Electronics' ban on camera phones inside its facilities).

its business, the industry, and the particular secrets at issue). In one case, a company required employees to sign a "Computer Security and Non-Disclosure Agreement," agreeing to maintain usernames and passwords in confidence.[228] Other companies provide each employee with an ID that has to be validated with a password, and that ID is tied to a specific level of access depending on the employee's role in the company.[229] Still, others add proprietary legends to their computer screens and mechanisms that lockout unauthorized users.[230]

Allowing employees to use sensitive company information, particularly where the information is transferred electronically and among various people without encrypting the information, represents weak protection.[231] Employers should be especially mindful of employees taking unencrypted information off site, such as on their laptops or to their offices at home.[232] The use of laptops generally should be carefully considered since it presents many risks for data loss, including the risk that the laptops themselves might be lost, stolen by a third party, or even sold to competitors.[233]

4. Known Risks from Protection Choices

As with information security generally,[234] trade secret owners should conduct risk assessments to assure that an effective strategy or infrastructure is in place to protect allegedly valuable trade secrets. Conducting a risk analysis of potential threats to the company's trade secrets should be comprehensive, paying attention to people, processes, and technology. However, reliance on technological measures alone will not be sufficient; one major limitation is that such measures tend to be more reactive than proactive.[235] For instance, the mere use of a password in itself may prove too

---

228 Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1327 (N.D. Ga. 2007). The policy, however, did not restrict employees from transferring information to their personal computers, and a departing employee did just that. *Id.* at 1329.

229 *See, e.g.*, Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1287 (S.D. Fla. 2003), *aff'd in part, rev'd in part sub nom.* Four Seasons Hotels v. Consorcio Barr S.A., 138 F. App'x 297 (11th Cir. 2005).

230 *See* Picker Int'l Corp. v. Imaging Equip. Servs., Inc., 931 F. Supp. 18, 29 (D. Mass. 1995), *aff'd sub nom.* Picker Int'l, Inc. v. Leavitt, 94 F.3d 640 (1st Cir. 1996).

231 Jordan Wiens, *Take a Stand Against Data Loss*, INFORMATIONWEEK, Nov. 19, 2007, at S1.

232 *Id.*

233 *See supra* text accompanying notes 124-26; *see also* Press Release, Dep't of Justice, Chicago, Illinois Man Pleads Guilty to Theft of Trade Secrets, Offered to Sell Online Interpreter's Information (Apr. 11, 2003), *available at* http://www.usdoj.gov/criminal/cybercrime/sunPlea.htm (describing a case where an employee sold a laptop containing stolen trade secrets to a competitor for three million dollars).

234 *See infra* Part IV.

235 *See* CIO, GLOBAL STATE OF INFORMATION SECURITY (2007), http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwc_giss2007.pdf [hereinafter GLOBAL STATE OF INFORMATION

risky. Many employees choose passwords that are too simple, which can be easily decrypted using free software.[236] Recall, for instance, that the passwords were cracked in the *Four Seasons*[237] case, allowing access to sensitive data.[238]

In general, a decision to implement certain security measures, done in a rational manner, suggests that certain additional measures were considered and rejected. Often it might be the case that the costs of additional measures relative to their perceived benefits were prohibitive,[239] or that some measures would be too disruptive to the company's productivity.[240] The court should consider the degree to which additional measures might have decreased the risk of disclosure in light of the known risks posed by the measures that were utilized.[241] To some extent, this will help create an upper limit of sorts such that in some circumstances additional, more costly measures will not be necessary for reasonableness, even though they may have countered the techniques used by the misappropriator. After all, it bears repeating that the standard is not one of absolute secrecy, but of relative secrecy, taking steps that are reasonably necessary under the circumstances to maintain secrecy.[242] As the *Restatement (Third) of Unfair Competition* advises, a trade secret owner should consider the risk of the type of conduct that may lead to loss, weighed against the cost and effectiveness of preventive measures, and viewed in context of the information's value.[243]

SECURITY] (noting that information security has been too skewed toward technology rather than proactive intelligence gathering and risk analysis); *see also* Scott Berinato, *The Fifth Annual Global State of Information Security*, CIO MAG., Aug. 28, 2007, *available at* http://www.cio.com/article/133600/The_Fifth_Annual_Global_State_of_Information_Security (summarizing the study's findings and conclusions).

236 *See* Ben Worthen, *Hacker Camps Train Network Defenders*, WALL ST. J., Apr. 1, 2008, at B6 (noting that "the best way to mitigate password risk is to put in additional authentication systems, such as biometric readers that scan fingerprints, or smartcards that workers have to swipe before they're granted access to a system").

237 Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268 (S.D. Fla. 2003), *aff'd in part, rev'd in part sub nom.* Four Seasons Hotels v. Consorcio Barr S.A., 138 F. App'x 297 (11th Cir. 2005).

238 *See supra* text accompanying note 92.

239 *See* Cundiff, *supra* note 223, at 363.

240 *See id.*

241 This is not to suggest that the court should conduct its own cost-benefit analysis, but that it should scrutinize the evidence in light of the guidelines proposed here to determine whether, overall, the decisions made by the plaintiff regarding technical precautions appear reasonable under the particular circumstances.

242 *See supra* Part II.B.1.

243 RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. c (1995).

B. *Defendant's Conduct as a Secondary Consideration*

The defendant's conduct in obtaining the trade secret information is not a proposed factor in the reasonable efforts determination mainly because under the UTSA and the *Restatement of Torts* the defendant's conduct is relevant to the misappropriation issue, not the threshold issue of whether the information qualifies as a trade secret.[244] Furthermore, consistent with the contributory negligence framework here, the plaintiff's conduct is only relevant as compared to the reasonable person. Thus, the basic outline of the approach compares what the plaintiff did to what it could have done to protect its proprietary information.

While the defendant's utilization of improper means to access or disclose the trade secret could be relevant in assessing the strength of protective measures taken by the trade secret owner to protect the secret, it muddies the analysis to give it too much weight and is perhaps best considered in the context of the factors described above. For instance, depending on the facts of the particular case, in considering the nature of measures taken to protect the secret and the known risks from protection choices (factors three and four), evidence of the defendant's conduct in accessing, using, or disclosing the alleged trade secret could be relevant to the overall evaluation of what additional measures the plaintiff could have used. Also, where a plaintiff makes a strong showing of reasonable efforts to protect trade secret information, a court is more likely to infer that the defendant used improper means to obtain the information.[245]

By way of illustration, assume a trade secret owner decides to protect sensitive data stored on a company network by requiring that only high-level employees sign general confidentiality agreements and not requiring special passwords to access the data. If a low-level employee who did not sign the confidentiality agreement, but who had access to the trade secret on the computer, e-mails it to a competitor, based on the framework presented in this Article, a court could find such efforts to be unreasonable and that the data does not deserve trade secret protection. In coming to this conclusion on reasonableness, the court would have considered the defendant's conduct in the context of making the judgment that, given the known risks to electronically-stored data, the trade secret owner should have taken additional steps to protect its secrets, such as requiring passwords keyed to vari-

---

244 The misappropriation inquiry focuses on whether the defendant employed improper means to acquire the trade secret. *See* UNIF. TRADE SECRETS ACT § 1 (amended 1985), 14 U.L.A. 537 (2005); RESTATEMENT (FIRST) OF TORTS § 757 cmt. a (1939).

245 Grubbs, *supra* note 66, at 427; *see also* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179 (7th Cir. 1991) ("The greater the precautions that [plaintiff] took to maintain the secrecy of the piece part drawings, the lower the probability that [defendant] obtained them properly and the higher the probability that it obtained them through a wrongful act . . . .").

ous levels of access, encrypting the data, and requiring that all employees sign confidentiality agreements.

It is interesting that the *Restatement (Third) of Unfair Competition*, which includes the reasonable efforts requirement as part of the misappropriation analysis, calls for an evaluation of "the extent to which the acquisition was facilitated by the trade secret owner's failure to take reasonable precautions against discovery of the secret by the means in question."[246] It further suggests that the "foreseeability of the conduct through which the secret was acquired" should be relevant to determining reasonableness.[247] Thus, under that framework, the foreseeability of the defendant's conduct plays a role in the ultimate determination of whether actionable misappropriation occurred.

IV. SOME PRACTICAL LESSONS FROM DATA SECURITY

The challenge of protecting trade secrets should be reviewed as part of the larger issue of data security generally, where preventing the loss of sensitive data is of critical importance. "The basic tasks of identifying sensitive data, monitoring where it goes, auditing who has access to it, and restricting that access" are common to both data loss prevention and the protection of trade secrets.[248] Accordingly, lessons from the data security field can be instructive, and a recent report on data security, discussed below, may provide some insights that could be helpful to trade secret protection. These insights have also informed some of the arguments made in this Article, particularly the view that reasonableness requires a conscious, risk assessment approach that better anticipates and ultimately stems the inappropriate dissemination or disclosure of the secrets.

CIO Magazine, *CSO Magazine*, and PricewaterhouseCoopers recently conducted a worldwide survey titled *The Global State of Information Security*.[249] The report produced from the survey reveals several interesting points that are relevant to the discussion about the larger issues surrounding trade secret protection and technology. First, a majority of the companies surveyed conduct enterprise risk assessments of their security strategy.[250] This suggests that all companies ought to include trade secrets as part of their security risk assessments. Trade secrets are a subset of the sensitive commercial data that must be protected, in addition to the private consumer information, and thus should not be left out of risk assessments. Too often, companies do not proactively track, monitor, and protect their trade secrets

246 RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. c (1995).

247 *Id.*

248 Wiens, *supra* note 231, at S1.

249 *See* CIO, GLOBAL STATE OF INFORMATION SECURITY, *supra* note 235.

250 *Id.* at 3.

until there has been a misappropriation incident, and at that point it may be too late.

Second, the use of technological tools such as firewalls,[251] user monitoring, and encryption are now more widely used to protect data.[252] Having these tools already in place and available in the workplace means that they could be implemented in a program to secure trade secrets without too much difficulty. However, reliance on the tools alone is not optimal, as technological tools tend to be reactive and are not capable of the intelligence and risk assessments that could avoid inappropriate access to trade secrets in the first instance.[253] It is also important to consider the people and processes that may affect trade secret protection.

Indeed, the third point of interest from the survey is that the most likely culprit in a "security incident," by an almost two-to-one margin, is not a hacker, but an employee.[254] This finding provides strong support for this Article's premise that reasonable efforts to protect trade secrets requires a comprehensive approach that takes into consideration a trade secret owner's measures to protect its secrets against outside threats, as well as the often overlooked inside threats from employees. This insight also bolsters the contention that the use of traditional security measures, which are generally facilities-based approaches, are insufficient. It makes little sense to build taller fences when the most likely thieves are already inside.

Finally, the report notes an interesting trend in how companies have come to view information security over the last few years: there has been a shift from ignorance of serious flaws in computer security to awareness of those flaws, but the final stage of using the awareness to fix the flaws has not yet been achieved.[255] To the extent that trends in trade secret protection may be similar to those in information security, knowledge about the importance of trade secret protection probably lags behind information security. As such, the level of knowledge for trade secrets might best be classified in the phase of "ignorance moving towards awareness." Indeed, part of the impetus for this Article is the hope that it will increase awareness of the enhanced risks that technology poses to trade secrets, and that a more stringent application of the reasonable efforts standard by the courts will eventually, in conjunction with other measures, compel trade secret owners to fix the flaws that currently exist in their trade secret protection strategies.

---

251 A firewall protects a computer from unauthorized use or intrusion on a network. Brad Gilmer, *Broadcast Security*, BROADCAST ENGINEERING (Overland Park), June 1, 2008, at 32.

252 *See* GLOBAL STATE OF INFORMATION SECURITY, *supra* note 235, at 3. The large increase in the use of encryption was noteworthy, with 72 percent reporting using some form of encryption compared to 48 percent the previous year.

253 *See id.* at 5.

254 *Id.* at 4.

255 *Id.*

CONCLUSION

What might have been a "reasonable" precaution ten years ago to protect a trade secret is not necessarily reasonable today in light of the changed circumstances created by technology. These changes increase the risk of trade secret misappropriation, and trade secret owners must be mindful to have adequate security measures, both technical and process-based, to deal with these enhanced risks. The approach presented in this Article, while guided by and grounded in a framework of contributory negligence doctrine, addresses the problem from two angles. First, it aims to guide, in a more consistent fashion through the use of objective guidelines, the way in which courts analyze reasonableness in cases where electronically-stored trade secrets are misappropriated. Second, this Article aims to encourage greater awareness and vigilance by trade secret owners before the misappropriation occurs. Trade secret protection cannot be an afterthought. Rather, in order to be reasonable, trade secret protection requires a more conscious, risk assessment approach that better anticipates and ultimately stems the inappropriate dissemination or disclosure of the secrets.