Corporate Cybersecurity Realism: Managing Trade Secrets in a World Where Breaches Occur

John Villasenor*
August 2015

I. INTRODUCTION

It would be an understatement to call trade secret cybersecurity a complex challenge. Trade secrets stored on company networks are ripe targets for cyber-intruders who have continuing access to new vulnerabilities via a robust global market for zero day exploits.[1] When a company has hundreds or thousands of laptop computers; servers; tablets; and smartphones; all of the associated software; and employees with varying degrees of security awareness, how can it assure the security of economically valuable confidential information? The answer, unsurprisingly, is that it cannot.

* John Villasenor is a professor of electrical engineering, public policy, and management at UCLA, a nonresident senior fellow at the Brookings Institution, and a National Fellow at the Hoover Institution at Stanford University

Suggested citation: John Villasenor, "Corporate Cybersecurity Realism: Managing Trade Secrets in a World Where Breaches Occur," *American Intellectual Property Law Association Quarterly Journal*, Volume 43, Numbers 2/3, Spring/Summer 2015.

---

1 The term "zero-day" refers to a security vulnerability that is not yet known in the cybersecurity community, and that can therefore be exploited by cyberattackers to circumvent existing defensive measures. LILLIAN ABLON ET AL., RAND CORPORATION, MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA 25 (2014), *available at* http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

As a result, the "every company has been hacked" theme has become a popular refrain in discussions about cybersecurity. In 2011, Dimitri Alperovitch, a former McAfee employee who later founded the cybersecurity company, CrowdStrike, wrote, "I am convinced that every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly), with the great majority of the victims rarely discovering the intrusion or its impact."[2] In a speech at the 2012 RSA conference, then FBI Director Robert S. Mueller, III said, "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."[3]

So what should companies do? First, and most obviously, companies need to take all reasonable steps to minimize the ability of cyber-intruders to get into their systems and make off with their trade secrets. There is a multibillion-dollar industry of products and services available to help plug security holes, and many companies have made cybersecurity a top priority.[4]

But, there is no such thing as perfect cybersecurity. Sometimes, despite all efforts to the contrary, skilled attackers who are intent on obtaining trade secrets will find their way into company systems. This inevitability leads to a second aspect of the corporate cybersecurity challenge that is not generally appreciated: companies need to manage their intellectual property in light of the affirmative knowledge that their computer systems will sometimes be breached.

Of the four types of intellectual property ("IP")—patents, trademarks, copyrights, and trade secrets—trade secrets are typically the most vulnerable. In

---

2 DMITRI ALPEROVITCH, MCAFEE, REVEALED: OPERATION SHADY RAT 2 (2011), *available at* http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

3 Robert S. Mueller III, FBI Director, Speech at the RSA Cyber Security Conference (Mar. 1, 2012), *available at* https://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

4 The annual RSA conference is an opportunity for security software companies to share their products with attendees. For examples of some of these cybersecurity products and services from the April 2015 conference, see *Exhibitor List*, RSA CONFERENCE, http://www.rsaconference.com/events/us15/expo-sponsors/exhibitor-list (last visited May 25, 2015).

large part this is because, unlike the other three types of IP, trade secrets derive value through the very lack of disclosure that helps define them.[5] And for this very same reason, they are particularly attractive targets for cyberintruders.[6]

Trade secrets are also different from other forms of IP in that when they make the news, it is often because a company knows or suspects that something has gone wrong. Trademarks are advertised, copyrighted works are marketed, and patents are featured in company press releases, product announcements, and on products themselves. By contrast, trade secrets are often described in news stories related to trade secret theft allegations, civil litigation, and criminal prosecutions.[7]

As a result, while there is plenty of information regarding how companies should respond to detected or suspected incidents of trade secret misappropriation, there is very little guidance on how to minimize the impact of the undetected incidents that probably constitute the vast majority of attacks. To help fill that gap, this article proposes a set of recommendations for handling trade secrets in a world where legal protections against misappropriation are weak in many jurisdictions and cybersecurity everywhere is imperfect at best. To properly frame those recommendations, this article begins with an explanation of trade secrets and an overview of the associated legal frameworks.

II. TRADE SECRETS: A PRIMER

A trade secret is information that derives actual or potential economic value from not being generally known, and that is subject to reasonable efforts to maintain its secrecy.[8] Formulas, computer programs, methods, techniques, and processes

---

5 *See infra* Part II.

6 *See infra* Part V.

7 *See, e.g.*, Chris Dolmetsch, *Goldman Code Theft Suspect Fights On*, BUSINESSREPORT (Apr. 7, 2015, 8:00 AM), http://www.iol.co.za/business/markets/currencies/goldman-code-theft-suspect-fights-on-1.1841277; Beth Winegarner, *Diablo Owes Netlist $6.5M for Chip Secret Theft, Jury Told*, LAW360 (Mar. 23, 2015, 7:05 PM), http://www.law360.com/articles/634744/diablo-owes-netlist-6-5m-for-chip-secret-theft-jury-told.

8 This definition is paraphrased from the definition in the Uniform Law Commission's Uniform Trade Secrets Act (UTSA), which in full reads as follows: "'Trade secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable

can all be trade secrets.[9] Perhaps the most famous trade secret is the Coca-Cola formula, which is reportedly held in a vault in Atlanta.[10] Other famous trade secrets include the Google search algorithm[11] and the recipe for Kentucky Fried Chicken.[12] The details of a manufacturing process can be a trade secret,[13] as can the breakdown of ingredients used by a perfume company to create a fragrance.[14]

Trade secrets are arguably the most foundational form of intellectual property. Undisclosed plans, designs, formulas, methods, processes, procedures, and computer code play a vital role in economic competitiveness, both for specific companies and, by extension, for entire countries.[15] Even patented inventions begin as trade secrets. When a company creates internal documents describing a new invention in anticipation of a possible patent filing, much of the information

---

by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." Unif. Trade Secrets Act § 1(4) (amended 1985), 14 U.L.A. 538 (Supp. 2010), *available at* http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

9 *Id*.

10 *See* Leon Stafford, *Coke Hides its Secret Formula in Plain Sight in World of Coca-Cola Move*, ATLANTA JOURNAL-CONSTITUTION (Dec. 8, 2011, 5:49 PM), http://www.ajc.com/news/business/coke-hides-its-secret-formula-in-plain-sight-in-wo/nQPMm/.

11 *See* Colleen Kane, *7 Sought-After Trade Secrets*, CNBC (Aug. 23, 2012, 10:18 AM), http://www.cnbc.com/id/48755451. Google's original page rank algorithm is patented. U.S. Patent No. 6,285,999 (filed Jan. 9, 1998). That patent, however, dates from the late 1990s, and Google's search algorithm today includes many features not reflected in that patent.

12 Kane, *supra* note 11.

13 *See* Hertz v. Luzenac Grp., 576 F.3d 1103, 1109 (10th Cir. 2009) (holding that the question of whether a manufacturing process is a trade secret should be considered in the aggregate).

14 *See, e.g.*, Gabriel M. Ramsey & Roland Chang, *Stop and Smell the Trade Secrets, Part II*, ORRICK TRADE SECRETS WATCH BLOG (Oct. 31, 2014), http://blogs.orrick.com/trade-secrets-watch/2014/10/31/stop-and-smell-the-trade-secrets-part-ii-two-major-companies-voluntarily-disclose-fragrance-ingredient-information/.

15 *See* Robert T. Neufeld, *Mission Impossible: New York Cannot Face the Future Without a Trade Secret Act*, 7 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 883, 926 (1997) ("[T]oday's sophisticated economy demands comprehensive trade secret protection.").

in those documents qualifies, at least temporarily, as a trade secret.[16] If a company elects not to file a patent application, the information can remain a trade secret.[17] If a patent application is filed, however, the information in the application could retain trade secret value until it is published, typically eighteen months later.[18]

Trade secrets also have a connection to copyright.[19] Although a published work is disclosed, the processes used by a movie or television studio, book publisher, or record label to foster the creation of copyrighted works and to decide when and under what conditions to bring them to market very often involve trade secrets. In addition, information about an unpublished copyrighted work (such as a movie or television show that has not yet been made or released) can also qualify as a trade secret. This was demonstrated in dramatic fashion in late 2014 when cyberattackers breached the systems of Sony Pictures Entertainment and leaked enormous amounts of data, including the "script for an unreleased pilot."[20]

Trade secrets differ from patents in important ways. Patents provide a time-limited, government-granted monopoly[21] with respect to an invention (though

---

16 *See* Philip L. Burke, *The 'Non-Informing Public Use' Concept and its Application to Patent-Trade Secret Conflicts*, 63 J. PAT. & TRADEMARK OFF. SOC'Y 459, 461–81 (1981) (explaining the relationship between trade secrets and patents).

17 See id.

18 In the absence of a non-publication request, patent applications are generally published by the PTO 18 months after the claimed priority date. 35 U.S.C. § 122(b)(1) (2012). After filing a patent application, a company may also elect to publish information in a patent application. *Id*. A company can publish this information before filing a patent application but doing so would generally eliminate the company's ability to file for patents in non-U.S. jurisdictions and would start a one-year clock ticking on the U.S. grace period for filing a U.S. patent application. *See* 35 U.S.C. §§ 102 and 103 (2013).

19 See Eduardo Gomez, "Pure Speech or Expressive Conduct?": The "Decss Saga" and the Inconsistent Treatment of Computer Code Under the First Amendment, 31 AIPLA Q.J. 231, 255 (2003) (explaining the distinctions between copyright and trade secret).

20 Tom Gar & Charlie Warzel, *A Look Through The Sony Pictures Data Hack: This Is As Bad As It Gets*, BUZZFEED (Dec. 2, 2014), http://www.buzzfeed.com/tomgara/sony-hack#.cfx73wzLOy.

21 Some object to the term "monopoly" in association with patents. The Supreme Court, however, has previously used such terminology. *See, e.g.*, Alice Corp. Pty. Ltd. v. CLS

not necessarily with respect to a market) in exchange for disclosure of the invention.[22] More specifically, a patent owner has the right to exclude others from making, using, selling, or importing the claimed invention in the relevant jurisdiction without the permission of the patent owner.[23] This right includes the ability to exclude those who might later[24] independently develop the same invention.

Trade secrets, by contrast, provide no power to exclude others who might later independently develop the same trade secret and use it to bring a competing product to market.[25] Patents generally expire 20 years after the filing date,[26] while trade secrets can be used for as long as their owner perceives them to have value and maintains their secrecy.[27]

Bank Int'l, 134 S. Ct. 2347, 2355 (2014) ("The latter pose no comparable risk of pre-emption, and therefore remain eligible for the monopoly granted under our patent laws.").

22 H.R. REP. NO. 112-98, pt. 1, at 52 (2011).

23 A patent owner has the "right to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States . . . ." 35 U.S.C. § 154(a)(1) (2012).

24 "Later" is important in this sentence because U.S. patent law contains a defense to infringement for prior commercial use. The prior commercial use provision applied to a very narrow set of patents starting in 1999, and to a much broader range of subject matter for patents issued on or after September 16, 2011. *See* David H. Hollander, *The First Inventor Defense: A Limited Prior User Right Finds Its Way into Us Patent Law*, 30 AIPLA Q.J. 37, 37 (2002).

25 *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 485 (1974) ("A trade secret law, however, does not offer protection against discovery by fair and honest means, such as by independent invention, accidental disclosure, or by so-called reverse engineering, that is by starting with the known product and working backward to divine the process which aided in its development or manufacture.").

26 35 U.S.C. § 154(a)(2) (2012). *See* MPEP § 2701 (9th ed. Original, Mar. 2014) for a more complete description of the rules for computing patent term.

27 *How are Trade Secrets Protected??*, WORLD INTELLECTUAL PROPERTY ORGANIZATION, http://www.wipo.int/sme/en/ip_business/trade_secrets/protection.htm (last visited May 24, 2015).

In addition, whereas patents protect inventions, trade secrets cover broader subject matter.[28] Some trade secrets cover inventions that, had the owner desired, could have been patented.[29] Trade secrets, however, can also protect information that is clearly patent-ineligible.[30] In 2013, for example, a federal district court in Ohio ruled that "confidential, proprietary information regarding business opportunities in the oil and gas development industry" could qualify as a trade secret.[31]

Also, patents are jurisdiction-specific and are issued in the United States by the U.S. Patent and Trademark Office ("PTO") following an examination process.[32] By contrast, trade secret status is automatic; there is no government entity that must first evaluate the information before it can qualify as a trade secret.[33] As long as the information meets the relevant statutory definition[34] it qualifies as a trade secret. And unlike trademarks, which can be examined and registered through the PTO, and copyrights, which can be registered through the U.S.

---

28 Andrew Beckerman-Rodau, *The Choice Between Patent Protection and Trade Secret Protection: A Legal and Business Decision*, 84 J. PAT. & TRADEMARK OFFICE SOC'Y 371, 379 (2002) ("In contrast to patent law, no specific categories exist for defining subject matter eligible for trade secret protection. . . . Almost anything that is maintained in secret, that is not generally known to competitors and which provides a competitive advantage is potentially protectable via trade secret.").

29 *Id*.

30 *Id*.

31 Wellington Res. Grp., LLC v. Beck Energy Corp., No. 2:12-CV-104, 2013 WL 5325911, at *5 (S.D. Ohio Sept. 20, 2013).

32 *General Information Concerning Patents*, USPTO (Oct. 2014), http://www.uspto.gov/patents-getting-started/general-information-concerning-patents#heading-1.

33 *How are Trade Secrets Protected??*, *supra* note 27.

34 As discussed herein, in the United States, with respect to civil litigation, the relevant statutory definition depends on the state. For trade secret theft under the federal economic espionage statute, the relevant statutory definition is provided in 18 U.S.C. § 1839(3) (2012). Internationally there are further variations in the definition of trade secret. *See* Karen A. Magri, International Aspects of Trade Secrets Law (1997) (unpublished manuscript), *available at* http://www.myersbigel.com/library-articles/international-aspects-of-trade-secrets-law-by-karen-a-magri/.

Copyright Office, there is no federal or state registry for trade secrets.[35] The government typically gets involved with trade secrets only in civil or criminal trade secret misappropriation trials, where courts are often asked to evaluate, among other things, a defendant's claim that the information at issue did not in fact qualify as a trade secret.[36]

III. AMERICAN TRADE SECRET LEGAL FRAMEWORKS

In the U.S., statutory protection for trade secrets is found in most states,[37] and in the case of economic espionage, at the federal level.[38] All but a few states have enacted civil trade secret statutes[39] based on the Uniform Law Commission's ("ULC") Uniform Trade Secrets Act ("UTSA"),[40] which was initially approved by the ULC in 1979 and revised in 1985.[41] Under the UTSA, a trade secret:

> [M]eans information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper

---

35 *How are Trade Secrets Protected??*, *supra* note 27.

36 *See, e.g.*, E.I. Dupont De Nemours & Co. v. Kolon Indus., 564 F. App'x 710 (4th Cir. 2014); United States v. Hanjuan Jin, 733 F.3d 718 (7th Cir. 2013); United States v. Agrawal, 726 F.3d 235 (2d Cir. 2013); United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012).

37 *Trade Secret Laws: State Law*, ORRICK TRADE SECRETS WATCH BLOG, http://blogs.orrick.com/trade-secrets-watch/trade-secrets-laws/ (last visited May 25, 2015).

38 *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489 (codified as amended at 18 U.S.C. §§ 1831–39 (2012)).

39 *See The Uniform Trade Secrets Act (UTSA)*, NDAS FOR FREE, http://www.ndasforfree.com/UTSA.html (last visited May 25, 2015). Some states have also enacted criminal trade secret statutes. *See, e.g.*, CAL. PENAL CODE § 499(c) (West 2015).

40 *See* Unif. Trade Secret Act (amended 1985), 14 U.L.A. 529 (2005), *available at* http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

41 *Legislative Fact Sheet – Trade Secrets Act*, UNIFORM LAW COMMISSION, http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act (last visited May 25, 2015).

means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[42]

Acquisition of a trade secret through improper means, or improper disclosure of a trade secret can constitute misappropriation.[43] Importantly, acquisition and disclosure are not necessarily linked. Someone who employs improper means (such as breaking into a computer system) to obtain a trade secret but who does not subsequently disclose it to anyone else is still committing misappropriation (and potentially other crimes as well).[44]

Notably, there is no current federal civil trade secret statute. Companies wishing to pursue a civil trade secret claim in the U.S. can face a complex landscape because many states have not yet adopted the language in the UTSA verbatim.[45] This disparity has led to differences among states in the scope of trade secret protection.[46] In addition, each state has a separate body of trade secret case law.[47]

---

42 Unif. Trade Secret Act § 1(4).

43 The full definition of "misappropriation" in the UTSA is: "(i) [A]cquisition 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; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who had utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake." *Id.* §1(2).

44 See id.

45 David S. Almeling, *A Practical Case For Federalizing Trade Secret Law*, LAW360 (June 16, 2009), http://www.law360.com/articles/106724 (providing examples of six states that vary in trade secret law).

46 *Id*.

47 Michael H. Bunis & Anita Spieth, *Common Law v. UTSA: The Last States Standing*, LAW360 (Apr. 2, 2012, 12:22 PM), http://www.law360.com/articles/321776/common-law-v-utsa-the-last-states-standing (observing "dissimilarities in the trade secret jurisprudence among different states . . . ").

There have been repeated attempts to introduce a federal civil trade secret statute, including in April 2014 when Senators Christopher Coons (D-DE) and Orrin Hatch (R-UT) introduced the Defend Trade Secrets Act of 2014 ("DTSA").[48]

Trade secrets are addressed in federal criminal statutes through the Economic Espionage Act ("EEA"),[49] which was enacted in 1996, and indirectly through the Computer Fraud and Abuse Act ("CFAA"),[50] which was enacted in 1986. The EEA addresses trade secret theft that would "benefit any foreign government," and more generally, for "the economic benefit of anyone other than the [trade secret] owner . . . ."[51] In 2012, the scope of the EEA was expanded to cover trade secret misappropriation "related to a product or service used in or intended for use in interstate or foreign commerce"[52] Prior to this change, the EEA covered trade secrets "included in a product that is produced for or placed in" commerce, which arguably excluded from protection trade secrets related to not-yet-released products, or used internally in a manner unrelated to products.[53] In 2013, the fines for trade secret theft under the EEA were increased.[54]

The CFAA makes it a crime to access a computer "without authorization or exceed[ing] authorized access" and to "thereby obtain[] . . . information from any protected computer."[55] The CFAA[56] also criminalizes accessing a "protected

---

48 Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014), *available at* https://beta.congress.gov/113/bills/s2267/BILLS-113s2267is.pdf.

49 *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489 (codified as amended at 18 U.S.C. §§ 1831–39 (2012)).

50 18 U.S.C. § 1030 (2012).

51 18 U.S.C. §§ 1831(a), 1832(a) (2012).

52 Prior to the Theft of Trade Secrets Clarification Act (TSCA), the EEA addressed theft of a trade secret "related to or included in a product that is produced for or placed in interstate or foreign commerce." 18 U.S.C. § 1832(a) (2006). Under the TTSCA, this was amended to "related to a product or service used in or intended for use in interstate or foreign commerce." Theft of Trade Secrets Clarification Act of 2012 (TTSCA), S. 3642, 112th Cong. (2d Sess. 2012) (amending 18 U.S.C. § 1832(a)). The new language is thus broader in several respects, as it removes "included in," "produced for," and "placed in" and instead uses "related to" and "used in or intended for use." *Id*.

53 18 U.S.C. § 1030 (2006).

54 Foreign and Economic Espionage Penalty Enhancement Act of 2012, H.R. 6029, 112th Cong. (amending 18 U.S.C. §§ 1831(a)-(b) (2012)).

55 18 U.S.C. § 1030(a)(2), (a)(2)(C) (2012).

computer without authorization, and as a result of such conduct, caus[ing] damage and loss."[57] Federal prosecutors pursuing cases involving alleged trade secret theft sometimes bring charges under both the EEA and the CFAA, or in some instances under the EEA alone.[58] Recently, the CFAA's applicability to trade secret cases has been called into question in light of developments in *United States v. Nosal*.[59]

When extraterritorial misappropriation of U.S. trade secrets is combined with importation, the U.S. International Trade Commission ("ITC") has an important role. The ITC conducts "Section 337"[60] investigations to, among other things, address "[u]nfair methods of competition and unfair acts in the importation of articles."[61] In a 2011 decision stemming from an appeal of an ITC determination, the United States Court of Appeals for the Federal Circuit considered "whether section 337 applies to imported goods produced through the exploitation of trade secrets in which the act of misappropriation occurs abroad."[62] The Federal Circuit held that section 337 did, in fact, apply even though misappropriation occurred

---

56 The CFAA has sometimes been criticized, not unreasonably, as being overly broad. *See, e.g.*, Mark Jaycox, *Increasing CFAA Penalties Won't Deter Foreign "Cybersecurity" Threats*, ELEC. FRONTIER FOUND. (Apr. 11, 2013), https://www.eff.org/deeplinks/2013/04/increasing-cfaa-penalties-wont-deter-foreign-cybersecurity-threats. Legislation that would have narrowed its scope was introduced in 2013 but not enacted. Cindy Cohn, *Aaron's Law Reintroduced: CFAA Didn't Fix Itself*, ELEC. FRONTIER FOUND. (Apr. 29, 2015), https://www.eff.org/deeplinks/2015/04/aarons-law-reintroduced-cfaa-didnt-fix-itself.

57 18 U.S.C. § 1030(a)(5)(C) (2012).

58 For example, in *United States v. Aleynikov*, the defendant was initially charged under both the EEA and the CFAA, though the CFAA charge was later dismissed by the court because the defendant was authorized to access his employer's source code while still an employee. 676 F.3d 71 (2d Cir. 2012). By contrast, in *United States v. Hanjuan Jin*, the defendant was charged under the EEA. 733 F.3d 718 (7th Cir. 2013).

59 676 F.3d 854 (9th Cir. 2012). In this decision, the Ninth Circuit wrote that the "general purpose [of the CFAA] is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets . . ." *Id*. at 863.

60 Named after Section 337 of the Tariff Act of 1930, now 19 U.S.C. § 1337 (2012).

61 19 U.S.C. § 1337(a)(1)(A) (2006).

62 TianRui Grp. Co. v. U.S. Int'l Trade Comm'n, 661 F.3d 1322, 1328 (Fed. Cir. 2011).

outside the United States, because the subsequent importation would lead to unfair competition.[63] This decision allowed the ITC to issue exclusion orders barring the importation of the products in question into the United States.[64]

IV. INTERNATIONAL TRADE SECRET LEGAL FRAMEWORKS

The international landscape with respect to trade secret laws is complex and evolving. The World Trade Organization's Trade-Related Aspects of Intellectual Property Rights ("TRIPS") Agreement states that to "ensur[e] effective protection against unfair competition . . . Members shall protect undisclosed information . . . ."[65] But, there are wide variations in the level to which member countries have implemented trade secret protections.

In late 2013, the European Commission released a draft directive "on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure."[66] If adopted, this would create a consistent civil trade secret law framework for European Union countries.[67] Trade secret protections are also among the intellectual property topics under discussion in the ongoing Trans-Pacific Partnership ("TPP")

---

63 *Id*. at 1324 ("We conclude that the [International Trade] Commission has authority to investigate and grant relief bed in part on extraterritorial conduct insofar as it is necessary to protect domestic industries from injuries arising out of unfair competition in the domestic marketplace.").

64 *Id.* at 1333.

65 Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C § 7 art. 39, 1869 U.N.T.S. 299 [hereinafter TRIPS Agreement].

66 Proposal for a Directive of the European Parliament and of the Council on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, European Commission (Nov. 28, 2013), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0813&from=EN.

67 *Id.* at 6 ("[C]onvergence of civil law remedies would allow innovative businesses to defend their rightful trade secrets more effectively across the EU.").

negotiations[68], as well as the more recent Transatlantic Trade and Investment Partnership ("T-TIP") negotiations.[69]

In addition, intellectual property protections and enforcement mechanisms, including with respect to trade secrets, are often on the agenda in American bilateral discussions with trading partners. For example, according to a fact sheet provided by the U.S. Department of Commerce, in December 2014, at the U.S.-China Joint Commission on Commerce and Trade ("JCCT") meeting, "[t]he United States and China agree[d] to exchange information on the scope of protection of trade secrets and confidential business information under their respective legal systems."[70]

A full review of international trade secret laws and developments is outside the scope of this article, however, there are many sources that address various aspects of this topic in much more detail. Examples include an April 2013 European Commission "Study on Trade Secrets and Confidential Business Information in the Internal Market,"[71] a November 2013 European Commission guide to trade secret laws in ASEAN (the Association of Southeast Asian Nations) countries,[72] an August 2013 Library of Congress report on "Protection of

---

68 David Levine, Trade Secrecy and the Trans-Pacific Partnership Agreement: Secret Lawmaking Meets Criminalization, INFOJUSTICE.ORG (Oct. 27, 2014), http://infojustice.org/archives/33502.

69 *See* Shayerah I. Akhtar & Vivian C. Jones, Cong. Research Serv., R43158, Proposed Transatlantic Trade and Investment Partnership (TTIP): In Brief 10 (June 11, 2014) ("[T]he T-TIP could lead to enhanced rules on trade secrets, an area of U.S. and EU concern in light of increased instances of trade secret theft internationally, including through cybercrime."); Shayerah I. Akhtar & Vivian C. Jones, Cong. Research Serv., R43387, Transatlantic Trade and Investment Partnership (TTIP) Negotiations 35–36 (Feb. 4, 2014).

70 U.S. DEPT. OF COMMERCE, U.S.-CHINA JOINT FACT SHEET ON 25TH JOINT COMMISSION ON COMMERCE AND TRADE (Dec. 29, 2014), *available at* http://www.commerce.gov/news/fact-sheets/2014/12/29/us-china-joint-fact-sheet-25th-joint-commission-commerce-and-trade.

71 EUROPEAN COMMISSION, STUDY ON TRADE SECRETS AND CONFIDENTIAL BUSINESS INFORMATION IN THE INTERNAL MARKET (Apr. 2013), *available at* http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf.

72 SOUTH-EAST ASIA IPR SME HELPDESK, GUIDE ON TRADE SECRETS, PROTECTING YOUR TRADE SECRETS IN SOUTHEAST ASIA (Nov. 2013), *available at*

Trade Secrets" in Brazil, China, India, the Russian Federation, and South Africa,[73] and the USTR's annual "Special 301 Report."[74]

V. CYBERSECURITY AND TRADE SECRET THEFT

There is good reason to believe that many trade secret misappropriation incidents are tied to cybersecurity breaches, although it is impossible to know how many[75] For starters, trade secrets are valuable and are, therefore, a prime target.[76] According to a 2010 Forrester Consulting paper, "[s]ecrets comprise two-thirds of the value of firms' information portfolios."[77] In 2012, then NSA Director General Keith B. Alexander wrote that the "ongoing cyber-thefts from the networks of public and private organizations, including Fortune 500 companies, represent the greatest transfer of wealth in human history."[78]

Merging information about vulnerabilities and incidents to place a specific value on economic losses due to cyber-enabled trade secret misappropriation is difficult. Among other challenges, reported incidents are not typically described in terms that enable valuation calculations.[79] In addition, although companies

---

http://www.asean-iprhelpdesk.eu/sites/default/files/publications/Trade-Secret-English.pdf.

73 THE LAW LIBRARY OF CONGRESS, PROTECTION OF TRADE SECRETS (Aug. 2013), *available at* http://www.loc.gov/law/help/tradesecrets/2013-009821_FINAL_2.pdf.

74 OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE, 2014 SPECIAL 301 REPORT (Apr. 2014), *available at* https://ustr.gov/sites/default/files/USTR%202014%20Special%20301%20Report%20to%20Congress%20FINAL.pdf.

75 Many breaches go undiscovered. Even when a breach is discovered it can be difficult to determine what specific information was accessed.

76 *See* FORRESTER CONSULTING, *The Value of Corporate Secrets: How Compliance and Collaboration affect Enterprise Perceptions of Risk* 2 (Mar. 2010), *available at* http://www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20Secrets.pdf/.

77 *Id.* The Forrester Consulting paper defined "secrets" as "trade secrets, confidential and other kinds of nonregulated but otherwise valuable data." *Id.* at 15.

78 Keith B. Alexander, *An Introduction by General Alexander*, 19 THE NEXT WAVE (2012), *available at* https://www.nsa.gov/research/tnw/tnw194/articles/pdfs/TNW194_article2.pdf.

79 Even when companies publicly disclose that they have discovered a breach, they often disclose no more information than is required by reporting laws

have reporting obligations when breaches expose their customers' personal data, they are not generally obligated to publicize intrusions that expose trade secret information unrelated to customer privacy.[80] More fundamentally, most intrusions probably go undetected.[81]

Despite these challenges, there have been some efforts to quantify losses attributable to cyber-related trade secret theft. One commentator for Symantec has written that IP theft (including but not limited to cyber-enabled theft) is "staggeringly costly to the global economy: U.S. businesses alone are losing upwards of $250 billion every year."[82] A May 2013 report from the Commission on the Theft of American Intellectual Property claimed that annual losses to the American economy due to international IP theft were likely over $300 billion.[83] Of course, reasonable people can differ regarding the accuracy of these assessments. It is beyond doubt, however, that the annual cost to American companies of trade secret theft generally, and of cyber-enabled trade secret theft specifically, is many billions of dollars.

Valuable trade secrets attract the attention of highly skilled attackers who have access to a continuing stream of new exploits. Citing data from the National

---

(for example, that require companies to disclose breaches that may expose customers to identity theft).

80 Defense Security Service, Executive Office of the President of the United States, *Foreign Spies Stealing US Economic Secrets in Cyberspace, in* ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS 41, 43 (Feb. 2013) ("No legal requirement to report a loss of sensitive information or a remote computer intrusion exists, and announcing a security breach of this kind could tarnish a company's reputation and endanger its relationships with investors, bankers, suppliers, customers, and other stakeholders."). An exception could occur in cases where a documented trade secret theft results in significant financial exposure for a public company, which could trigger reporting obligations to shareholders.

81 ALPEROVITCH, *supra* note 2, at 2 ("[T]he great majority of [cybersecurity] victims rarely discover[] the intrusion or its impact.").

82 Rich Dandliker, *Information Unleashed: Putting a Face on Intellectual Property Theft*, SYMANTEC (July 11, 2012), http://www.symantec.com/connect/blogs/putting-face-intellectual-property-theft.

83 THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY, THE IP COMMISSION REPORT 2 (May 2013), *available at* http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

Vulnerability Database,[84] Hewlett-Packard's ("HP") 2013 Cyber Risk Report noted that over 4700 new vulnerabilities were reported during the period from January 2013 through November 2013, and that this number was about six percent lower than the new vulnerabilities reported for the same period in 2012.[85] Stated another way, the number of *reported* new vulnerabilities averages well over ten per day; the number of *unreported* new vulnerabilities is clearly higher.[86] The HP report also cited approximately 250 vulnerabilities disclosed in 2013 through HP's Zero Day Initiative, which provides compensation to researchers who disclose verified vulnerabilities, and then coordinates the release of patches by the affected product vendor.[87]

In addition, cyberespionage attacks are notable both for their sophistication and their increasing frequency. The Verizon 2014 Data Breach Investigations Report[88] examined 511 cyber-espionage incidents in 2013, noting "consistent, significant growth of incidents in the dataset" and that cyberespionage "exhibits a wider variety of threat actions than any other pattern."[89]

It is also important to note that not all incidents of cyber-related trade secret misappropriation are due to external attacks.[90] An insider who attempts to access thousands of trade secret documents in the days before moving to a new job at a competing company is engaging in behavior that, at the very least, is highly suspicious. In a well-designed and well-managed corporate network, patterns of

---

84 *NVD Data Feed and Product Integration*, NATIONAL VULNERABILITY DATABASE, http://nvd.nist.gov/download.cfm (last visited on May 25, 2015).

85 HEWLETT-PACKARD SEC. RESEARCH, CYBER RISK REPORT 2013, HEWLETT-PACKARD ENTERS. SEC. 20 (Feb. 2014), *available at* http://info.hpenterprisesecurity.com/register_hpenterprisesecurity_cyber_risk_report_2013 .

86 See id.

87 *Id*. at 21.

88 VERIZON ENTER. SOLUTIONS, 2014 DATA BREACH INVESTIGATION REPORT (Apr. 23, 2014), *available at* http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf/.

89 *Id*. at 38.

90 *See, e.g.*, Bill Leonard, *Are 'Inside Jobs' the Biggest Cybersecurity Threat to Employers?*, SOCIETY FOR HUMAN RESOURCE MANAGEMENT (Nov. 24, 2014), http://www.shrm.org/hrdisciplines/safetysecurity/articles/pages/biggest-cybersecurity-threat-employers.aspx.

insider document access indicative of potential trade secret misappropriation will immediately be flagged and investigated.

Against this backdrop, companies should make securing their trade secrets a top priority. The good news is that many have, and corporate systems today are generally far more secure than in the past. Information regarding best practices is readily available,[91] as are a growing array of cybersecurity products and services: according to Gartner, global "security software" revenue was $19.9 billion in 2013.[92]

But cybersecurity is an arms race, and no matter how well companies attempt to protect their networks, cyberintruders will still sometimes manage to penetrate company systems and make off with trade secrets.[93] In light of that reality, here are some recommendations that can help companies manage trade secrets.

A. *Recommendation 1: Companies Should Segment Both Their Networks and the Trade Secret Information on Those Networks*

Simultaneously segmenting both trade secrets and the networks on which they are stored can be vital to impeding cyber-enabled trade secret theft. Segmentation distributes information so that no single cybersecurity breach exposes enough of a trade secret to allow the attacker to obtain the full set of information needed to replicate a targeted invention, product, or service.[94]

In the context of manufacturing, the value of segmenting trade secrets is well understood.[95] Through segmentation, a manufacturing process can be partitioned

---

91 *See, e.g.*, FENWICK & WEST LLP, TRADE SECRETS PROTECTION: A PRIMER AND DESK REFERENCE FOR MANAGERS AND IN HOUSE COUNSEL (2001), *available at* http://www.fenwick.com/FenwickDocuments/Trade_Secrets_Protection.pdf; VERIZON ENTER. SOLUTIONS, *supra* note 88, at 42.

92 *Gartner Says Worldwide Security Software Market Grew 4.9 Percent in 2013*, GARTNER (Jun. 10, 2014), http://www.gartner.com/newsroom/id/2762918.

93 Mueller, *supra* note **Error! Bookmark not defined.** (conceding that all organizations are vulnerable to hacking, no matter their security precautions).

94 Nimmy Reichenberg, *Improving Security via Proper Network Segmentation*, SEC. WEEK (Mar. 20, 2014), http://www.securityweek.com/improving-security-proper-network-segmentation.

95 *See, e.g.*, BRUCE GOLDNER & JONATHAN HILLEL, TOLL MANUFACTURING TRANSACTIONS: TRADE SECRET AND IP PROTECTION, PRACTICAL LAW

into multiple steps, each contracted out to a separate company.[96] But segmentation does not need to be limited to manufacturing, nor does it need to be limited to managing information shared with third parties. It can also be applied more broadly to how trade secrets are stored and used on a company's own networks.[97] For example, consider a company that uses a series of sophisticated algorithms that are run on the company's servers to deliver a service to consumers through a smartphone app. The source code associated with different components of those algorithms could be stored and accessed in a manner that minimizes the likelihood that the entire set of source code could be accessed by a cyberintruder who manages to penetrate one of the company's networks. More fundamentally, the structure of the code can be designed in a modular manner that specifically facilitates partitioned storage that can increase cybersecurity.[98]

Trade secrets should be analyzed to identify ways in which they can be partitioned into segments that can then be distributed only on a need-to-know basis, both within and outside a company. Computer code can be designed and tested in a modularized manner, minimizing the number of computers on which the entire set of source code is stored.[99] Companies engaged in chip design can also leverage the modular structure of most chips by limiting the number of locations where information about the full design is stored. Access to internal databases of customer lists and other sensitive information can be structured to minimize the proliferation of copies when that information is accessed. "Negative information," which is the term used in trade secret law to describe information about what *doesn't* work—often obtained through extensive, costly

---

COMPANY 3 (2013), *available at* http://www.skadden.com/sites/default/files/publications/Toll%20Manufacturing%20Transactions%20Trade%20Secret%20and%20IP%20Protection%20(8-525-5209).pdf.

96 *See generally* ERNST & YOUNG, SUPPLY CHAIN SEGMENTATION (2012), *available at* http://performance.ey.com/wp-content/uploads/downloads/2013/02/Supply-chain-segmentation_DC0121.pdf (detailing the benefits to companies of segmenting their supply chains among various third parties).

97 Trade secret segmentation is related to, but different from, the need-to-know partitioning of information that has long been common in the defense and defense contractor worlds.

98 *See* Dan Shoemaker & William Conklin, Cybersecurity: The Essential Body of Knowledge 296 (2011).

99 See id.

research[100]—can often be stored in a very limited set of locations because it does not need to be frequently accessed.

Employees have a key role in implementing trade secret segmentation. Employees should be made aware of the value of segmentation and be encouraged to store and exchange trade secret information only to the extent necessary to do their jobs. In addition, employees can actively help identify ways to segment information in ways that promote robustness to breaches without compromising efficiency.

With respect to computer networks, the cybersecurity advantages of segmentation, which aims to ensure that an attacker who has breached one part of a network cannot freely move through the entire network, are well recognized. As the Verizon 2014 Data Breach Investigations Report noted, "[g]ood network and role segmentation will do wonders for containing an incident, especially where actors intend to leverage access to one desktop as a stepping-stone to the entire network."[101] Segmenting *both* trade secrets *and* the networks on which they are stored can greatly reduce the utility of information accessible to cyber-intruders.

B. *Recommendation 2: Companies Should Avoid Overreliance on NDAs as Mechanisms to Protect Trade Secrets, Because Over-Disclosure Can Lead to Increased Exposure to Cyber-Enabled Trade Secret Theft*

Most companies are quite careful about requiring nondisclosure agreements ("NDA") before revealing trade secrets to third parties, such as suppliers, partners, consultants, or attorneys.[102] NDAs, however, are commonly viewed as a legal box to be checked, as opposed to part of an overarching approach to managing trade secrets. In many cases, the disclosing party performs little or no diligence regarding the security practices of the party that will receive information under an NDA, and once an NDA is in place, companies often over-

---

100 *What is a Trade Secret?*, BOHAN MATHERS INTELLECTUAL PROPERTY LAW, http://www.bohanmathers.com/what-is-a-trade-secret.html (last visited on May 25, 2015).

101 VERIZON ENTER. SOLUTIONS, *supra* note 88, at 42; *see also* Reichenberg, *supra* note 94.

102 *See* BAKER BOTTS, THE FUTURE OF CYBER-SECURITY: THREATS AND OPPORTUNITIES 15–17, *available at* http://files.bakerbotts.com/file_upload/documents/CyberSecurityBrochure.pdf.

disclose. As a result, trade secret information that should have been kept in-house gets replicated on the computer systems of one or more third parties.

If a company's trade secrets are compromised in a cyberintrusion targeting a third party to whom those secrets have been disclosed, an NDA may be of little use. Although NDAs generally require third party recipients to exercise at least a reasonable degree of care in protecting information, a sufficiently sophisticated intrusion might circumvent even very strong security measures, giving the third party grounds to assert that it honored the NDA despite the compromise.[103] Not to mention, arguing about responsibility for a breach does nothing to recover the lost information. Furthermore, many sophisticated intrusions will simply go undetected, leaving both the trade secret owner and the third party partner none the wiser that the information has been compromised.[104]

There are several steps that companies can take to better protect trade secrets shared with third parties. First, they can perform better diligence on third party cybersecurity practices and capabilities. As noted above, in many cases diligence is either absent altogether or perfunctory. Before agreeing to provide documents containing trade secrets under an NDA, a company should ask who will have access to the documents, where on the third party's networks and systems they will be stored, what measures the third party will take to ensure that the documents are only accessed on a need-to-know basis, and whether the third party will be willing to confirm that the documents have been erased once they are no longer needed. Where appropriate, information derived from the responses can be incorporated into the language of the NDA prior to its execution.

Second, companies can be more conservative in determining what to share. Too often, there is an assumption that once an NDA is in place, anything can be shared. The resulting tendency is to over-disclose needlessly and risk trade secret information that should have been kept in-house. For example, under an NDA companies will often provide documents that contain far more information than

---

103 Consider an NDA requiring, for example, that the recipient 1) safeguard the received confidential information with the same level of care used to safeguard the recipient's own confidential information and 2) use at least a reasonable degree of care in safeguarding the received information. If the recipient adheres to these requirements, but the information is nonetheless compromised in a sophisticated cyberattack, the recipient could argue that it did indeed honor the language of the NDA.

104 ALPEROVITCH, *supra* note 2, at 2.

is necessary. This could involve providing a fifty-page document, of which only five pages are relevant to the discussions with the third party. While it takes more time, a far better approach is to perform a careful need-to-know analysis regarding materials to be shared, and when appropriate, to create revised versions of the documents containing only the information that the third party has a need to know.

Third, when sharing information with third parties, companies should consider strategically withholding certain information that may be less central to the work the third party is performing, but would lead to greater harms if compromised. Every piece of confidential information has a particular utility when used as intended by the third party, and every piece of information can be associated with a level of potential harm if it is misappropriated.[105] When the ratio of utility to potential harm is low, companies will often be better off withholding the information, even when an NDA has been signed.

C. *Recommendation 3: Companies Should Act More Quickly on Patentable Inventions*

Recent changes to U.S. patent law have worsened the potential consequences of cybersecurity breaches that could allow a competitor to steal information relating to inventions not yet patented.[106] Put simply, there is an increased incentive for unethical actors to steal inventions and front-run the legitimate inventors in patent filings.[107] One simple way to reduce the probability of invention theft is to act quickly in decisions regarding whether to file for a patent or whether to maintain the invention as a trade secret.[108]

Under the America Invents Act ("AIA"), the United States moved from a "first-to-invent" patent system to what is called, only partially accurately, a "first-to-file" system.[109] To see how these two systems differ in a manner that impacts

---

105 *See id*.

106 John Villasenor, *How to Protect Your Company From Invention Theft*, FASTCOMPANY (Apr. 6, 2012, 12:30 AM), *available at* http://www.fastcompany.com/1829563/how-protect-your-company-invention-theft.

107 *Id*.

108 *See id*.

109 The first-to-file rules apply to patent applications with an effective filing date of March 16, 2013, or later. *See* Leahy–Smith America Invents Act, Pub. L. 112-29, § 3, 125 Stat. 284 (2011) [hereinafter AIA].

trade secret security, consider an example involving two inventors who independently arrive at the same invention. Suppose that Inventor 1 conceives an invention in June and files the associated patent application in September. Subsequently, Inventor 2 independently conceives the same invention in July and files for a patent in August.

Who gets the patent? Under the old first-to-invent rules, Inventor 1 could get the patent thanks to his or her earlier invention,[110] which, if needed, could potentially be proven through internal company documents.[111] By contrast, under the new first-to-file system, U.S. patent rights depend not on the dates of respective invention, but instead on a combination of the dates of patent filings and of any pre-filing public disclosures of the invention.[112] If there are no pre-filing public disclosures,[113] the first-to-file system really is a race to the patent office, just as the term implies.[114] And even if one or both inventors make a public disclosure prior to filing an application, it will be the disclosure dates and/or filing dates, and not the invention dates that determine U.S. patent rights under the first-to-file system.[115]

This new landscape gives unethical competitors an increased incentive to extract information about undisclosed inventions that have not yet been the subject of patent filings by the legitimate owner, and then to quickly file patent applications based on the stolen information. This could involve breaking into a company's networks to obtain documents describing inventions under development, and then using those documents to create patent filings that the company responsible for the cyber-attack would claim as its own. Under U.S. law

---

110 With respect to the pre-AIA first-to-invent system, it is assumed in this example that Inventor 1 works diligently to reduce the invention to practice during the period from June to September.

111 *See, e.g.*, Monsanto Co. v. Mycogen Plant Sci., Inc., 261 F.3d 1356, 1363, 1370 (Fed. Cir. 2001) (finding that internal documentation, such as an inventor's notebook, was sufficient proof of the date of the inventor's work).

112 Pre-filing public disclosures of an invention can eliminate patent rights in non-U.S. jurisdictions.

113 One very important downside of public disclosures made in advance of a patent application is that they can eliminate patent rights in non-U.S. venues. They can also eliminate patent rights in the U.S. if a patent application is not filed within one year of the first disclosure. AIA § 102(b)(1)(A).

114 AIA § 3.

115 *Id.*

there is a new "derivation proceeding" that, in principle, can address this sort of behavior.[116] Initiating a derivation proceeding to address the above scenario, however, would require filing a petition "supported by substantial evidence"[117] of misappropriation. Furthermore, the window during which the theft victim has the right to file a derivation proceeding petition is quite short.[118] In practice, it will often be difficult or impossible to show that information about an invention—which at the time of the theft constituted trade secrets—was stolen. And, the unethical competitor might choose to use the stolen information as the basis for a patent filing in a non-US jurisdiction.[119]

In short, the longer a company sits on a new invention without filing a patent application, the more opportunity this gives to both ethical competitors who might independently conceive and file for a patent on the same invention, and to unethical actors who might steal it. Acting quickly does not mean that companies should file patent applications for all of their inventions, as this would be impractical for financial and other reasons.[120] It also does not mean that companies should fail to put the proper care into preparing patent applications.

---

[116] *Derivation Proceeding*, U.S. PATENT AND TRADEMARK OFFICE, http://www.uspto.gov/patents-application-process/appealing-patent-decisions/trials/derivation-proceeding (last visited May 24, 2015) ("A derivation proceeding is a trial proceeding conducted at the Board to determine whether (i) an inventor named in an earlier application derived the claimed invention from an inventor named in the petitioner's application, and (ii) the earlier application claiming such invention was filed without authorization.").

[117] See id.

[118] *Id.* ("An applicant subject to the first-inventor-to-file provisions may file a petition to institute a derivation proceeding only within 1 year of the first publication of a claim to an invention that is the same or substantially the same as the earlier application's claim to the invention.")

[119] *See, e.g.*, Brocade Commc'n Sys., Inc. v. A10 Networks, Inc., No. C 10-3428 PSG, 2013 WL 831528, at *1 (N.D. Cal. Jan. 10, 2013) (finding by jury that A10 misappropriated Brocade's unpatented trade secrets and subsequently used the secrets as the basis for certain of A10's own patents).

[120] Even in a hypothetical company with an unlimited budget for filing patent applications, there would be practical limits on how many applications could be filed. A patent filing can require a substantial time commitment by the inventors to create the drawings and text to describe the invention in a suitably detailed manner.

Rather, it means that companies should make decisions regarding patent filings as early as possible, and for those inventions where the decision is to apply for a patent, the filing (either a suitably detailed provisional application or a full utility application) should be made expeditiously.

One way companies can help ensure timely patent decisions is to convene frequent (e.g., once a month) meetings of an IP committee charged with reviewing disclosures of potential inventions and deciding when to proceed with a patent application. For this process to be effective, employees need to be trained to promptly report potential inventions for consideration. To facilitate this, companies can: (1) put in place incentive programs to reward employees who submit disclosures deemed worthy of patenting; and (2) provide training to employees so that they will be better positioned to identify innovations that may be patentable.

D. *Recommendation 4: Companies Should Ensure That Cybersecurity Considerations Are Part of Their Patent and Trade Secret Decisions*

Companies have long needed to determine whether to disclose patentable inventions by filing a patent application, or to retain them as trade secrets.[121] What has changed is that cybersecurity exposures make it harder to keep the "secret" in "trade secret." When there is sufficient economic motivation, sophisticated cyberattackers will often succeed in obtaining files containing trade secrets.[122] Most corporate networks are far more porous than company executives (and information security managers) would like to believe.[123] No matter how carefully companies train their employees, the laws of statistics essentially guarantee that a well-designed "spear phishing" attack—in which employees are targeted by highly personalized e-mails that appear to be legitimate but actually

---

121 *See, e.g.*, DEAN W. RUSSELL ET AL., KILPATRICK STOCKTON LLP, *Choosing Between Trade Secret and Patent Protection*, *in* INTELLECTUAL PROPERTY DESK REFERENCE 215, 222 (Jan. 1, 2009), *available at* https://clients.kilpatricktownsend.com/IPDeskReference/Documents/Trade%20Secret%20or%20Patent%20Protection.pdf.

122 *See* FORRESTER CONSULTING, *supra* note 76 at 2 (finding that "[t]he more valuable a firm's information, the more incidents it will have").

123 *See* ALPEROVITCH, *supra* note 2, at 2.

contain (or link to) malware—will succeed.[124] Thus, a realistic view of trade secret security should be an explicit consideration in the decision on what to patent.

Some types of trade secrets (e.g., customer databases, or plans for marketing a new product) simply are not eligible for patent protection.[125] But many trade secrets are in the form of potentially patentable inventions,[126] and in cases where companies are on the fence regarding which option to choose, cybersecurity considerations can bias decision-making away from trade secrets and in favor of patents.[127] When weighing the patent/trade secret decision, there are three different possibilities with respect to the duration of trade secret protection associated with information about the invention.

First, if a company elects not to file a patent application at all, the invention can remain a trade secret permanently—or until it is intentionally or unintentionally disclosed,[128] or independently developed by a third party.[129] Second, if the company elects to file a patent application without submitting a "non-publication request," then the invention can remain a trade secret until the

---

124 *See, e.g.*, Dan Bowman, *Security Experts Worry About 'Spear Phishing' in Wake of CareFirst Breach*, FIERCEHEALTHIT (May 21, 2015), *available at* http://www.fiercehealthit.com/story/security-experts-worry-about-spear-phishing-wake-carefirst-breach/2015-05-21.

125 *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 485 (1974) ("Trade secret law will encourage invention in areas where patent law does not reach . . . ."); *Patents or Trade Secrets?*, WORLD INTELLECTUAL PROPERTY ORGANIZATION, http://www.wipo.int/sme/en/ip_business/trade_secrets/patent_trade.htm (last visited May 25, 2015) ("[T]rade secrets may concern inventions or manufacturing processes that do not meet the patentability criteria . . . .").

126 *See Patents or Trade Secrets?*, *supra* note 125 ("[T]rade secrets may concern inventions that would fulfill the patentability criteria and could therefore be protected by patents.").

127 *See id.* ("If the secret is embodied in an innovative product, others may be able . . . [to] discover the secret and be thereafter entitled to use it. Trade secret protection of an invention in fact does not provide the exclusive right to exclude third parties from making commercial use of it. Only patents and utility models can provide this type of protection.").

128 *See supra* Part II.

129 *See Kewanee Oil Co.*, 416 U.S. at 474 ("A trade secret law, however, does not offer protection against discovery by fair and honest means, such as by independent invention . . . .").

application is automatically published by the PTO eighteen months after the claimed priority date.[130] Of course, a company may choose to publicize the invention after filing the application without waiting until the end of the eighteen-month period, but in that event the company would lose trade secret status with respect to the disclosed information.[131]

Third, if the company files a patent application with a non-publication request, the invention can remain a trade secret until the patent issues.[132] If the patent never issues, then the company can retain the invention as a trade secret.[133] Non-publication requests are only available for inventions that have not been, and will not be in the future, the subject of a foreign patent application.[134] In practice, only a minority of companies choose this third approach, because a non-publication request eliminates the opportunity to pursue foreign patents, and removes the ability to assert provisional rights domestically with respect to the published claims in the pending application.[135]

Companies choosing among these options should perform an assessment of the difficulties associated with protecting a particular trade secret over the long term. This requires an understanding of who within and outside a company will have access to the trade secret, where it will be stored, and the extent to which it can be subjected to partitioning or other steps that would protect the trade secret during a network compromise. The extent of the challenge depends in part on the nature of the trade secret. A trade secret that, in the process of being used, ends up stored in human-readable form (as opposed to non-readable compiled code) on hundreds of different computers, including the personal smartphones of company employees, probably will not stay secret for very long. If the trade secret covers patent-eligible subject matter, companies should consider a patent application. On the other hand, a trade secret that can be tightly controlled will

---

130 *See* 35 U.S.C. § 122(b)(2)(B)(i) (2012).

131 *See id*. at (b)(2)(B)(iii).

132 *See* Russell, *supra* note 121, at 122.

133 See id.

134 *See* 35 U.S.C. § 122(b)(2)(B)(i).

135 W. EDWARD CROOKS, HAHN LOESER & PARKS LLP, TO PUBLISH OR NOT TO PUBLISH? (2006), *available at* http://www.hahnlaw.com/wp-content/uploads/2015/02/447.pdf (detailing how "provisional rights" are not available to patent applicants who choose to forego publication of the patent application).

have a higher chance of remaining undisclosed, thereby increasing its long-term value.[136]

E. *Recommendation 5: For Inventions Retained as Trade Secrets, Early Commercial Use Can Provide Important Protection if the Trade Secret is Later Patented by a Third Party*

Commercially using a trade secret that might later be patented by a competitor has advantages. As stated above, many trade secrets are patent-eligible, and there is nothing to stop a competitor from independently inventing and patenting the same trade secret. Thanks to a new "prior user rights" feature of patent law, if the competitor sues for patent infringement, the company that independently—and at an earlier date—developed the same trade secret, a sufficiently early commercial use of the trade secret can prevent a finding of infringement.[137] As Representative Lamar Smith (R-TX), one of the sponsors of the patent reform legislation in 2011, explained, the "inclusion of prior user rights is essential to ensure that those who have invented and used a technology but choose not to disclose that technology—generally to ensure that they do not disclose their trade secrets to foreign competitors—are provided a defense against someone who later patents the technology."[138]

---

136 *See* Gene Quinn, *The Trade Secret Value Proposition: The Secrecy Requirement*, IPWATCHDOG (Apr. 19, 2014), http://www.ipwatchdog.com/2014/04/19/the-trade-secret-value-proposition-the-secrecy-requirement/id=49086/ ("Secrecy is, therefore, at the very heart of a trade secret, and is what creates the value proposition."); *see e.g.*, *Revisting Buffett: Coca-Cola in 1988*, GURUFOCUS (Jan. 19, 2013), http://www.gurufocus.com/news/205476/revisiting-buffett--cocacola-in-1988 (showing that the maintained secrecy of Coca-Cola's formula resulted in annual incomes that more than doubled between 1979 and 1988).

137 The expanded prior commercial use defense to infringement in the AIA only applies to patents on "subject matter consisting of a process, or consisting of a machine, manufacture, or composition of matter used in a manufacturing or other commercial process" issued on or after September 16, 2011. 35 U.S.C. § 273(a) (2012). In addition, prior user rights generally do not apply to patents covering a university invention *See id*. § 273(c)(2). And, the prior commercial use defense only applies if the commercial use occurred sufficiently early. *See id*. § 273(a)(2).

138 America Invents Act, 157 CONG. REC. E1219 (daily ed. June 28, 2011) (statement of Rep. Smith).

Prior user rights are designed primarily to protect companies against patents arising from *independent* invention by a competitor.[139] But they also have a potential role if an invention is stolen through an undetected cybersecurity intrusion. Having a trade secret stolen and then patented by a competitor is a clearly a bad thing. Being sued by a competitor armed with a patent obtained using the stolen information is even worse.

In an ideal world, this should never happen. But in the real world, it could. In cases where there is no evidence of misappropriation, early commercial use of the trade secret can be vital to ensuring a company's right to continue using it.[140] The flip side is that the prior user rights provision does not provide any protection to a company that sits on a trade secret without using it commercially.[141]

VI. CONCLUSION

Much of the attention to corporate cybersecurity is directed towards minimizing the chances of security breaches. But that alone is not enough. Cybersecurity breaches, including breaches specifically designed to extract trade secrets, will sometimes happen even to companies with highly sophisticated systems and a security-aware workforce. This article has provided some recommendations for how companies can manage trade secrets in light of that inevitability.

---

139 *See* U.S. PATENT & TRADEMARK OFFICE, REPORT ON THE PRIOR USER RIGHTS DEFENSE 7 (Jan. 2012), *available at* http://www.uspto.gov/sites/default/files/aia_implementation/20120113-pur_report.pdf ("[T]he defense is available to persons who independently commercially employed the invention in the United States . . . .").

140 The commercial use must have occurred "at least 1 year before the earlier of either–(A) the effective filing date of the claimed invention; or (B) the date on which the claimed invention was disclosed to the public in a manner that qualified for the exception from prior art under section 102(b)." 35 U.S.C. §273(a)(2). Of course, this means that if the trade secret is stolen in an undetected cyber-intrusion and used by the thief in a patent application within one year of the first commercial use, the prior user rights provision will not apply. By contrast, if the would-be-cyber-intruders can be kept out of company systems for at least a year after the first commercial use, the prior user rights provision could apply.

141 *See id.* § 273(a).