Working Paper Series
No. 14012

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

John Villasenor
University of California, Los Angeles
Hoover Institution
Brookings Institution

August 2014

Hoover Institution Working Group on
Intellectual Property, Innovation, and Prosperity
Stanford University

www.hooverip2.org

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

(This is a manuscript of an article to be published in the
American Intellectual Property Law Association Quarterly Journal, 2015)

John Villasenor[1]
August 28, 2014

Abstract

Cybersecurity intrusions aimed at extracting trade secrets are an unfortunate feature of the 21st century business landscape. In response, many companies have made cybersecurity a top priority, and their networks and systems have become much more secure as a result.

However, while improving security is a critical goal, it should not be the only goal. Companies also need to give attention to what might be called the corporate cybersecurity elephant in the room: How does the inevitability that their networks will sometimes be compromised impact best practices for handling trade secrets *despite* those breaches? This paper aims to provide some answers to that question.

As discussed herein, companies should 1) "segment" not only their networks but also the trade secret information on those networks, thereby limiting the impact of any single cybersecurity breach, 2) avoid overreliance on NDAs, since over-disclosure can lead to increased exposure to cyber-enabled trade secret theft, 3) act more quickly on patentable inventions in light of recent changes to U.S. patent law that can increase the incentives driving trade secret theft, 4) ensure that cybersecurity considerations are be part of patent/trade secret decisions, and 5) be aware of—and, as appropriate, take advantage of—new changes to U.S. patent law the increase the potential benefits of early commercial use of trade secrets.

[1] Professor, UCLA; Nonresident senior fellow at the Brookings Institution; National Fellow at the Hoover Institution. Contact: villa@ee.ucla.edu

Introduction

It would be an understatement to call trade secret cybersecurity a complex challenge. Trade secrets stored on company networks are ripe targets for cyberintruders who have continuing access to new vulnerabilities, including via a robust global market for zero day exploits. When a company can have 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 security of economically valuable confidential information be assured? The answer, unsurprisingly, is that it can't.

As a result, the "every company has been hacked" theme has become a popular refrain in discussions about cybersecurity. In 2011 Dimitri Alperovitch, who was then with McAfee and went on to found 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.

But there is no such thing as perfect cybersecurity. Sometimes, despite all efforts to the contrary, skilled attackers 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, copyright, and trade secrets—it is trade secrets that are typically the most vulnerable. In 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. And for this very same reason, they are particularly attractive targets for cyber-intruders.

---

[2] Dmitri Alperovitch, *Revealed: Operation Shady RAT*, MCAFEE, at 2 (2011), *available at* http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf (last visited on August 21, 2014).

[3] Robert S. Mueller, III, *Speech at the RSA Cyber Security Conference*, San Francisco, CA (March 1, 2012), *available at* http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

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.

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. To help fill that gap, this paper provides 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, the paper starts with an explanation of trade secrets and an overview of the associated legal frameworks.

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.[4] Formulas, computer programs, methods, techniques, and processes can all be trade secrets. The most famous trade secret is probably the Coca Cola formula, which is reportedly held in a vault in Atlanta.[5] Other famous trade secrets include the Google search algorithm[6] and the recipe for Kentucky Fried Chicken.[7] The details of a

[4] 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 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." See Unif. Trade Secret Act §1(4) (1985), 14 U.L.A. 538 (Supp. 2010), *available at* . http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf (last visited on August 21, 2014).

[5] Leon Stafford, *Coke hides its secret formula in plain sight in World of Coca-Cola move*, ATLANTA JOURNAL-CONSTITUTION, Dec. 8, 2011, http://www.ajc.com/news/business/coke-hides-its-secret-formula-in-plain-sight-in-wo/nQPMm/.

[6] Colleen Kane, *7 Sought-After Trade Secrets*, CNBC.COM, at slide 8 (Aug. 23, 2012, 10:18 AM EST), http://www.cnbc.com/id/48755451. Google's original page rank algorithm is patented (U.S. patent number 6,285,999). However, that patent dates from the late 1990s, and Google's search algorithm today clearly includes many features not reflected in that patent.

[7] Id. at slide 6.

manufacturing process can be a trade secret, as can the breakdown of ingredients used by a perfume company to create a fragrance.

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. 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 in those documents qualifies, at least temporarily, as a trade secret. If the company elects not to file a patent application, the information can remain a trade secret. And if a patent application is filed, the information in the application could retain trade secret value until it is published, typically 18 months later.[8] Trade secrets also have a connection to copyright. While published works themselves are obviously not trade secrets, 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 can certainly involve trade secrets. In addition, information about an unpublished copyrighted work (such as a movie that has not yet been released) can also qualify as a trade secret.

Trade secrets differ from patents in important ways. Patents provide a time-limited, government-granted monopoly[9] with respect to an invention (though not necessarily with respect to a market) in exchange for disclosure of the invention. 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.[10] This right includes the ability exclude those who might later[11] independently develop the same invention, as well as those who identify the invention using reverse engineering.

---

[8] In the absence of a non-publication request, patent applications are published by the PTO 18 months after the claimed priority date. After filing a patent application, a company may also elect to publish information in a patent application. A company can also publish this information before filing a patent application, but in doing so would generally eliminate its 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.

[9] Some object to the term "monopoly" in association with patents. However, the Supreme Court has used that characterization (e.g., "The latter pose no comparable risk of pre-emption, and therefore remain eligible for the monopoly granted under our patent laws." *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, __ U.S.___, 82 L.Ed.2d 296, 305 (2014).

[10] 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).

[11] "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.

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. Patents generally expire 20 years[12] after the filing date, while trade secrets can be used for as long as their owner perceives them to have value and maintains their secrecy.

In addition, while patents protect inventions, trade secrets cover broader subject matter. Some trade secrets cover inventions that, had the owner desired, could have been patented. However, trade secrets can also protect information that is clearly patent-ineligible. 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.[13]

Patents are jurisdiction-specific, and are issued in the United States by the United States Patent and Trademark Office (PTO) following an examination process. Trade secret status is automatic; there is no government entity that must first pass judgment on the information before it can qualify as a trade secret. If the information concerned meets the relevant statutory definition,[14] then it is a trade secret. And unlike trademarks, which can be examined and registered through the PTO, and copyright, which can be registered through the U.S. Copyright Office, there is no federal or state registry for trade secrets. The government typically gets involved in evaluating trade secrets only in civil or criminal trade secret misappropriation trials, when courts are often asked to evaluate, among other things, defendants' claims the information at issue did not in fact qualify as a trade secret.

American Trade Secret Legal Frameworks

In the United States, statutory protection for trade secrets is found in most states, and in the case of economic espionage, at the federal level. All but a few states have enacted civil[15] trade secret statutes based on the Uniform Law Commission's (ULC's) Uniform Trade Secrets Act (UTSA),[16] which was initially approved by the ULC in 1979 and

---

[12] See *2701 Patent Term [R-11.2013]*, United States Patent and Trademark Office - Department of Commerce, *available at* http://www.uspto.gov/web/offices/pac/mpep/s2701.html (last visited on August 21, 2014) for a more complete description of the rules for computing patent term.

[13] Opinion & Order at 8, *Wellington Res. Grp., LLC v. Beck Energy Corp.*, No. 2:12-cv-00104-ALM-EPD (S.D. Ohio Sept. 20, 2013), ECF No. 150.

[14] As discussed herein, in the United States, with respect to civil litigation the relevant statutory definition depends on the state, and for trade secret theft under the federal economic espionage statute, the relevant statutory definition is provided in 18 U.S.C. § 1839. Internationally, there are further variations in the definition of trade secret.

[15] In addition, some states have criminal trade secret statutes. See, e.g., CAL. PENAL CODE § 499c.

[16] See Unif. Trade Secret Act (amended 1985), 14 U.L.A. 529 (Supp. 2010), *available at* http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf (last visited on August 21, 2014).

revised in 1985. Under the UTSA, a trade secret

> means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[17]

Either acquisition of a trade secret through improper means or improper disclosure of a trade secret can constitute misappropriation.[18] 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).

Trade secrets are addressed in federal criminal statutes through the Economic Espionage Act (EEA),[19] which was enacted in 1996, and indirectly through the Computer Fraud and Abuse Act (CFAA), which was enacted in 1986. The EEA addresses trade secret theft for the "benefit any foreign government" as well as, more generally, trade secret theft for "the economic benefit of anyone other than the [trade secret] owner."[20] 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",[21] and in the 2013

---

[17] Id. §1(4), 14 U.L.A. 538.

[18] The full definition of "misappropriation" in the UTSA is: " 'Misappropriation' means: (i) 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; 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." Unif. Trade Secret Act §1(2) (amended 1985), 14 U.L.A. 537 (Supp. 2010).

[19] Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489 (1996) (codified at 18 U.S.C. §§ 1831–1839).

[20] 18 U.S.C. §§ 1831(a), 1832(a).

[21] Theft of Trade Secrets Clarification Act of 2012 (TTSCA), S. 3642, 112th Cong. (2d Sess. 2012), amending 18 U.S.C. § 1832(a). Prior to the TTSCA, 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." Under the TTSCA, this was amended to "related to a product or service used in or intended for use in interstate or foreign commerce." The

the fines for trade secret theft under the EEA were increased.[22]

The CFAA makes it a crime to access a computer "without authorization or exceed[ing] authorized access" and "thereby obtain[] . . . information from any protected computer."[23] The CFAA[24] also criminalizes accessing a "protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss."[25] Federal prosecutors pursuing trade secret theft cases sometimes bring charges under both the EAA and the CFAA, or in some instances under the CFAA alone.

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"[26] investigations to, among other things, address "[u]nfair methods of competition and unfair acts in the importation of articles."[27] In a 2011 case, 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."[28] The Federal Circuit held that it does, finding that while the misappropriation occurred outside the United States, the subsequent importation would lead to unfair competition addressable by the ITC under Section 337. This allows the ITC to issue exclusion orders barring the importation of the products in question into the United States.

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 since not all states have adopted the language in the USTA verbatim, leading to differences among states in the scope of trade secret protection. In addition, each state has a separate body of trade secret case law. There have been repeated attempts to introduce a federal civil trade secret statute, most recently in April 2014 when Senators Christopher Coons (D-DE) and Orrin Hatch (R-UT) introduced the Defend Trade Secrets Act of 2014 (DSTA).[29]

International Trade Secret Legal Frameworks

---

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."

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

[23] 18 U.S.C. § 1030(a)(2), (a)(2)(C).

[24] The CFAA sometimes been criticized, not unreasonably, as being overly broad. Legislation that would have narrowed its scope was introduced in 2013 but not enacted.

[25] 18 U.S.C. § 1030(a)(5)(C).

[26] Named after Section 337 of the Tariff Act of 1930, now 19 U.S.C. § 1337.

[27] 19 U.S.C. § 1337(a)(1)(A).

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

[29] Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014), *available at* https://beta.congress.gov/113/bills/s2267/BILLS-113s2267is.pdf (last visited on August 21, 2014).

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[.]"[30] However, there are wide variations in the level to which member countries have implemented trade secret protections.

In late 2013, the European Commission released a proposed Directive "on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure."[31] If adopted, this would create a consistent civil trade secret law framework for European Union countries. Trade secret protections are also among the intellectual property topics under discussion in the ongoing Trans-Pacific Partnership (TPP) negotiations as well as the more recent Transatlantic Trade and Investment Partnership (T-TIP) negotiations.

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. Trade Representative, in December 2013, at the U.S.-China Joint Commission on Commerce and Trade (JCCT), "China's National Leading Group on Combating IPR Infringement and the Manufacture and Sales of Counterfeit and Substandard Goods commits to adopt and publish an Action Program on trade secrets protection and enforcement."[32]

A full review of international trade secret laws and developments is outside the scope of this paper, though 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,"[33] a November 2013 European Commission guide to trade secret laws in ASEAN (the

---

[30] The World Trade Organization's Trade-Related Aspects of Intellectual Property Rights, § 7, art. 39 (2014), *available at* http://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm (last visited on August 21, 2014).

[31] European Commission, *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* (Nov. 28, 2013), COM(2013) 813 final – n° 2013/0402 (COD), *available at* http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/131128_proposal_en.pdf (last visited on August 21, 2014).

[32] U.S. Department of Commerce, *Fact Sheet: 24th U.S. – China Joint Commission on Commerce and Trade Fact Sheet* (Dec. 20, 2013), *available at* http://www.ustr.gov/about-us/press-office/fact-sheets/2013/December/JCCT-outcomes (last visited on August 21, 2014).

[33] European Commission, *Study on Trade Secrets and Confidential Business Information in the Internal Market, Final Study* (Apr. 2013), MART/2011/128/D, *available at* http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf (last visited on August 21, 2014).

Association of Southeast Asian Nations) countries,[34] an August 2013 Library of Congress report on "Protection of Trade Secrets" in Brazil, China, India, the Russian Federation, and South Africa,[35] and the USTR's "2014 Special 301 Report."[36]

Cybersecurity and Trade Secret Theft

It is impossible to know how many trade secret misappropriation incidents are tied to cybersecurity breaches. But there is good reason to believe that many of them are. For starters, trade secrets are valuable and are therefore a prime target. According to a 2010 Forrester Consulting paper, "[s]ecrets comprise two-thirds of the value of firms' information portfolios."[37] In 2012, then-NSA Director Gen. 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."[38]

For obvious reasons, merging information about vulnerabilities and incidents to place a specific value on economic losses due to cyber-enabled trade secret misappropriation is very difficult. Among other challenges, reported incidents are not typically described in terms that enable valuation calculations. In addition, while companies have reporting obligations when breaches expose personal data of their customers, they are not generally obligated to publicize intrusions that expose trade secret information unrelated to customer privacy.[39] Most fundamentally, most intrusions probably go undetected.

---

[34] European Commission, *GUIDE ON TRADE SECRETS, Protecting Your Trade Secrets in Southeast Asia* (Nov. 2013), *available at* http://www.asean-iprhelpdesk.eu/sites/default/files/publications/Trade-Secret-English.pdf (last visited on August 21, 2014).

[35] 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 (last visited on August 21, 2014).

[36] Office of the United States Trade Representative, *2014 Special 301 Report* (Apr. 2014), *available at* http://www.ustr.gov/sites/default/files/USTR%202014%20Special%20301%20Report%20to%20Congress%20FINAL.pdf (last visited on August 21, 2014).

[37] Forrester Consulting, *The Value of Corporate Secrets: How Compliance and Collaboration affect Enterprise Perceptions of Risk*, at 2 (Mar. 2010), *available at* http://www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20Secrets.pdf (last visited on August 21, 2014). The Forrester Consulting paper defined "secrets" as "trade secrets, confidential and other kinds of nonregulated but otherwise valuable data." Id. at 15.

[38] *An Introduction by General Alexander*, THE NEXT WAVE, Vol. 19, No. 4 (2012), *available at* http://www.nsa.gov/research/tnw/tnw194/article2.shtml (last visited on August 21, 2014).

[39] Except, of course, to the extent that the compromised trade secrets include the type of personal information for which reporting is required. In addition, in cases where a

Despite these challenges, there have been some efforts to put a number on losses. 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."[40] A May 2013 report from the Commission on the Theft of American Intellectual Property claimed that annual losses to the American economy due from international IP theft were likely over $300 billion.[41]

Reasonable people can of course 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 Vulnerability Database,[42] HP's 2013 "Cyber risk report" noted that over 4700 new vulnerabilities were reported through November 2013, and that this number was about 6% lower than the corresponding number for 2012.[43] Stated another way, the number of *reported* new vulnerabilities averages well over ten per day; the number of *unreported* new vulnerabilities is clearly higher. 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 patch by the affected product vendor.[44]

In addition, cyberespionage attacks are notable both in their sophistication and in their increasing frequency. The Verizon 2014 Data Breach Investigations Report[45] examined 511 cyberespionage incidents in 2013, noting "consistent, significant growth of incidents

---

documented trade secret theft results in material financial exposure for a public company, there would be reporting obligations to shareholders.

[40] 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.

[41] The Commission of the Theft of Intellectual Property, *The IP Commission Report* (Washington, D.C.: National Bureau of Asian Research, May 2013), at 2, *available at* http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf (last visited on August 21, 2014).

[42] *NVD Data Feed and Production Integration*, NATIONAL VULNERABILITY DATABASE, http://nvd.nist.gov/download.cfm (last visited on August 21, 2014).

[43] HP Security Research, *Cyber Risk Report 2013*, at 20 (Feb. 2014), *available at* http://www8.hp.com/h20195/v2/GetPDF.aspx%2F4AA5-0858ENW.pdf (last visited on August 21, 2014).

[44] Id. at 21.

[45] Verizon Enterprise 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 (last visited on August 21, 2014).

in the dataset"[46] and that cyberespionage "exhibits a wider variety of threat actions than any other pattern."[47]

It is also important to note that not all cyber-related trade secret misappropriation is due to penetrations that occur from outside a company. 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 insider document access indicative of potential trade secret misappropriation will immediately be flagged and investigated.

Against this backdrop, companies need to 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,[48] as are a growing array of cybersecurity products and services: According to Gartner, global "security software" revenue was $19.9 billion in 2013.[49]

But no matter how well companies attempt to protect their networks, cyber-intruders will still sometimes manage to make their way into company systems and make off with trade secrets. In light of that reality, here are some recommendations that can help companies manage trade secrets.

Recommendation 1: Companies should segment <u>both</u> their networks <u>and</u> the trade secret information on those networks

Simultaneously segmenting both trade secrets and the networks on which they are stored can be vital in 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.

In the context of manufacturing, the value of segmenting trade secrets is well understood.[50] Through segmentation, a manufacturing process can be partitioned into

---

[46] Id. at 38. The cyberespionage incidents tallied by Verizon including both those targeting companies as well as those targeting public sector organizations.
[47] Id.
[48] See, e.g., Fenwick & West LLP, *Trade Secrets Protection: A Primer and Desk Reference for Managers and In House Counsel* (June 2, 2003), *available at* http://www.fenwick.com/FenwickDocuments/Trade_Secrets_Protection.pdf (last visited on August 21, 2014) and Verizon Enterprise Solutions, *supra* note 44, at 42.
[49] Gartner Press Release, *Gartner Says Worldwide Security Software Market Grew 4.9 Percent in 2013*, Jun. 10, 2014, http://www.gartner.com/newsroom/id/2762918.
[50] See, e.g., Bruce Goldner & Jonathan H. Ashtor, *Toll Manufacturing Transactions: Trade Secret and IP Protection*, PRACTICAL LAW COMPANY, at 3 (2013), *available at* http://www.skadden.com/sites/default/files/publications/Toll%20Manufacturing%20Tran

multiple steps, each contracted out to a separate company. But segmentation doesn't need to be limited to manufacturing, and it doesn't 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.[51]

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. Companies engaged in chip design can also leverage the modular structure of most chips to limiting the locations where information about the full design is stored. Access to internal databases of customer lists and other sensitive information can be structured to ensure that new copies database information created in response to queries are erased as soon as they are no longer needed. "Negative information," which is the term used in trade secret law to describe information (often obtained through extensive, costly research) about what *doesn't* work, can be stored in an extremely limited set of locations since it doesn't 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 can't 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.[52] Segmenting *both* trade secrets *and* the networks on which they are stored can greatly reduce the utility of information accessible to cyber-intruders.

Recommendation 2: Companies should avoid overreliance on NDAs as mechanisms to protect trade secrets, since over-disclosure can lead to increased exposure to cyber-enabled trade secret theft

---

sactions%20Trade%20Secret%20and%20IP%20Protection%20(8-525-5209).pdf (last visited on August 21, 2014)..

[51] 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.

[52] Verizon Enterprise Solutions, *supra* note 44, at 42. See also Nimmy Reichenberg, *Improving Security via Proper Network Segmentation*, SECURITYWEEK.COM, Mar. 20, 2014, http://www.securityweek.com/improving-security-proper-network-segmentation.

Most companies are quite careful about requiring NDAs before disclosing trade secrets to third parties including suppliers, partners, consultants, or attorneys. However, NDAs 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-disclose. The result: Trade secret information that should have been kept in-house instead gets replicated on the computer systems of one or more third parties.

If a company's trade secrets are compromised in a cyber-intrusion targeting a third party to which they have been disclosed, an NDA may be of little use. While NDAs generally require third party recipients to use 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. In addition, 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.

There are several steps companies can take to better address sharing of trade secrets with third parties. First, they can perform diligence on third party cybersecurity (and other security) capabilities. As noted above, in many cases that diligence is either absent altogether or perfunctory. 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 to over-disclose needlessly risks trade secret information that should have been kept in-house.

Third, when sharing information with third parties, companies should consider strategically withholding certain information that may be less critical to the work the third party is performing, but that would lead to greater harms if compromised. More specifically, 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. 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.

Recommendation 3: Companies should act more quickly on patentable inventions

Due to recent changes to U.S. patent law, the potential consequences of cybersecurity breaches that might allow a competitor to steal information relating to inventions not yet the subject of patent applications have worsened. Put simply, there is an increased incentive for unethical actors to steal inventions and front-run the legitimate inventors in patent filings. 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.

Under the America Invents Act, the United States moved in 2013 from a "first-to-invent" patent system to what is called, only partially accurately, a "first-to-file" system.[53] To see how these two systems differ in a manner that impacts trade secret security, it is helpful to 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. Suppose, in addition, that 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,[54] which, if needed, could be proven through internal company documents. 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.[55] If there are no pre-filing public disclosures,[56] the "first-to-file" system really is a race to the patent office, just as the term implies. And even if one or both inventors makes 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.

This new landscape gives unethical competitors an increased incentive to extract information about as undisclosed inventions that have not yet been the subject of patent filings by the legitimate owner, and then to quickly file a patent application based on the stolen information with the U.S. PTO or with a foreign patent office. Under U.S. law there is a new "derivation proceeding" designed, in principle, to address this sort of behavior. However, initiating a derivation proceeding requires filing a petition "supported by substantial evidence"[57] that the invention was misappropriated. Furthermore, the window during which the theft victim has the right to file a derivation proceeding petition

---

[53] The "first-to-file" rules apply to patent applications with an effective filing date of March 16, 2013, or later.

[54] With respect to the pre-America Invents Act 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.

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

[56] 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.

[57] See *Derivation Proceedings*, United States Patent and Trademark Office - Department of Commerce, *available at* http://www.uspto.gov/aia_implementation/faqs_derivation_proceedings.jsp (last visited on August 21, 2014) for a description of the requirements for filing a petition to institute a derivation proceeding.

is quite short.[58] 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.

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 doesn't mean that companies should file patent applications for every single invention they come up with, as this would be impractical for financial and other reasons. And it doesn't mean that companies should fail to put the proper care into preparing patent applications. Instead, it means companies should make the decision regarding patent filings earlier rather than later, and for those inventions where the decision is to apply for a patent, the filing (either a suitably detailed provision application or a full utility application) should be made expeditiously.

Recommendation 4: Companies should ensure that cybersecurity considerations are part of the patent/trade secret decision

Companies have long had the need to determine whether to disclose patentable inventions by filing a patent application or to retain them as trade secrets. What has changed is that cybersecurity exposures make it harder to keep the "secret" in "trade secret." 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 aren't eligible for patent protection. But many trade secrets are in the form of potentially patentable inventions, and in cases where companies are on the fence regarding which way to go, cybersecurity considerations can act to bias decisions away from trade secrets and in favor of patents. 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.

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 application is automatically published by the PTO 18 months after the claimed priority date. Of course, a company may choose to publicize the invention after filing the application but without waiting until the end of the 18-month period, and in that event the company would obviously lose trade secret status with respect to the disclosed information.

Third, if the company files a patent application with a non-publication request, the

[58] *Id.* "The petition must be filed within 1 year of the date 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."

invention can remain a trade secret until the patent issues, if it ever does. And if the patent never issues, then the company can retain the invention as a trade secret. Non-publication requests can only be submitted for inventions that have not been, will not be in the future, the subject of a foreign patent application. In practice, only a minority of companies elect this third approach because a non-publication request eliminates the opportunity to pursue foreign patents and also removes the ability to assert provisional rights with respect to the published claims in the pending application.

Companies choosing among these options should perform a realistic assessment of the difficulty associated with protecting a particular trade secret over the long term. 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, will end up stored in human-readable form (as opposed to in the form of compiled code) on hundreds of different computers, including the personal smartphones of company employees, probably won't stay secret for very long. If the trade secret covers patent-eligible subject matter, it could be a good candidate for a patent application. On the other hand, a trade secret that can be tightly controlled will have a higher chance of remaining undisclosed, increasing its likely long-term value.

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 can have advantages. As stated above, not all trade secrets are patent-eligible. But many are. There's nothing to stop a competitor from independently coming up with one of your company's trade secrets and then patenting it. Thanks to a new "prior user rights"[59] feature of patent law, if the competitor then sues your company for patent infringement, sufficiently early commercial use by your company of the trade secret can prevent a finding of infringement against your company.

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 not disclose their trade secrets to foreign competitors—are provided a defense against someone who later patents the

[59] The expanded prior commercial use defense to infringement in the America Invents Act 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. In addition, prior user rights generally don't to patents covering a university invention. And, the prior commercial use defense only applies if the commercial use occurred sufficiently early. See 35 U.S.C. § 273(a).

technology."[60]

Prior user rights are designed primarily to protect companies against patents arising from *independent* invention by a competitor. But they also have a potential role if an invention is stolen through an undetected cybersecurity intrusion. Having your company's trade secret stolen and then patented by a competitor is a clearly a bad thing. If the competitor then turns around and sues your company for practicing the very technology it stole from you, that's even worse.

In an ideal world, this should never happen. But in the real world, it could. In cases where there is no evidence that could be used to pursue a misappropriation claim, early[61] commercial use of the trade secret by your company can be vital in ensuring your company's right to continue using it. The flip side is that the prior user rights provision doesn't provide any protective power for a company that just sits on a trade secret, without commercial using it.

Conclusions

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

[60] America Invents Act, 157 Cong. Rec. E1219, E1219 (June 28, 2011) (Extended Remarks of Rep. Smith), *available at* http://www.gpo.gov/fdsys/pkg/CREC-2011-06-28/pdf/CREC-2011-06-28-pt1-PgE1219-2.pdf (last visited on August 21, 2014).

[61] The commercial use must have occurred "at least 1 year before the earlier of either . . . the effective filing date of the claimed invention" or "the date on which the claimed invention was disclosed to the public in a manner that qualified for the exception from prior art" under 35 U.S.C §102(b). See 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 won't 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.